PREMIER EDITION - RSA® CONFERENCE 2013

CDM

CYBER DEFENSE MAGAZINE

CDTL ANTI-VIRUS

CYBER DEFENSE TEST LABS CERTIFIED

We've tested some of the most promising next generation anti-virus products for consumers, small businesses and larger enterprises. Read the results in this special edition.

OUR LEADING INDUSTRY EXPERTS WRITE ABOUT...

- Cyber Crime and Cyber War Predictions for 2013
- What's Happening @ the RSA Conference 2013
- Government and Privacy IT Security Concerns
- Anti-phishing, Cloud Security, Covert Channels and Much More!

RSA® CONFERENCE

SECURE YOUR IT WORLD. THE PREMIER SOURCE FOR IT SECURITY INFORMATION.

PREMIER EDITION

DISCOVERING INFOSEC INNOVATION

THAT'S OUR MISSION AND OUR PASSION.

Every month we publish our electronic edition of Cyber Warnings Magazine. This Special Edition of CDM is published once per year, Print-edition exclusively available at the RSA Conference

WELCOME ABOARD

We are thrilled to join you at the RSA Conference 2013 with our Premier Edition of Cyber Defense Magazine. We're also honored to be here in San Francisco - one of the greatest cities on Earth. From the Gold Rush to the Cyber Security Rush, the race is on...in this fast paced city, we come together once a year to meet and discuss the future of IT Security. Surrounded by some of the brightest and most passionate minds in INFOSEC, one cannot help but feel the electricity in the air. As the field of Computer Science continues to evolve, creating new technologies and innovations, one can only imagine that the future in our field may be one of the most valuable on this planet of ours. We've reshaped communications, enabled every industry from banking to health care to e-commerce and the list goes on and on and on. It is sincerely an honor, to bring to you these fresh pages of new content covering what we like the most - What's Next? Hop on board the Next Generation INFOSEC Express. What's next for Malware? What's next in the Cloud? What's next in Government and Privacy? What can we predict for Cyber Crime and Cyber War in 2013? Turn these pages, read on and you might just find out...

Gary S. Miliefsky, CISSP
Executive Producer

Pierluigi Paganini,CEH
Editor-in-Chief

In this edition

Contents

CDM CREDITS

Cyber Defense Magazine (CDM) is distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats. All electronic editions are available for FREE, always. No strings attached. A limited number of print editions are available on a subscription basis and distributed at the RSA Conference 2013.

EXECUTIVE PRODUCER

Gary S. Miliefsky, FMDHS, CISSP®
garym@cyberdefensemagazine.com

EDITOR-IN-CHIEF

Pierluigi Paganini, CEH
Pierluigi.Paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

CDTL - LAB REVIEWS

Stevin Victor
stevinv@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Edward A. Adams
Phillip Hallam-Baker
Jeff Bardin
Allan Cowen
Clement Dupuis
Aaron Higbee
Peter Jenney
Colonel Michael Lacey
Christian Mairoll
Paul Paget
Tim Pierson
Dave Porcello
David Rosen
Richard Thieme
Dr. Hugh Thompson

Interested in writing for us:
writers@cyberdefensemagazine.com

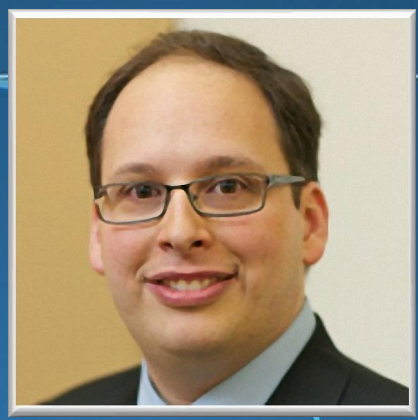
CONTACT US:

Cyber Defense Magazine

Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense

Email:
marketing@cyberdefensemagazine.com

Magazine:
www.cyberdefensemagazine.com



RSA CONFERENCE 2013: SECURITY REIMAGINED

Hugh Thompson, Ph.D.
PROGRAM COMMITTEE CHAIR, RSA CONFERENCE

Once a year, the world's leaders in information security overrun the city of San Francisco. The RSA Conference website will tell you that the event officially begins on a Tuesday – technically perhaps – but security pros have been at it since the weekend. You'll find them in nearly every restaurant, coffee shop and bar, talking about the challenges of PKI, the disruption caused by hacktivism, and why we need to shore up the supply chain. But amidst the discussions of familiar topics, if you listen closely, you'll hear a new tone of urgency. It's different from a decade ago when we were under assault from worms like CODE RED and NIMDA. It is also different from the worries that swept through our industry after STUXNET surfaced. The world has changed over the last 24 months: sophisticated and highly targeted attacks have risen dramatically, and in contrast to the hoopla over other security events like the Conficker worm, there is reason to believe that these new attacks are going heavily underreported and often undetected. Also on the minds of security professionals is the rapid migration of enterprise applications to the cloud and the growing use of mobile devices that carry sensitive data. These tectonic shifts in the threat environment and the way we work forces us to revisit some of the foundational assumptions of information security.

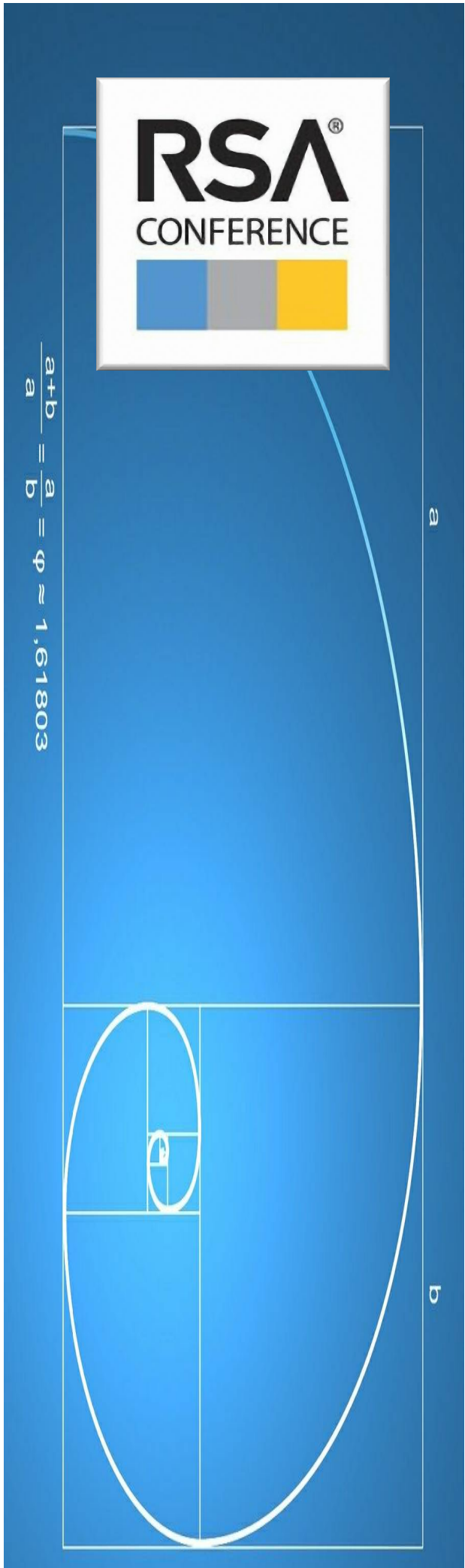
Part of that transformation in IT security is being driven by us losing control of IT. Cloud-based solutions targeting consumers are somehow now storing and transporting sensitive documents. Free consumer email accounts are used to shuttle corporate information to personal laptops in the name of productivity, but in breach of corporate policy. And employee-owned mobile phones and tablets are the new tools of business. All this change, so quickly, has forced security professionals to look for new controls to keep information safe. At RSA Conference, you'll see every facet of mobile security explored – from device management to mobile malware. You'll also find researchers, vendors and practitioners trying to unlock secrets of attacks, threats and vulnerabilities through analytics. Many organizations have found no refuge in the law or in their own security defenses against state-sponsored attacks and are poised to try what some are calling "active defense." Some have made progress on this front; while others are at the conference to see if the approach has promise.

As we've seen from a wave of targeted attacks over the past 24 months, one area of security that has been alarmingly under-addressed is the human element. If you look back at many of the sophisticated targeted attacks over the past couple of years and trace its roots, inevitably you'll find a well-meaning employee that made an unknowingly risky choice. As an industry, it's our Achilles heel and one of the greatest threats to businesses and government agencies. We force users to make nuanced security choices: do I accept this expired certificate or reject it? Do I click on this shortened URL or not? Should I install this browser plugin or skip the rich content on this website?

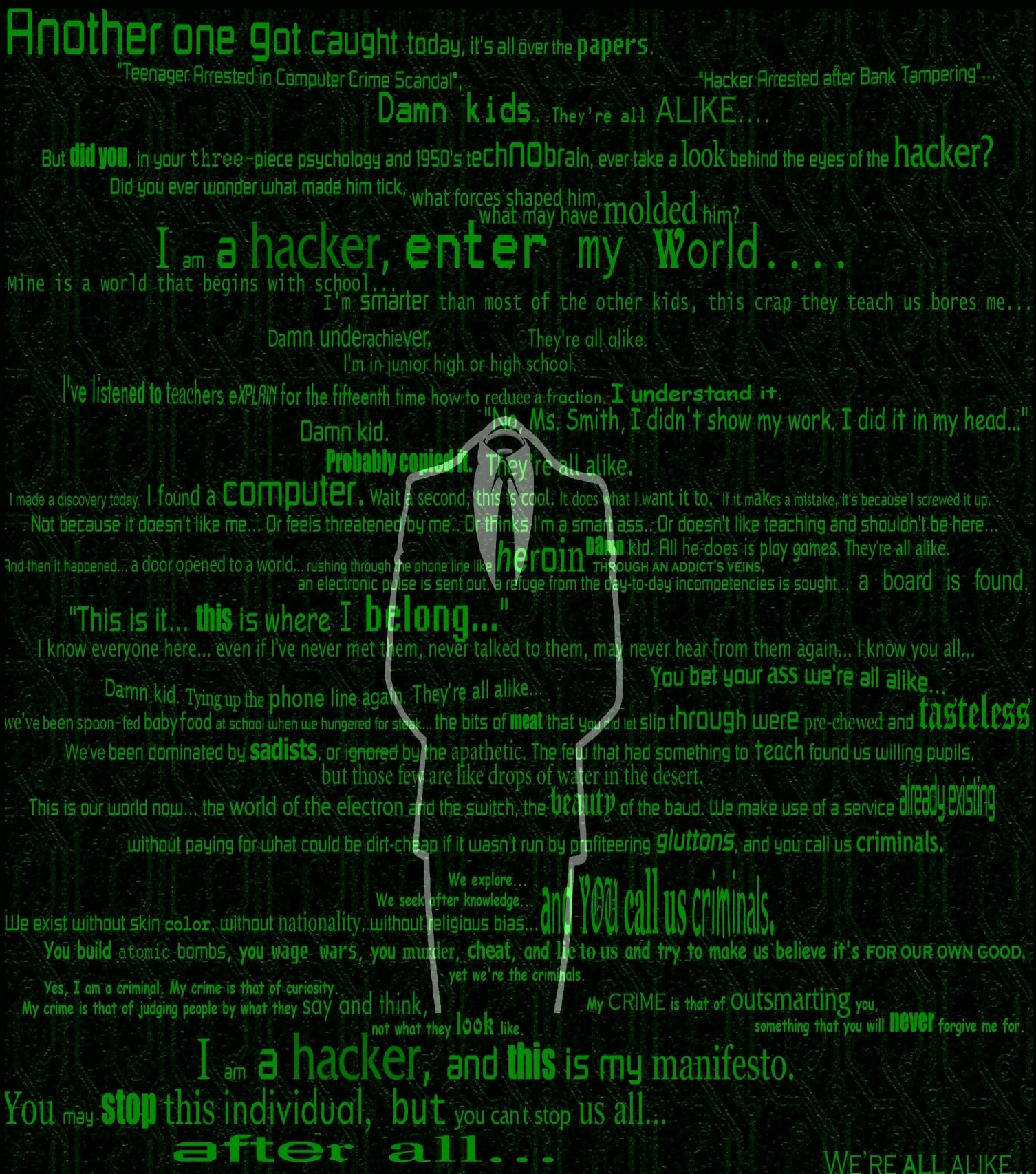
Even IT pros have problems with some of these decisions and in confusion and ambiguity lays opportunity for attackers. Beyond getting some malware on a machine or asking you to email out sensitive data, attackers have figured out that the game isn't to outwit security controls, it's to exploit the software running in the minds of employees. We all have vulnerabilities. Some of us are suckers for news about our favorite sports team. Some of us abandon our intellect if we see an email that pretends to come from the IRS.

Everyone, at some point, can be deceived. Imagine that we solved the DLP problem on the network and endpoint – attackers will start sending printed forms and give victims just the right cover story to induce them to take out a pen and bleed internal secrets onto a page. Then only a postage stamp sits between an organization's data and attackers. No vendor has a patch for the ball point pen, and the postal service isn't running DLP on sealed envelopes.

The battleground is shifting. It's moving from a perimeter that was once closely guarded to an information infrastructure that extends to the cloud, mobile phones, tablets and our own mind. The good news is that the information security community is vibrant, and despite criticism over the years about us rehashing the same problems, innovation is happening. Look for "security intelligence," "active defense," "analytics" and a few other themes in conference talks this year. Swing by Innovation Sandbox on the Monday of conference week to see what some of the most provocative security startups are working on. Hit at least three vendor parties and ask them what they think the world will look like three years from now. I hope you'll see the week as I do: RSA Conference 2013 is the place to recalibrate and reimagine what information security is. All the raw ingredients are there – smart people, passion for our field and the motivation of an active, intelligent set of adversaries. Turn the pages of this magazine, meet with innovators, listen to experts in the field and you'll have a taste of what's to come. *Let the innovation begin…*



Cyber Defense Starts With Awareness. Have You Read The Hacker Manifesto?



Now You Have. Let The Journey Begin…

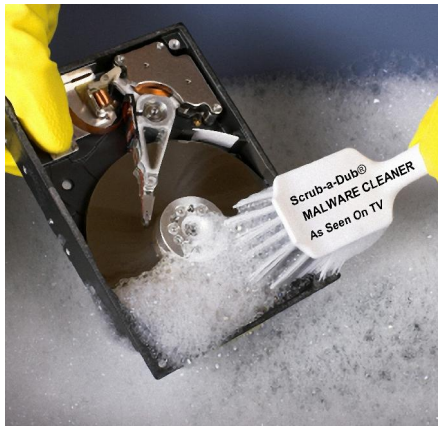
MALWARE CLEANING – A DANGEROUS ILLUSION OF SECURITY?

BY CHRISTIAN MAIROLL, FOUNDER AND MANAGING DIRECTOR OF EMSISOFT

When a computer is infected, almost every Anti-Virus program offers a cleaning routine. But whether it makes sense or not to clean infected computers is a topic of repeated heated discussion in the IT security world. Questions such as "Can a computer that has been malware-infected once be a clean computer again? " or "Is it technically possible to completely clean a system?" always come to the forefront of these discussions. How does Malware infect computers? There is no one general way of malware infection. Each malware type infect computers different and they must be analyzed individually in order to understand that:

Viruses

Until recently, most of the known damaging programs were viral in nature. One property of Viruses is that they



use other host applications in order to be able to run. A Virus always attaches itself to a benign program by inserting its own Virus program code into the executable file of another program (e.g. an .EXE file). Once the benign program is loaded the Virus can begin its damaging routines and use other programs to reproduce itself. These days, Viruses play a much smaller and less important role in the Malware sector.

Trojans, Backdoors, Bots and Worms

Most of the new damaging programs these days are Trojans and Bots. They do not require a host program to run because they are independent programs. Bots attempt to remain as inconspicuous as possible and usually hide well camouflaged in the depths of the operating system. Their activities include opening the PC for attackers who thereby gain full control of the PC, mass-mailing of illegal Spam mails, or the coordinated overloading of individual websites through too many manipulated queries at once (DoS). The PC can only be regarded as infected when this type of software is actually active. Files that are not running do not represent a danger. However, Trojans and Bots usually have numerous

"TO FORMAT OR NOT TO FORMAT"

That is the question...

"Even after cleaning, a hidden Rootkit may still exist on the computer that is not yet detectable by current technology."

LET'S SCRUB THAT SCREEN SCRAPER

AND KEYLOGGER RIGHT OFF YOUR MONITOR

features to ensure that they are automatically started every time the system is booted. Autostart entries are created in a wide variety of system Registry locations, file suffix assignments are redirected, or other new tricks are used that most security tools are not yet aware of.

Spyware, Adware, Bogus Security Software

A new Malware trend is to manipulate important system components so that the Malware file can no longer simply be deleted. Some types of Spyware start multiple processes (program instances) in parallel that monitor each other. When one process is terminated the other process starts it again, etc. Bogus security software, so-called rogue Anti-virus and Anti-spyware tools, inject themselves into essential system processes such as (e.g.) winlogon.exe. If you attempt to terminate the Malware, by terminating the host process and deleting the damaging file, the action ends with the dreaded bluescreen and the system comes to a standstill.

Rootkits go one step further. They manipulate the operating system so that the Rootkit files are no longer visible and can no longer be detected by Anti-virus programs. Registry entries, open ports, and active processes can also be made invisible, thus leaving no traces of the presence of a Rootkit. The infection types described above represent the most common Malware segments. Of course, various combinations of these techniques also exist.

So is it however possible and sensible to clean a system?

Malware constructed in a simple manner can usually be completely removed from a system with a high level of reliability. With more complex types a number of problems can occur:

Virus Disinfection

Since Viruses attach themselves to other programs, cleaning just requires removal of the appended code. This sounds easy but can be tricky. When a Virus not only appends itself but also manipulates the original program file in other ways, e.g. through compression or encryption, then disinfection is almost impossible. As a result of the evolutionary development of Viruses, years ago the Anti-virus manufacturers began completely deleting infected files or placing them in quarantine. This also prevents a failed disinfection from destroying a program file. Virus disinfection can also be extremely technically complicated and is usually only provided for the most common Viruses.

Cleaning a Trojan Infection

To free a PC of Trojans or Bots it is usually sufficient to kill the active damaging process and then delete the executable Trojan file(s). Almost all Anti-virus and Anti-malware scanners do this. Some scanners also then search the system for Autostart entries or additional Malware modules and destroy these as well (even if they no longer represent a direct threat).

> "A New Malware trend is to manipulate important system components so that the Malware file can no longer simply be deleted."

Removing Spyware and Adware

The term Spyware now covers a relatively wide spectrum of programs. Some are regarded as undesirable software because they gather data and violate user privacy. Apart from this, these programs do not attempt to prevent their deletion. In an ideal case you can simply de-install them via "Control Panel / Add or Remove Programs" or using the uninstall feature of the program itself. Adware or bogus Anti-virus programs are a completely different case. These use every possible means to force the user to spend money. The creativity shown by the programmers seems to be unlimited.

Often, the only way to remove some of these programs is to use special tools that allow files to be deleted before the system actually boots. Very few security programs are currently capable of removing such infections.

Removing Rootkits, the Premiere League

Rootkits have almost perfect camouflage properties. To remove them you must first know that a Rootkit even exists.

This brings us to the main problem in this topic: All current Rootkit scanner technology is unable to provide a guarantee that an active Rootkit has not fooled the scanner and hidden its own existence.

This is the same old cat and mouse game: Hackers find new ways of hiding - Anti-rootkit manufacturers discover these and extend their detection methods, until the Hackers once more find new ways...

Once the PC is infected - Install from scratch!

The more complex the Malware, the more difficult the cleaning process. The main problem is that you can never be really sure that the cleaning was completely successful.

In many cases the cleaning functions of security products function as placebos that disguise the true facts: The logical conclusion that the PC can no longer be trusted once it has already been infected by Malware.

Why?

Even after cleaning, a hidden Rootkit may still exist on the computer that is not yet detectable by current technology.

It is much more likely that an infection has manipulated important operating system components.

For example, file shares may have been created that open the PC to attacks, or programs may have been changed so that they embed damaging code in created files.

The ONLY way of making the PC usable again is therefore to format the hard drive and reload the operating system!

The perfect solution: avoid infections

People visit doctors not only when they are sick, but also for prophylaxis. The question about the reliability of cleaning does not even play a role when Malware isn't able to infect a computer. However: Do not trust cleaning alone. Protecting the PC against Malware infection in the first place is always better than subsequently attempting to clean up the chaos created by an infection. This means using a multi-layer protection system consisting of:

Keeping software up to date

A significant number of damaging programs gain access to the PC through security holes. Always keep your operating system up to date. The automatic Windows Update should always be activated because often only a few days pass between the publication of a security hole and the massive exploitation of this hole by Worms. It is also necessary to keep all programs accessing data via the Internet up to date. These include Browsers, PDF Readers, MP3 Players, Image Viewers, etc. because these process data that can contain damaging code.

Surf Protection

Avoid navigating to dubious websites where you can catch Malware. This can be easily implemented by using Host Blockers or Firewalls with appropriate functions.

First Major Hurdle: Signature Scan

If you still download and start a dangerous file, there is a 99% probability that this will be detected and prevented from starting by a signature-based Malware Guard.

"Protecting the PC against Malware infection in the first place is always better than subsequently attempting to clean up the chaos created by an infection."

Second Major Hurdle: Behavior Analysis (proactive detection)

New Malware, and programs designed for specific individual attacks can only be detected and prevented from starting by behavior analysis based Malware Blockers.

About the Author

Christian Mairoll is the Founder and Managing Director of Emsisoft HmbH. He and his team are committed to delivering the best possible virus detection and protection for home and business users. More than 6 million users world-wide use Emsisoft award winning products for their quality and outstanding detection rate. Visit Christian online at http://www.emsisoft.com to learn more.

Scrub-A-Dub® Malware Cleaner Disclaimer: Most hard drives will not function after we have cleaned the surface. If the Hard Drive is infected with zero-day malware such as H1N7 or STEXNUT, magnetic drive wiping may be required.

"Pwnie Express the Best of Class for Penetration Testing 2013"

Cyber Defense Magazine

Thanks for the props. See you at RSA Booth #2747

Cyber Defense Magazine has named Pwnie Express "Best of Class for Penetration Testing 2013." We're dedicated to bringing the best pentesting equipment to light in 2013.

PWNIE EXPRESS

PwnieExpress.com | 802-227-2PWN

- Pwn Plug
- Power Pwn
- Pwn Phone
- EPA

Put Cyber-Sabotage in the Terrorism Box

By Dr. Hallam-Baker, Co-inventor of the World Wide Web

One of the oldest fallacies in the history of warfare is the belief that a new weapon will prove to be so destructive as to give one party a permanent advantage over all others. The chief challenge of military planers today is to work out what role information weapons will play in the battlefield of the future. In this piece I argue that the leading powers should abandon one particular form of information warfare, cyber-attacks on critical infrastructure, a type of attack I call cyber-sabotage. Like terrorism, cyber-sabotage is a form of warfare that is a resort of the weak, a tactic that has unpredictable effects that fall almost entirely on non-combatants. Making the argument against one form of information warfare does not mean that we can or should forgo all forms of information engagement. On the contrary, information warfare provides a unique and unprecedented capability. For the first time in history popular opinion is the most important factor in bringing conflicts to an end. Had the wisdom of Washington elites been the deciding factor, the US would still have an army of occupation in Iraq still holding out hope that the next six months would see a change in fortunes. Unless, that is, the continuing engagement in Vietnam had not prevented the misadventure in Iraq first. Elites naturally see this role of popular opinion as an affront to their own position and a threat to national security. But popular opinion is ultimately what gave the West victory in the cold war. Freedom won because the youth of East Germany and the rest of Eastern Europe simply walked away from a system that they could see was rotten to the core.

Freedom will ultimately win the Arab Spring. Even if the politicians who replace the dictatorships of the past are just as corrupt, they know that their regimes must survive in an age where the Internet and the camera-phone can turn any incident of government abuse into an occasion of government accountability.
The democratic powers were strongest during the cold war when they spoke with moral authority. The cold war was not won by the squalid realpolitik that saw democracies pushed aside in favor of despots in the name of stopping the spread of communism. The cold war was won by big ideas like the ability to speak the truth about the government without being threatened with the gulag.
In an information war, the moral high ground is the strategic high ground. The US is not going to win an engagement with Russia or China by crippling their civil infrastructure. Nor are groups of hacktivists whether state sponsored or irregular going to do effect any political change by threatening to hold civilization hostage. In an earlier age the pen was mightier that the sword. Today the proof is all around us that the keyboard is mightier than Mao's barrel of a gun.
The cold war might have been won faster if the Western powers had listened more to Ghandi and less to Kissinger. We should not repeat the same mistake in the new age of information wars.

Web Security Comes Full Circle

Recent government and politically motivated attacks on industrial control systems (aka 'SCADA') bring Web Security full circle. When I first began work on the World Wide Web in 1992, it was a tool for experimental physicists. The Web protocols had to be made secure before they could be used to control experiments involving expensive equipment, extreme heat, extreme cold and radiation. Making the Web protocols secure would be an important part of winning the race to establish the definitive network information system.
Surprising as it might seem today, the Web was not the first network information system or even the first based on hypertext. In 1992 the Web was considered so far behind its rivals that the paper describing the Web to the annual international conference on hypertext was rejected. The Web had certain technical and social aspects that gave it an advantage, one of the most important being that the code and the protocols were all in the public domain. But even in 1993 as the Web began to eclipse early competitors such as Gopher, it was clear that a new entrant might eclipse the Web in turn. In 1993 the Web was thriving in academia but commercial use was essentially non-existent outside the computing industry itself.
A similar situation had developed during the introduction of the microcomputer. The Commodore PET and Apple II went into an early lead but the market was thick with new competitors until the arrival of the IBM PC and its clones. The IBM PC was more than just a micro-computer, it legitimized the idea of personal computing in business. To win the network information system race we needed an endorsement by a universally credible third party to legitimize the Web.
A week after I first met Tim Berners-Lee and saw the Web at the launch in Annecy, this mode of thinking led me to contact Jock Gill who was then in charge of the Clinton-Gore '92 online campaign. The Web community stood at about a hundred users so I naturally suggested using the Web in the Clinton White House. The Web would meet the campaign's desire to 'disintermediate' the press and talk directly to voters. But putting the Web into the White House raised a whole new set of security concerns.

Put Cyber-Sabotage in the Terrorism Box (continued)

Security of any government information system is a national security issue. The success of a coup d'état usually depends on the ability of the coup plotters to take control of the television and radio stations. Francis Bacon was only partially correct when he said that knowledge is power: Control of information and in particular the ability to distribute disinformation can also bring power. The White House could only establish an online presence if it could assure the President that it would be secure. This concern were validated during the Russian invasion of South Ossetia in 2008. The Russian advance was facilitated by a series of cyber attacks against government sites run by the Government of Georgia.

Twenty years later I find myself attending meetings of serious government people at which we are told that the threat of cyber-warfare today is as great as the threat of nuclear warfare during the cold war. We are told that the Western powers are falling behind and we must therefore take urgent steps to establish dominance of this new form of warfare or face the threat of cyber-Armageddon. These are men of action: declare war or martial law or better both at the first hint of a cyber-strike. There will be no time to think: Ready! Fire! Aim!

After listening to these arguments at length I find myself asking if developing capabilities to disrupt or destroy civilian infrastructures are in the national interest or merely the personal interest of those proposing them. The cold war arms race certainly provided a lot of satisfaction to the generals and the politicians involved and large profits to the contractors. But did it really serve the national interest?

Some of those involved would rather obviously welcome a cyber-arms race. They talk in terms of 'signaling' and 'deterrence' how Russia and China might be persuaded to agree rules for the new game. They ask me as a technologist to find a means of 'attribution' for cyber-attack so that cyber can be made to fit into the ideology of nuclear deterrence that has dominated their government careers.

From a technical point of view, cyber-weapons could hardly be further removed from nuclear. Nuclear deterrence is possible because the number of parties with nuclear weapons is very small and all (appear to) understand the rules of the deterrence game. This in turn is because the design and manufacture of a nuclear warhead requires a vast commitment of resources that is limited to a small number of states that are wealthy in absolute terms if not necessarily on a per capita basis.

The barrier to entry in production of cyber weapons is very low. A zero day attack can be purchased online for a few thousand dollars or less. Turning such an attack into a cyber-weapon is well within the capabilities of an engineer of ordinary skill in the art.

For the patient attacker, the barrier to entry for acquisition of cyber weapons is zero. Whatever target the authors of the Flame and Stuxnet malware intended to strike, their creation has been repurposed and retargeted on many occasions. The opportunist cyber-warrior does not need to invest heavily in technical research, he can free ride on the practically infinite stock of malware already in circulation.

If cyber warfare is really the new nuclear weapon, it is a nuclear weapon that the target can collect up from the battlefield and reassemble to throw back at the attacker. Deterrence requires the ability to correctly attribute attacks to the attacker. Without attribution, a threat of retaliation becomes an invitation to a false flag attack. The US can draw a 'red line' and threaten a 'kinetic' response to a cyber-attack, but where does it send the missiles? If the US promises to respond to a cyber attack on US critical infrastructure

that is the purported issue of concern.
Although nuclear and cyber are very different from a technical point of view there are two important similarities. The first is a tendency to use euphemisms to avoid admitting the full scope of what is being discussed. Rather than refer to the use of bullets and bombs to cause death and destruction, the Cyber warfare community prefers the word 'Kinetic', a term that seems to cute by half. Second and more importantly, like nuclear bombs, drones and almost every other new development in warfare, cyber weapons look most attractive when the ability to deploy them is limited to 'our' side.

The unmentioned precedent: Terrorism

The closest precedent to cyber-attacks against critical infrastructure is not nuclear warfare but terrorism. Like terrorism, cyber-attacks present a low barrier to entry with plausible deniability for state actors. Like terrorism, cyber-attacks are primarily a weapon of fear rather than effect.
A reason sometimes given for resisting this comparison is that it 'exaggerates' the extent of the threat and could serve as a pretext for over-reaction. Deciding that cyber-attacks against critical infrastructure have similar characteristics to terrorism does not commit governments to any particular form of response. It does however preclude considering cyber-attack as an alternative to warfare.
Neither China, nor Russia have any such qualms about the use of term 'terrorism' and they are anxious to secure an international ban on practices they call 'Information terrorism' and liberal democracies call 'freedom of speech'.
Here we face the real difficulty of cyber-warfare, what forms of engagement are legitimate and which illegitimate? Is it the techniques or the targets or the intended consequences that render cyber-attack illegitimate? The line between 'terrorism' and 'legitimate warfare' has always been an ambiguous one. When information becomes a weapon, the ambiguity increases further.
This is a difficult question that nobody can fully answer. Some forms of attack are clearly illegitimate: Since poisoning the water supply through a conventional attack is already acknowledged as illegitimate then so is achieving the same end result through a cyber attack. At the other end of the scale the mere movement of information from one place to another is not a use of force and cannot therefore be an illegitimate use of force. The line between legitimate information engagement and illegitimate terrorism lies somewhere between those poles but we do not have to place it exactly to outlaw attacks that threaten the fabric of civilization.
State sponsored cyber crime such as the Russian Business Network (RBN) is criminal and reprehensible but granting immunity from prosecution to such groups does not amount to an act of war. Employing the RBS to perform cyber-sabotage would.
The extensive cyber-espionage efforts undertaken by the Chinese government are not acts of war either. All states engage in espionage and it is usually to the mutual benefit that they do so. The intelligence community has long understood that there is a distinction between espionage and sabotage. The line may be crossed but never without consideration.
The form of engagement that the Russian and Chinese governments would like to see prohibited is the flow of ideas intended to effect political change. It is likely that their concern extends beyond the survival of their own regimes. From the perspective of Moscow or Beijing, the Arab Spring must look remarkably like a recapitulation of the 'domino theory' that led the US into its misadventure in Vietnam.

In this case the path of the falling dominos leads much closer to home, to the unstable ex-Soviet satellites that create a buffer zone between the South Western border of Russia and the North Western border of China. Many of these countries have large ethnic Russian and Chinese populations. A civil war in this region might easily pull one of the major powers into the conflict, or both.

It will take some time to determine which forms of cyber attack are legitimate and which are not but the need is urgent as adverse precedents accumulate. If such a process had begun five years ago we might have expected that an initial consensus that cyber attacks against civil nuclear facilities were off limits. Yet now we discover that the adverse precedent in this respect has been set by our own side and that the target of the attack is busy demonstrating its ability to retaliate against the oil infrastructure that provides fuel to the West

Development of cyber-sabotage capabilities is not only unethical it is counter-productive to efforts to defend against them. Like terrorism, cyber-sabotage is a form of warfare that developed nations fight at a considerable disadvantage: We offer many targets, our opponents present few or none. Like terrorism, torture, and use of chemical and biological weapons, cyber-attacks against critical infrastructure should be considered war crimes and prohibited by international treaties.

While such a proposal may appear an unachievable utopian fantasy, history suggests the opposite to be the case. In history, unrestricted warfare has been the exception rather than the rule. One of the key attributes that distinguishes the leading powers of every age is their ability to define the rules of the game. The law of war has developed as the leading powers of the day have outlawed tactics and modes of warfare that are to their disadvantage.

The Potential of CyberSabotage

One of the imponderables of cyber-weapons is whether they can really be called a proper weapon at all. One of the main properties that distinguishes a weapon from a random object used in desperation is that its ability to inflict damage is predictable. A knife is a weapon but a paving slab is only a weapon of last resort. The efficacy of a nuclear weapon is depends only on the engineering skill or its designers and the laws of physics. The effect of a cyber weapon is unknown until it is deployed and once deployed it can be turned against the attacker with relative ease.

Estimates of the potential consequences of cyber-sabotage range from none-at-all to a total collapse of civilization. A plausible argument may be made for both cases. It is most probable that the consequence of a cyber sabotage will be modest to negligible but there is a possibility if however unlikely that the result will be catastrophic.

Modern civilization depends on technology to an unprecedented degree. In his 1978 Tv documentary series Connections, James Burke argued that we live in a technology trap: Life in modern cities is not just unthinkable without access to clean water, sewage and power, it is impossible. We depend on a complex web of infrastructures, the interdependencies between which are only partially understood.

Without power for the pumps at filling stations the transport infrastructure fails. Without transport there is no means of harvesting food or bringing it to the population centers. Power, water, transportation and communications are all interlinked and interdependent.

These assessments are not entirely theoretical. The New York City blackout of 1977 triggered rioting and looting

Put Cyber-Sabotage in the Terrorism Box (continued)

that resulted in $300 million of damage. Over 1,600 stores were affected and the fire department responded to over 1,000 fires. Some hypothesize that the effects of a cyber-attack could be wider and last much longer leading to a complete descent into anarchy. The New York City blackout lasted less than 24 hours, what if it had continued for several months? But also note the fact that blackouts of similar scale since have not been accompanied by social unrest.

The power distribution infrastructure is of particular concern because of the way in which it can fail: A cascade failure. In a cascade failure an overload in of one part of the grid causes it to shut down which causes neighboring parts of the grid to become overloaded. The neighboring parts of the grid then shut down overloading their neighbors in turn. Eventually the outage becomes so widespread that the only way to prevent further damage is to intentionally shut down the whole grid and restart.

It is not just the power generation and distribution infrastructure that we depend on. Without clean water and sewage modern cites quickly become a public health catastrophe. The Internet is becoming a source of dependency and not just vulnerability. Without the Internet, the vast supply chain infrastructure that brings food and other necessities from ports and farms to supermarkets collapses.

The power distribution system is susceptible to cascade failures because the system is interconnected and interdependent. The Internet is likewise interdependent and interconnected and so is every computer connected to it. As with terrorism, there will always be a possibility that an attack might have devastating consequences even if the likely consequences are small or inconsequential.

Such apocalyptic scenarios are much easier to propose than dismiss. Suggesting a potential vulnerability requires only a little familiarity with the subject matter. Demonstrating that an attack is infeasible requires an in-depth audit of each and every facility that might be targeted.

But even accepting the catastrophic potential for such attacks, the military value is negligible. No country surrenders because they have suffered a devastating attack. A country surrenders because they fear a devastating attack will be repeated. Cyber-weapons offer only a one time use and cannot be relied on to work even once.

However unlikely such events might appear, past experience only provides a lower bound on future risk. The idea that any government much less the US might attack a foreign nuclear facility with a sophisticated logic bomb appeared far-fetched before the discovery of Stuxnet and the tacit US admission of responsibility.

War by Other Means

Perhaps the most dangerous aspect of cyber-sabotage is the appearance that it offers (to misstate Clausewitz) 'war by other means'. A cyber attack intended to damage or disrupt is a use of force and thus a form of warfare but the appearance of plausible deniability makes it tempting to see it as an alternative to actual war.

Some hold that deployment of Stuxnet against Iran's nuclear program was preferable to the alternative of bombing the nuclear enrichment facilities, an act which would almost certainly have led to a full scale war. Framed in this fashion the argument

Put Cyber-Sabotage in the Terrorism Box (continued)

for choosing cyber-sabotage over conventional warfare is a strong one. But these are not the only choices President Obama faced. To do nothing at all is almost always an option and very frequently the best available option.

Statistics published by the Federation of American Scientists suggest that the number of uranium enrichment centrifuges in operation in Iran was reduced from approximately 4,700 to 3,900 during the time period in which it is believed that Stuxnet was deployed. The best that can be said for Stuxnet from a strategic point of view is that it achieved a temporary reduction in the number of nuclear weapons that Iran might have acquired.

There are many who argue the case that the US should go to war rather than permit Iran to acquire any nuclear weapons but I have yet to see the argument made in any quarter that the US should risk war in order to limit Iran to three bombs rather than four or thirty bombs rather than forty.

Eighteen months after the exposure of Stuxnet, no conventional attack has taken place. We must conclude therefore that Stuxnet was not deployed as an alternative to a conventional attack. If the cyber option had not been on the table, the most likely course of action would have been to do nothing at all.

The political interests of the administration are not identical to the national interest. Deploying Stuxnet avoided the need for the Obama administration to expend political capital to discourage an Israeli air strike that would have led to diplomatic crisis and most likely begun a wider war. But the cost of that political convenience is a precedent by which the US holds it to be acceptable to perform cyber-sabotage against declared civil nuclear facility under International Atomic Energy Authority monitoring.

Like terrorism, cyber-sabotage offers the option of an attack in circumstances where the most likely course of action would have been to do nothing. Rather than providing 'war by other means', cyber-sabotage blurs the boundary making it easier to slide from peace into war.

It is not just the states themselves that might cause or encourage such a slide. 'Hacktivism' by independent and not so-independent activists is now a feature of almost every international crisis. While diplomats are seeking to diffuse a situation and seek common ground the hacktivists are busy trying to escalate the conflict and reject any compromise.

In the wake of 9/11 the US held the Taliban government accountable for the attack planned and performed by Al Qaeda operating within their territory. The same precedent might be applied in the case of a major cyber-sabotage and could be applied by any country that had been attacked against any suspected attacker.

An event that crippled the critical infrastructure of Russia or China could lead to a global war regardless of whether that attack was performed by the US government, state sponsored hacktivists or a freak event that was misattributed as an attack. If the objective is to avoid war, it is in the interests of the US that the Russian and Chinese civil infrastructure is protected.

Rather than regarding weaknesses in the Chinese and Russian critical infrastructures as potential vulnerabilities to be exploited, we should consider them as potential causes of war. Rather than considering defensive measures to protect critical infrastructure as a strategic security advantage to be jealously guarded we should encourage their use.

Put Cyber-Sabotage in the Terrorism Box (continued)

The Cost of the Cyber 'Option'

For the Western powers the prospect of cyber-sabotage is that of the man who lives in a very large greenhouse: Whatever the benefits of developing a stone throwing capability might be, his real problem is that he is living in a greenhouse and so are some of his rivals. Maintaining the option of throwing stones makes it much harder to develop and deploy stone-resistant greenhouse technology, both at home and abroad.

Reserving the option of performing a cyber-sabotage compromises the position of the US government when it attempts to collaborate with industry to protect cyber assets.

The US government and US government contractors have played a major role in the development of Internet Engineering Task Force (IETF) security protocols. In particular the PKIX standard that is the principle authority on the use of public key cryptography in Internet protocols. In recent years there has been a marked divergence of opinion between engineers working in the commercial and government sectors with the commercial sector seeking a more pragmatic approach and the government sector resisting any modifications to the specification.

While there is no evidence to suggest that this disagreement is due to anything more than an honest disagreement of views, there is a clear motive for and no evidence to disprove a conspiracy to maintain known vulnerabilities that parts of the US government might have planned to use as exploits.

Attacks on public key infrastructure appear to be something of an NSA house style. The Flame and Stuxnet malware both relied on the illegitimate use of public key certificates.

The Stuxnet attack involved the use of two code signing certificates that had been legitimately issued by VeriSign.

The Flame attack involved certificates that had been issued by means of a cryptanalytic attack on a Certificate Authority run by Microsoft.

VeriSign and Microsoft are both US companies that play a major role in the computer security industry. How can the US government collaborate with these companies when its own military is attacking them?

The cause of Internet security was set back by at least a decade by the 'crypto-wars' of the 1990s. Fearing the loss of their ability to intercept communications, the NSA and FBI mounted a campaign of harassment against advocates of civil cryptography such as Phil Zimmerman who spent several years under threat of indictment for an alleged breach of the Export Control Act.

Some of the consequences of the crypto-wars live on in Internet security protocols today. During the crypto-wars the first concern of most cryptographic security protocol architects (including I am sorry to say, myself) was to defeat government interception efforts. In some cases defeating government interception was also the last and only concern. The result was a generation of security technologies where most will work perfectly in theory but so difficult to use that even the creators don't use them.

For Internet security to improve we need the government and commercial sectors to work together. Maintaining the option of performing cyber sabotage will fuel mutual suspicion and greatly damage these efforts.

One of the main concerns Western cyber-defense practitioners face today is the fact that much of the computing and control equipment deployed in Western countries is made in China, one of the two countries considered most likely to be a cyber adversary. This situation has led many to propose a technological form of autarky in which the US would only permit equipment made and manufactured in the US to be used in US critical infrastructure.

Such an autarky policy would be a foolish illusion as anyone familiar with US high technology industry will realize. The US education system does not produce enough software engineers to meet the demands of the US technology industry. The commercial sector relies heavily on immigrant labor and outsourcing for software development work.

According to Pike Research, the market for industrial control systems is a mere $369 million/year. Even assuming rapid growth in the wake of Stuxnet, the market is too small to justify a different development approach. Control engineering is unfashionable enough without requiring software to be written to the peculiar (and expensive) dictates of classified projects.

The Chemical Weapons Ban

One of the principal arguments made against a ban on cyber-sabotage is that unilateral disarmament is unacceptable and a multilateral approach is unfeasible. Again the nuclear analogy is misleading.

Cases of unilateral disarmament are actually very common. No modern army deploys swords, canons or catapults. These weapons have been abandoned in favor of alternatives that are more effective. The major powers have abandoned chemical and biological weapons and insist that they would never engage in 'terrorism'.

Unilateral nuclear disarmament requires a government to give up a weapon that is known to be effective in return for the hop that others will do likewise. Giving up a weapon that has a marginal utility is considerably easier.

In 1812, the British naval hero Thomas, Lord Cochrane proposed the use of 'sulphur ships' as a means of winning a decisive naval victory against France in the Napoleonic wars. The proposals were turned over to a panel of experts which concluded that the ideas had merit but pursuing them was 'inexpedient'. As the Duke of Wellington put it, this was a game that 'two might play'.

The role of chemistry in the late Victorian era was very similar to that of information technology in our own. Electric power and the telegraph existed of course, but like bio-technology today, these were the rising stars whose full potential would only start to be realized a generation later. Chemistry was the driving technological force of the day. It was developments in chemistry that made mass production of high quality steel possible, chemistry that enabled the revolution in pharmacology, chemistry that created the aniline dyes that had turned Germany into an industrial power. An understanding of the capabilities of modern chemistry was as essential to the politicians of the age as an understanding of information technology is in our own.

The policy makers were well aware of the potential of chemical warfare and rejected them at the first opportunity.

Use of poison or poisonous weapons banned was banned at the Hague conference of 1899 but this did not prevent the use of chemical weapons in World War I. Use of tear gas by the French was followed by bombardment with chlorine gas by the Germans which led to its use by the British at the battle of Loos in 1915. It was at this point that the British discovered the chief practical drawback to chemical warfare: Attacks frequently backfire on the attacker. This lesson was later re-learned when Germany deployed mustard gas against the Russians at Riga. The gas caused large numbers of casualties but contaminated the soil preventing capture of the abandoned trenches.

Put Cyber-Sabotage in the Terrorism Box (continued)

According to a 1984 US army study, over 50,000 tons of chemical weapons were used in World War I, resulting in approximately 85,000 fatalities. While the effects of chemical weapons were hardly negligible, this is a small fraction of the 16 million total fatalities in the war. The casualty rate dropped quickly after the initial surprise as the French, Germans and British developed effective gas masks.
This outcome is very similar to experience of cyber-sabotage. The practical effect of cyber has proved to be modest and diminishing over time as the element of surprise has been lost and targets have deployed effective defenses.
Use of chemical weapons did not end with World War I but the major powers have formed a consensus that chemical and biological weapons are an illegal form of warfare. Use but not possession of chemical and biological weapons was banned under the 1925 Geneva Protocol. Possession of chemical weapons was banned under the 1968 Chemical Weapons Convention and possession of biological weapons was banned under the Biological Weapons Convention of 1972.
These treaties have consequences, at least as far as lesser powers are concerned. In making the case for war against Iraq, Secretary of State Colin Powell asserted that "there can be no doubt that Saddam Hussein has biological weapons and the capability to rapidly produce more, many more." The mere possession of chemical or biological weapons is now established as a casus belli.
While the major powers have the ability to violate the treaties, the incentive to do so is weak. One of the principal reasons that chemical and in particular biological weapons have been abandoned is that they are not very effective and there is a very strong likelihood that they will backfire.
Current research into chemical and biological weapons has to be undertaken under at least the pretense of developing defenses against their use. But even this can backfire as the US anthrax attacks in 2001 demonstrate. While it is likely that decisions taken by the FBI investigators mean that the identity of the attacker will never be known with certainty, it is now generally accepted that the anthrax spores used in the attacks came from a US government biological weapons research lab.

Could a multilateral ban work?

The Hague protocols did not prevent the use of poison gas but that was not the only failure in the system. The Hague III protocol (1907) also required that hostilities must not commence without warning, a requirement that Germany had violated in the invasion of Belgium.
The primary purpose of the protocols was to prevent a European war rather than mitigate the consequences. In the event they did neither. The third convention planned for 1914 had to be abandoned due to the start of World War I. Nor should this be surprising. At the time they were signed the Hague Conventions were merely another international treaty. They only began to establish their current status as one of the foundations of modern international law after World War I when the victorious allies realized that they provided a convenient basis for blaming Germany.
The now universal condemnation of the use of torture has similar origins. At the start of the reformation, use of torture was routine in every country in Europe. By the start of the 17th century what had begun as a largely political dispute in which religion was arguably a pretext rather than a cause had become an ideological conflict. Ideological conflicts are fought with ideas. The image of the martyr resisting the tortures of the inquisition was a powerful and attractive one for the Protestant side.
A century after they were agreed the Hague Protocols and the system of international law that emerged from them are as deeply embedded in government thinking as the Congress of Vienna that established modern diplomacy and codified the role of ambassadors. States can and from time to time do violate these norms, as the recent examples of the 1979 Iranian hostage crisis and the 1984 murder of PC Yvonne Fletcher demonstrate. But states cannot violate these norms without cost to their legitimacy and authority. The isolation of Iran in the wake of the hostage crisis was amongst the factors that provided Iraqi leader Saddam Hussein with the opportunity to begin the Iran-Iraq war in 1980.

The precedents of terrorism, torture, chemical and biological warfare all suggest that a prohibition on the use of a tactic or weapon of warfare is achievable provided that the weapon in question is not very useful in practice.
Cyber-sabotage is such a weapon. Cyber-sabotage is inherently unattributable and unpredictable. A stockpile of cyber-weapons may be rendered obsolete with a single software update. Like biological warfare, the consequences of deploying a cyber-weapon can rebound on the attacker. Like terrorism, cyber-attacks permits warfare with plausible deniability and is thus inherently destabilizing and antithetical to world order.
Cyber-sabotage has no place in the arsenal of civilized nations. It is to the common interest but more importantly to the individual interest that we reject it. Put cyber-sabotage in the same box as torture, chemical warfare, biological warfare and terrorism, weapons and tactics that the leading nations have decided to prohibit because it is in our interest to do so.

About The Author:

Dr Hallam-Baker is an internationally recognized computer security specialist and is credited with 'significant contributions' to the design of HTTP 1.0, the core protocol of the World Wide Web.

His first book 'dotCrime Manifesto: How to Stop Internet Crime' sets out the first technical blueprint for how to make the Web and the Internet a less crime permissive environment by introducing accountability controls for transactions that require them.

Hallam-Baker currently divides his time between private consulting work and a part time position as Chief Scientist of Default Deny Security Inc.

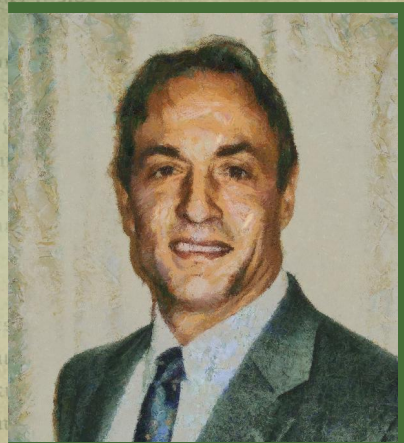
During twelve years as Principal Scientist at VeriSign Inc., Hallam-Baker made significant contributions to core Internet security protocols, including XKMS, SAML, WS-Security, WS-Trust and is currently co-chair of the KEYPROV working group. He has participated in standards groups in IETF, W3C and OASIS and played a key role in establishing the concept of Extended Validation certificates as an Industry standard.

A noted public speaker, he has addressed hundreds of audiences, including delivering the conference keynote address at Comdex Brazil and chairing a conference on Electronic Cash in Amsterdam.

UNCLASSIFIED

Counterpoint by US ARMY OFFICER

Colonel Michael Lacey



LEGAL DISCLAIMER:

The views expressed in the following article are those of the author alone and in no way represent the position of the US Army, Office of the Director of National Intelligence or the US government.

Digital Dresdin?

The similarities between pre-World War II airpower and the cyber weapons of today are startling and worth study. Before the Second World War, airpower represented a vast, untapped, destructive resource without any law of war regulation. In addition, its proper application and use was misunderstood by not only the theorist, but by most military establishments. Some war theorists saw it as an unstoppable, omnipotent, doomsday type weapon. Others saw it as just another weapon, like the machine-gun or the tank. Cyber weapons face the exact same challenges in their potential for use in the next conflict.

The Importance of Cyber WEAPONS IN OUR

next conflict cannot be overstated. The reported recent use of such a weapon by the United States against Iran's Uranium enrichment process clearly demonstrates that they are a technology and a tactic that is here to stay. However, much like airpower before the Second World War, cyber weapons and their attacks are without specific treaty regulation and represent an area under the law of war ripe for misuse and misapplication with tragic effects. This stems because of an almost complete lack of understanding of cyber weapons second and third order effects, as well as the overall lack of legal constraints or restrictions upon their use.

It was only in the Second World War that the awesome destructive power of airpower was recognized by military professionals. During the First World War, aircraft were primarily used for reconnaissance and gaining limited air supremacy. Although there were some nascent bombings by German blimps of London and by Allied aircraft of the Ruhr, negligible damage resulted.

Airpower was fundamentally flawed by two constraints in the First World War - technology and the inability of senior commanders and national governments to understand its role and potential in the conflict. Bi-planes made of fabric and wood, with speeds of under 200 miles-per-hour and limited range and payload were the standard. Also very few senior commanders had any experience with the implementation of this new weapon. Field commanders were limited by their previous experiences, none of which included the use of airpower in planning or execution of military operations.

There were various attempts to regulate airpower between the wars. These failed, however, because nations did not understand the awesome, destructive power the new technology would bring to the battlefield. The Hague Air Rules of 1923 represent the best known attempt to impose operational constraints on air power. Article 22 of the rules stated "any air bombardment for the purpose of terrorizing the civil population or destroying or damaging private property without military character or injuring of non-combatants is forbidden." Unfortunately, these rules were never adopted by any of the major powers and as a result the dogs of war would be fully unleashed during the next conflict - resulting in the German destruction of Warsaw and Rotterdam, their blitz on London and the Allied firebombing of Hamburg, Dresden, Tokyo and others.

War theorist also missed the mark on how air power would be employed during the next conflict. At one end of the spectrum was Guilo Douhet's influential book - Command of the Air. The book portrayed airpower, particularly the bomber, as the end- all-be-all for the next conflict. Douhet forecast that vast fleets of bombers would so destroy the opposition's national will by leveling their cities that conventional armed forces would not be necessary.

At the other end of the spectrum were war theorists and national policy makers whose shortsightedness on the potential of airpower led them to discount its use in the next conflict. Their desire to fight the next war with the weapons that lost the last was best represented by their opposition to early profits of air power. American Brigadier General William "Billy" Mitchell was a loud proponent for the independence of airpower during the interwar years. As a result of his vehement candor and passion he was court-martialed in 1925 and demoted to Colonel.

ANOTHER UNABLE TO SEE THIS NEW WEAPON'S

utility or destructive power was Secretary of the Navy Joesphus Daniels. Before Billy Mitchell's proposed bombing test on the obsolete battleship Iowa Daniels stated, "I'm so confident that neither the Army nor Navy aviators can hit the Iowa when she is under way that I would be perfectly willing to be on board her when they bomb her."

The actual results produced by airpower during World War II showed both camps were wrong. Airpower proved that while it was a crucial component to victory, it alone could not bring an enemy to his knees. The failure of the German "blitz" on London and the Allies attacks on German and Japanese cities demonstrate that the breaking of national will was a fleeting objective. Indeed in the pursuit of such a campaign, both sides inflicted unspeakable destruction resulting in hundreds of thousands of civilian casualties. Although airpower may have failed on the strategic level, it was an absolutely crucial component to any successful land attack during the war.

As a result of the terrible destruction and caused by the bombings of civilian targets in World War II, an authoritative set of rules were adopted by nations under the law of war. The Geneva Conventions of 1949 and their subsequent Protocols in 1977 both offer comprehensive restrictions on how the civilian populace and their infrastructure must be considered and avoided in any military attack. As a result of the world's military establishments adhering to these international legal standards, civilian casualties and collateral damage are at an all time low. Indeed, any civilian casualties attributed to airpower are now front page news and are to be avoided at all costs by the belligerents.

Today cyber weapons stand at the same threshold as airpower in the interwar years with regard to not only its importance, but in its almost total lack of regulation. It will clearly be a powerful, perhaps decisive component in the next conflict. Recognizing its importance, the national command structure has stood up a new headquarters - Cyber Command - to deal with the myriad of issues presented by the new weapons. Our rivals and emerging peer competitors such as China, North Korea, Iran, and Russia, have all invested huge amounts of resources in cyber weapons, technology and computer network defense. Finally, it has been used with great success in recent major powers forays against their weaker opponents such as Russia against Estonia in 2007 and Georgia in 2008 or the alleged recent United States intervention against Iran.

But also like airpower during the interwar years, there is no clear consensus on just how dominate the cyber domain will be in the next conflict. Like Douhet, there are the doomsday profits that predict that the cyber weapons will prove to be decisive and render all other weapons obsolete. Richard Clarke and Robert Knake argue that a successful cyber attack on the United States in the next conflict could result in complete economic collapse with electrical systems failing, commerce and communication infrastructure grinding to a halt and a possible collapse of civilization or government.

However, much like the U.S. military establishment response to Billy Mitchell's predictions in the 1920s, our DoD response to the cyber threat has been lacking. Admiral Mike McConnell, former Director of the National Intelligence Office (ODNI), predicted that the coming cyber attack could well result in a banking collapse or a shutdown of the electrical grid. causing irreversible damage. He stated that until such a disaster happens, there is no political or national will to make the much needed changes to how we view cyber war. In testimony in front of

"...CYBER WEAPONS OPERATE IN A VACUUM OF INTERNATIONAL LAW AND REGULATION..."

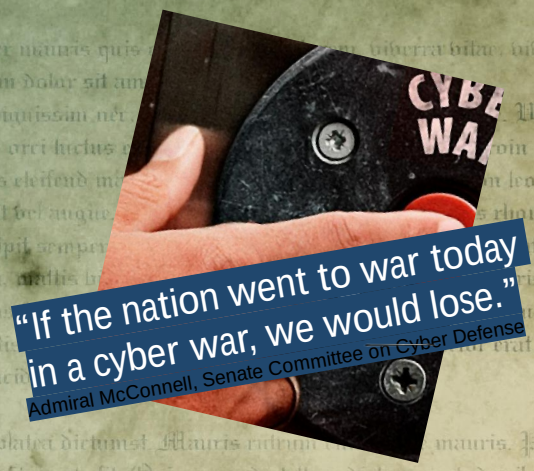
a Senate Committee recently, Admiral McConnell stated, "If the nation went to war today in a cyber war, we would lose." Similarly, James Clapper, the current head of the ODNI, testified to a congressional panel that the U.S. is on the verge of losing the coming cyber war without serious changes and it is the nation's most important security concern.

Also like airpower before the Second World War, cyber weapons are currently operating in a vacuum of international law and regulation. While there have been some small success in regulating transnational internet crime, to date there are no specific treaties dealing with the use of cyber weapons in the jus ad bellum or jus en bellum realms.

Obviously the Geneva Conventions of 1949 and subsequent law of war treaties are in effect and applicable, but these treaties were developed before the advent of the cyber world and mostly in response to the indiscriminate and deadly air attacks of the Second World War. Such treaties are ill-equipped to address the unique abilities and effects that characterize a cyber attack. For example, during international armed conflict should it be lawful for your opponent to use a cyber attack to shut down the electric grid which serves the Pentagon but also controls all traffic lights in Washington DC as well as the air traffic control systems for local airports?

When a the law of war fails to address a new weapons system or attack method the belligerents are left to their own devices to determine its legality - often with unfortunate results. Poison gas was not regulated by any convention before the First World War with tragic results.

The Geneva Conventions of 1929 failed to impose restrictions on airpower - the new destructive weapon standing in the wings and the major belligerents could not come to agreement with regard to the 1923 Hague Air Rules. Without black and white



rules on the legal scope of this new weapon, Hitler was free to reduce both Warsaw and Rotterdam to rubble in the name of military exigency.

Airpower entered the Second World War an unregulated and much misunderstood component of military might. The subsequent unforeseen destruction it wrought resulted in international treaties and state policies that severely limited its use - resulting in relatively few civilian casualties and collateral damage in subsequent conflicts.

Cyber weapons today stand in the same stead. While one can call for its regulation by a "Geneva Convention like" regime, it is an unrealistic scenario. The international treaty process is painfully slow and bogged down by state self-interest and mutual suspicion. Only another international conflict with horrendous civilian casualties or suffering (as predicted by Admiral McConnell), will summon enough state will to enter into such pacts of mutual sacrifice for the common good of the international community.

The inability to predict the 2nd and 3rd order effects of attacks is yet another similarity between cyber weapons attacks and strategic airpower. Air theorist ended up making faulty predictions concerning the ability of airpower to reduce civilian morale. Indeed in some cases it actually strengthened the civilian's populace will to resist such as in the German blitz on London.

"An attack targeting the command and control communications hub of the enemy could easily bleed over into the shared civilian infrastructure paralyzing civilian air traffic control, emergency response and perhaps even shut down the government's ability to communicate its intention to negotiate or surrender."

With cyber attacks, the 2nd and 3rd order effects are also almost impossible to predict. While the intended target for a cyber attack could be an opponent's national banking electronic network, it could well end up disabling the entire international banking system. An attack targeting the command and control communications hub of the enemy could easily bleed over into the shared civilian infrastructure paralyzing civilian air traffic control, emergency response and perhaps even shut down the government's ability to communicate its intention to negotiate or surrender.

State practice stands as the only possible timely and realistic control over these cyber war "Enola Gays" and "Little Boys." The United States has the unique opportunity and responsibility to impose the most restrictive interpretations on such law of war terms as "military objective, proportionality, civilian, and indiscriminate" that are found in the post World War II law of war treaties regarding the use of force. Although these terms were originally intended to regulate and restrict air and land power, they represent the only realistic legal template for the U.S. policy makers to impose upon themselves to set the example for the international community on the potential use of such cyber weapons.

In the absence of clear legal parameters or prior examples of disastrous use causing excess collateral damage, state practitioners will be tempted to push the cyber attack frontier to the very edge. The desire to utilize cyber attacks has already surfaced in such small forays as Russia's attack against Estonia or the United State's alleged intrusion into the Iranian nuclear program.

But much like the Luftwaffe's attack upon the city of Guernica during the Spanish Civil War, such cyber attacks only hint at the devastation to come unless definitive state practice involving restraint evolves to govern the use of these weapons.

ABOUT THE AUTHOR

Colonel Michael Lacey is currently serving a US Army War College Fellowship with duty at the Office of the General Counsel at the Office of National Intelligence in Washington DC. He was commissioned in the infantry in 1987 after graduating from the United States Military Academy. After completion of law school at the University of Illinois in 1994, he became a member of the Judge Advocate General's Corps, specializing in the area of International and Operational Law. His assignments have included deployments to Iraq in 2004-2005 and Afghanistan, where he served as LEGAD (Legal Advisor) for NATO's Regional Command South based at Kandahar in 2010-2011. Colonel Lacey has served both as a Professor and Chair of the Department of International and Operational Law at the Judge Advocate General's School in Charlottesville Virginia. He has published numerous articles on such topics as the law of war, the military commissions, military history and was the editor of the Army's premier deployed law resource - the Operational Law Handbook in 1999 and 2000. His decorations include the Bronze Star, the Purple Heart and the Meritorious Service Medal.

RED OCTOBER, RBN AND TOO MANY QUESTIONS STILL UNRESOLVED

The recently discovered cyber espionage campaign "Red October" has shocked world wide security community, the principal questions raised are:

Who is behind the attacks? by Pierluigi Paganini

How is possible that for so long time the campaign went undetected?

Which is the role of AV company in these operations?

To try to understand who is behind the attacks it is necessary to evaluate the way the hackers have operated, they used old Java exploits to infect system from various sectors, in particular government agencies and diplomatic offices.

According the first revelations of Kaspersky team the hackers could have a Russian origin, but they adopted exploits common in Chinese cyber espionage campaign, be aware this not means that Chinese government is involved.

One of exploits for the Microsoft Word documents had been used in previous spear-phishing campaign aimed at Tibetan activists according to Kaspersky experts, the hackers behind the Red October operation have just changed the executable that was embedded in the document. Symantec experts declared:

"This is not the first time that a high-profile attack campaign has used spear phishing emails and, as a popular method, it likely will not be the last . However, we are now seeing increased adoption of watering hole attacks being used in campaigns (compromising certain websites likely to be visited by the target organization)."

Kaspersky researchers verified two exploits for Microsoft Word flaws (CVE-2010-3333 and CVE-2012-0158) flaws and one exploit for an Excel vulnerability (CVE-2009-3129), all patched prior to attacks between May 2010 and December 2012.

THE MALWARE IS WITHOUT DOUBT THE WORK OF PROFESSIONALS THAT HAVE TARGETED VARIOUS PLATFORMS AND VENDORS IN MANY COUNTRIES MAINLY LOCALIZED IN EASTERN EUROPE.

Red October's primary attack methods relied on exploits for flaws in Microsoft documents typically sent via email, one tested scheme. What is sure is that the attackers have evolved their methods of attack over the time using every time new exploit to target also vulnerabilities recently found such as the Java (CVE-2011-3544) flaw, patched by Oracle in October 2011.

The circumstance that is concerning is that none of the exploits used for the Red October attacks were zero days vulnerabilities. Kaspersky researchers identified that at least three different known vulnerabilities have been exploited:

- CVE-2009-3129 (MS Excel) [attacks dated 2010 and 2011]
- CVE-2010-3333 (MS Word) [attacks conducted in the summer of 2012]
- CVE-2012-0158 (MS Word) [attacks conducted in the summer of 2012]

The security researchers from Seculert have discovered the usage of another delivery vector in the Red October attacks that allows the attackers to infiltrated victim network(s) via Java exploitation –' NewsFinder.jar'), known as the 'Rhino' exploit.

> *"The Red October attacks are interesting because of the large scale of the espionage done by a single entity, and the long time span they cover."*

Another interesting data provided by the investigation is that oldest domain name used in the Red October network was registered in November, 2007, and the newest in May, 2012.
In January 16th Kaspersky team published a new post on the investigation "Red October – Java Exploit Delivery Vector Analysis" in which is revealed that the early February 2012 timeframe that hackers would have used 'Rhino' exploit. It seems that this vector was not heavily used by the attackers, in fact when the security experts downloaded the php used to serve the '.jar' malcode archive, the line of code delivering the java exploit was commented out.
It becomes clear the importance of the discovery, probably this is one of the most extended cyber espionage campaign, what is singular, as observed by Kaspersky in its last post, is that it hasn't detected any PDF exploits yet, which common for this kind of operations.
Costin Raiu, director of Kaspersky's global research and analysis team, declared that other methods of distributing the cyberespionage malware might have been used although they are not yet identified.
Jeffrey Carr, founder and CEO of Taia Global, Inc, published an excellent post on his blog making interesting observations on the event.

Malicious servers
178.63.208.49 matches to 178.63.
188.40.19.247 matches to 188.40.
78.46.173.15 matches to 78.46.
88.198.30.44 matches to 88.198.

Mini-motherships
91.226.31.40 matches to 91.226.

I agree with Carr when he assumed a collaboration of RBN with Russian government, probably the RBN never stopped its action but simply operated below the radar.
Russia has always been known for its skill in virus design, just to provide some samples Bagel, Netsky and MyDoom. RBN in considered a cybercrime company able to provide any kind of malicious service such as phishing, DDoS, malware hosting, gambling and child pornography.I agree with Carr when he assumes that Kaspersky is one of the most important discoveries of the decade. To the RBN are recognized multiple skills:

- Network skills
- System skills
- Internet understanding
- Cybercrime relations
- Legitimate companies relations
- Law enforcement corruption

that make the organization very dangerous. Many exponents of worldwide security community believe that Red October campaign is the work of a group of cyber criminals that are collecting high-value information to sell subsequently to interested parties. Of course governments and intelligence agencies could be most interested in the information stolen.

In the post "Every Month is Red October" probably is provided the answer to the second question, the article in fact reiterates that security firms "see thousands of similar documents in our systems every month. The Red October attacks are interesting because of the large scale of the espionage done by a single entity, and the long time span they cover. However, the sad truth is that companies and governments are constantly under similar attacks from many different sources. In that sense, this really is just everyday life on the Internet."

It 's really impossible to avoid similar incidents despite the fact that AV systems installed are update?

Referring to the third question that is impossible to answer without proof … is it possible that some government had done pressure on AV manufacturers in exchange for "favors" to make sure that some threats do their course?
Despite this theory could appear extremely imaginative it is shared by many conspirationists and for this reason we could ignore it…often the reality surpasses the imagination.

About The Author

Pierluigi Paganini is the Editor-in-Chief of Cyber Defense Magazine, a Chief Information Security Officer, Security Evangelist, Security Analyst and Freelance Writer. He is a security expert with over 20 years experience in the field. Certified Ethical Hacker at EC Council in London. He has a passion for writing and a strong belief that security is founded on sharing and awareness led him to found the security blog "Security Affairs", which can be found at http://securityaffairs.co/wordpress. Today, he is the Director of Operations for Bit4id company, a leader in identity management, and he freelances as a writer with some major publications in the field such as Cyber Defense Magazine, Infosec Institute, Cyber War Zone, Infosec Island and The Hacker News.
Pierluigi is also the author of the books: *The Deep Dark Web Book* and *Digital Virtual Currency and Bitcoin.*

HOW DO NEXT GENERATION INFOSEC PRODUCTS AND SERVICES "CROSS THE CHASM" AND REACH MORE CUSTOMERS? AND WHAT'S WRONG WITH TRADITIONAL DISTRIBUTION CHANNELS?

By Allan Cowen, Managing Director, Solantus, Inc.

"Is your internal network truly safer by running bigger brand name company INFOSEC products and services? Actually not."

Never Heard of Them, So Why Risk IT?

IBefore getting involved with Cyber Defense Magazine, I never heard of Comodo, Bullguard or Emsisoft as up and coming Anti-virus companies and only heard of F-Secure once or twice. My research shows that they have not only received awards from CDTL but other test labs as well, yet when you talk with the typical CIO or IT security staff, they usually go glassy eyed on you when you don't drop names like IBM, Cisco, Juniper, Symantec and McAfee.

You know the expression "I never get fired for buying from IBM or Cisco or Symantec...etc." I think that will become an expression of the past when it comes to next generation and innovative network security solutions.
There are key drivers to why it's becoming more important to consider visionary products and INFOSEC innovators over the big names. Usually you'll hear from a CIO or IT security pro that: "IBM, Cisco and Symantec are big, doing well and will never go out of business. If I buy from a smaller player, I might have to vet them even more - their company size, financials, product roadmap, etc. I'd rather just buy big because my investment is safe" But is it really?

What happens when you invest in a TARGET - yes these guys are big but they have become the top targets for exploitation. Their hardware and software are more prone to be exploited. There are more vulnerabilities (visit http://nvd.nist.gov and search out any of them and you'll see), more patches, more management, more complexity and therefore MORE RISK when it comes to actually securing your network.

Yes, they may be in business for years to come but so will these smaller less profiled vendors who actually make much more innovative and proven security products - remember the Rocky movie series...he was a hungry fighter and he stayed in the game when everyone said he wouldn't go the distance - he was a nobody but he had the 'eye of the tiger' and he made it to become a champion. That's what I see in these smaller yet emerging vendors. They are hungry and thus work harder. They out-think and out-move the big, slow corporate behemoths. They are more flexible and creative in putting forth proposals to meet today's budgetary pressures that face most organizations. They listen to customers and respond to specific needs and requirements better. They are BY FAR, a better buy and offer the best return on investment. They have proven their place and presence within the specific market they address.

We have to start spreading the word and help them gain market share in order to "cross the chasm". I believe the so called Value Added Distributor (VAD), Value Added Reseller (VAR) and the Direct Market Reseller (DMR) operate under out dated business practices as they take products and services to market. These folks aren't adding much value anymore (Did they ever?) other than acting as box pushers, fulfillment agencies and promotion parakeets. They would rather keep it simple and

"Here in the back corners of the RSA Conference Expo, you'll find the real Magical Quadrant of INFOSEC innovation and you shouldn't have to seek endlessly to find them."

Allan Cowen, Managing Director, Solantus, Inc.

"take orders" for high volume low margin big branded products than serve as vehicles to help facilitate the introduction of the technology innovator in order to drive market acceptance. While these margin cry babies continue their journey to the bottom many others are racing to the top as they realize the margin magic that comes with the emerging technology value proposition. It's time this industry gets shaken up and these innovators get a better chance.

Customers should think twice when buying the Big Brand Names because they are actually increasing their network security risk, training time, installation and support headaches, just for someone with a huge balance sheet. Think Linux vs. Windows.

Half the world is running linux and it has a ZERO balance sheet. Microsoft is doing extremely well but their Windows product continues to gain bloat, requiring more memory, weekly patches, bigger hard drives, faster processors and it's always in the news as a hacker haven. Those of us that embraced Linux realized that while it could 'go away', this open source was started by a much smaller group than Microsoft but gained worldwide support and praise for being small, solid, stable and innovative. Linux is here to stay.

Take this philosophy into the VAD, VAR and DMR channel and we might actually start to see some of these incredibly innovative and best of breed INFOSEC products and services becoming more mainstream. It's time we embraced innovation and change knowing that it ultimately will improve our INFOSEC posture, not weaken it because the smaller player is...well...smaller. Over the coming issues of Cyber Defense Magazine, I hope to share with you Industry insights and well formulated business practices that will help with product selection and perhaps initiate the process of building a better network of regional Channel Partners to take the innovative Technology Provider message to market.

I trust that you will become inspired to seek out and explore technology innovation to address the various security concerns and challenges that you are confronted with. An opportunity to establish new partnerships with those that are in positions of responsibility to insure the success of your IT initiatives. Remember, if you are an IT VAD or VAR, becoming dependent on the ongoing success of the larger players means you become a tiny pawn in their game of business chess - at some point you will be either kicked off the board or ignored. If you work with the smaller, more innovative next generation companies you'll be helping them improve the state of cyber security, while you make a healthier margin and are treated like a King or Queen on their chess board. Over time, they may grow big, but they'll never forget your hard work and passion at helping them cross the distribution chasm while improving the state of INFOSEC for your customer base.

Ultimately, we'll see our networks safer, at a lower Total Cost of Ownership (TCO) with a much more Rapid Return on Investment (ROI). It's time to shakeup distribution and help get these solutions to the marketplace en masse. If you are walking the show floor of RSA Conference 2013 after reading this, I'll bet in the smaller booths and the back corners of the Expo floor, you'll find those next generation innovators. It's time we move them to the front of the line and explore their possibilities first.

"Linux has a ZERO balance sheet, yet half the world is willing to risk running their critical infrastructure, ecommerce, cloud computing and so much more on this platform."

ABOUT THE AUTHOR:

Allan Cowen is an INFOSEC distribution expert with over 25 years of experience developing and putting into practice better go to market strategies for security and other technology innovators. He frequently speaks at various Distributor and Reseller conferences and events to drive End-User product awareness. He is the Managing Director of Solantus, Inc., a non-traditional distributor headquartered in Canada but offering product distribution services throughout North America and International markets. On a mission to build the "Channel of Competency" To learn more about Allan, visit him online at: www.solantus.com.

LOCKDOWN SCADA

by Peter H. Jenney
and Paul Paget

It’s time to get off our butts and lockdown SCADA.

State

Industrial Control System (ICS) cyber security is weak and exploitable and we need to get off our butts and get to work locking things down. It also may be the next best place for IT Security Professionals to apply their talents.

A couple of years ago nobody ever heard about ICS or SCADA but the STUXNET attack on the Iran's Natanz nuclear facility in 2010 changed all that, and the fact that it was a weaponized attack tool launched by you know who makes it all the more interesting that the first volley has been lobbed. The cyber security weakness problem has evolved with an increase in attack vectors and access to a variety of systems that include vulnerable device controllers, weak network configurations and exposed control software, specifically Supervisory Control and Data Acquisition aka SCADA. Each of these

LOCKDOWN SCADA

areas have unique vulnerabilities, some pathetic where a single ping on a controller port can crash the whole unit, and others more obscure such as zero days used by STUXNET to propagate across networks. In all cases there are huge numbers of vulnerabilities and there is contention in the technology management organization that makes it difficult to cleanly address the issues.

Before we move any further, let's look quickly at what ICS/SCADA is for context. ICS/SCADA is used to control most of the things we need to stay alive: Water, power, and critical manufacturing.

It includes electricity generation with coal, hydro, oil or nuclear plants; water purification and waste-water management; HVAC systems; production of food, products and chemicals; transportation systems and more. Consider what would happen if someone managed to knock out the power grid in a major metropolitan area for longer than the reserves for typical power outages.

1. No Heat or Air Conditioning
2. No Water - electric pumps move it around
3. No Sewerage - electric pumps move it around
4. No Elevators
5. No Money (ATMs)
6. No Trains
7. No Lights
8. No Cabs
9. No Gas
10. No Food
11. No Police or Fire Departments

This is a hack that you don't measure in the number of credit cards stolen or money. This hack you measure in terms of loss of life, environmental impact and cost of recovery. It would be devastating. Cyber security is so bad in ICS/SCADA that it wouldn't be hard to do.

OK, pop quiz: How many confirmed successful Cyber Attacks have there been against global critical infrastructure? Answer: Zero. There have been several accidents caused by software failures that could easily have been hacks, but they weren't. STUXNET was a failure also. It did manage to infiltrate and do a little damage, but it got caught and eradicated before it could complete its mission.

OK, pop quiz #2: How many confirmed successful Cyber Attacks against global critical infrastructure will it take for the industry to get moving a lightspeed to protect themselves? Answer: Probably One. Sad but true, but that's the way these things work and in this case it's kind of like Russian roulette.

Fugue

So what's the problem with ICS/SCADA networks and why are so worried about them? It has to do with growth management, money and the Internet.

LOCKDOWN SCADA

Process control networks are focused on creating products and services, keeping the lights on or other key things that make it possible to live in modern conditions. The process is the primary concern and all emphasis is placed on keeping the process going. IT Networks are focused on data and security is critical to protect it. IT managers spend a significant amount of time locking things down, managing users and modernizing equipment where possible. In an Industrial Control facility such as a power plant, both process control networks and IT networks exist and are supposed to be completely isolated from one another by an "Air Gap." They're not. Fixing the problem should be a simple matter of applying IT best practices and implementing security to protect the ICS side of the facility, but it's more complicated than that. Part of the problem is focus and personality. The IT network folks think the ICS network folks are knuckle draggers because they don't know the first thing about security and the ICS folks think the IT folks are clueless because they actually shut down devices to work on them and change them in ways that might break the process! The descriptions might be a little harsh but the contention is real. Looking at Table 1 we can see that they are in fact quite different and both teams have legitimate issues that guide their decisions. In fact those decisions make for some nearly insurmountable problems that give us a baseline for here we stand today with regard to cyber security in the ICS space.

Carrying this a little further we see that the ICS/SCADA network has many more problems to deal with than meets the eye. The process is king and nothing can stop it. A security tech was once told by an ICS Network manager when asked if the process could shut down for the day to upgrade a piece of equipment - "Dude, our maintenance window is 4 hours per year..." true story. You get the picture. It explains why when you look at an ICS network you'll usually find an old Windows XP SP1 machine doing something critical. They can't upgrade to SP2 because SP2 breaks all the process management software on the system because it defaults to shutting ports off rather than leaving them open. They can replace systems with new stuff, but they have to be sure the new hardware and software will work perfectly with the controllers they have installed.

Category	IT Implementation	ICS Implementation
Security Priorities	1) Confidentiality 2) Integrity 3) Availability	1) Availability 2) Integrity 3) Confidentiality
Performance Requirements	• Non-real time • Consistent response	• Real time • Response is time critical
Component Lifetime	3-5 Years	10 – 20 years

Table 1 - ICS vs. IT Priorities [1]

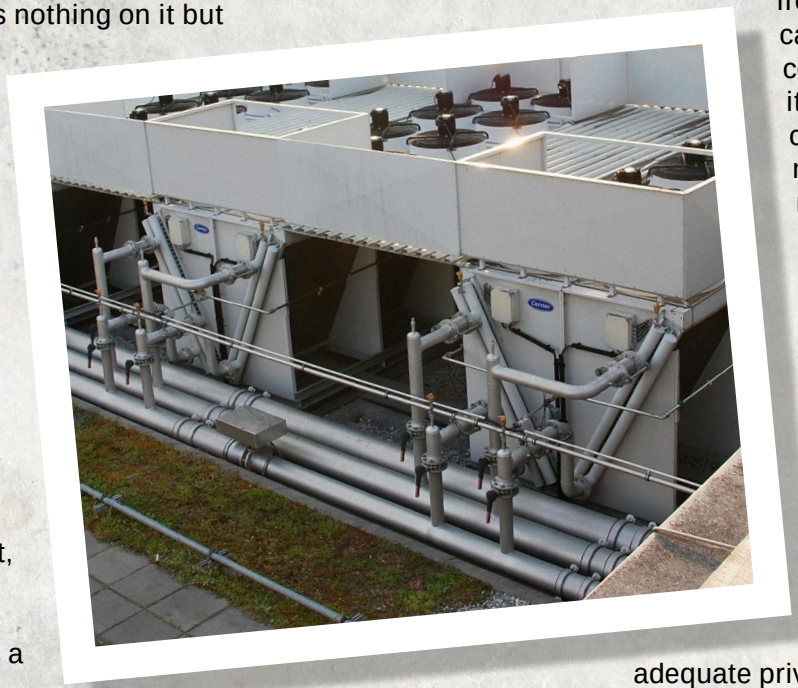
LOCKDOWN SCADA

Attack Vectors

Here are a couple of anecdotes to chew on before the serious stuff starts:

Scenario One - Returning from a business trip

An employee on the corporate side of an industrial company returns from a trip with a memory stick freebie. Once back from lunch the employee inserts the stick into their workstation and sees nothing on it but a gigabyte of free space- sweet! Behind the scenes what actually occurred was a clever piece of malware loaded itself onto the system, erased the memory stick behind it and started snooping around the network looking for SCADA Human Machine Interfaces (HMI) and Master Terminal Units (MTU). Once finding an appropriate system it installed itself as a root kit, making it invisible to normal operating system tools, and sets itself up as a man in the middle, intercepting all commands from the HMI software and replacing it with its own, and providing responses to the HMI software that makes it believe everything is normal. This network is compromised and completely open to the attacker! The protections normally in place, specifically Air Gap and anti-malware software should have protected the industrial control side, but it didn't. The air gap didn't really exist. The anti-virus software didn't catch the new, smart and polymorphic malware that was able to change the way it looks in memory, its signature, and slipping past to do its dirty work.



Scenario Two - Taking a shopping break

An operator sitting at the console running the Human Machine Interface (HMI) software on the SCADA network is a bit bored. The operator opens a browser and surfs out to a site that sells inexpensive knockoff shoes. There are banners and videos galore showing off the latest in faux fashion. A click to see the catalog opens a PDF version. Behind the scenes, the second that the Adobe Reader software loaded the PDF, code embedded in the PDF exploited the reader and loaded its own code onto the system and started to run. Seeing that the it was actually on an HMI it set itself up as a root kitted man in the middle and takes over the SCADA network. The anti-malware that was supposed to stop this from happening didn't catch it because the code rewrote itself as it was loading and came out looking like nothing that the anti-malware recognized, giving the virus free rein on the system. That malware not only controls the HMI it installed itself in, but also now has access to the internet to call out and freely download whatever it wants, such as a controller attack module, and it has adequate privileges, because its installed on a control system, to access and infect any other workstation or controller on the network.

"In a recent [2011] survey by the Ponemon Institute it was found that 96% of the organizations interviewed in the utilities and energy sectors believed both that SCADA security is their largest problem and that it is the hardest to address. Of those interviewed, 43% identified the largest security threats to their systems were "Negligent Users" and 40% identified "Insecure Web Applications."

"Mr. Sean McGurk, the Director of National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security put it best: "In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

Whose bright idea was this?

Why is this happening? Earlier the statement was made that unmanaged growth was a culprit, and to a great extent it is. ICS networks have grown through three SCADA generations, with each generation becoming cyber lamer.

Generation 1 - mainframe or minicomputer based. ICS processes were controlled by independent systems such as the IBM 360 or DEC PDP 11 with the remote terminal units (RTU) being hard wired into a single point. Access to the processes was (and in some cases is) via trusty 3270 or VT100 terminals and the systems are not networked or have any access to the Internet

Generation 2 - distributed control systems (DCS). ICS processes got their own proprietary control systems, sensors and other equipment and said control systems reside on a LAN to share information. Connectivity with the outside world was possible through modem pools but other than that the system was [is] tight

Generation 3 - networked systems. ICS processes have their own control stations built from cheap off the shelf parts that connect to controllers serially or using TCP/IP that carries the controller protocol as its payload. The network is attached to the Internet, there are wireless access points and poorly configured user accounts and other basic IT security flaws. SCADA components including Human Machine Interfaces (HMIS), Engineering Workstations and Data Historians are all mostly Windows PCs or Servers and have access to everything, and sometimes with the default password being, "password" and sometimes the system stops working if the default password is changed.

Attack Vectors

So, therein lays the problem. Organic growth in the transition from Gen2 to Gen3 SCADA opened attack vectors and made our critical infrastructure vulnerable to attack. Some quick examples of vectors that might be exploited are:

1. Old modem pools that are still connected and running, but forgotten
2. Antimalware Update ports
3. DMZ based help desks
4. Open wireless access points
5. Poorly implemented firewall rules
6. Weak Application Security

There are hundreds of similar examples and all can lead to disaster if exploited. Recall that measuring the cost of an cost of an IT attack. In the later, costs are measured in numbers of credit cards stolen or other personal information. In an attack on critical infrastructure cost is measured in loss of life, environmental impact and cost of recovery.

The Problem

Understanding the environment gives us a baseline from which we can describe the problem set and start applying fixes. There are several key areas where focus is required, but the big three are:

1. Perimeter defense - try and keep the bad guys out
2. Controller defense - deal with buggy, weak controller software and hardware
3. Application defense - deal with buggy software and old operating systems

Each of these areas is critical and each has several layers of other security that are required at the top level, user management and access control for example. So, the question is where do we start?

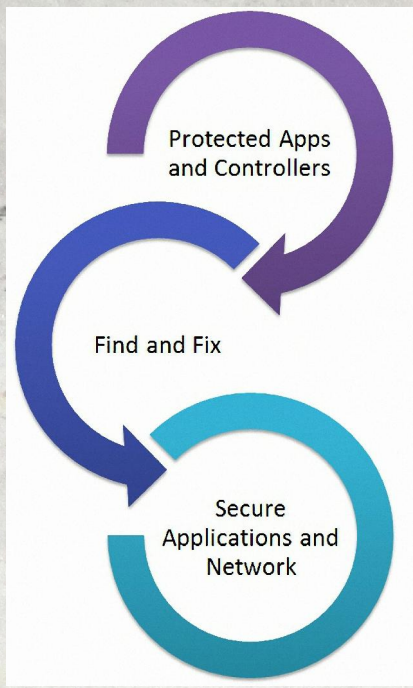
- Today perimeters are porous and locking them down without breaking anything is a huge task. Best to address it when there are cycles to do a complete analysis and design, with the analysis including finding and documenting all of the stuff that can be used to get on and off the Internet.

- Controllers can be pretty unstable, there are a lot of them and they may be from different vendors and use different operating systems. The matrix of things that need to be considered is too big to consider if time constrained.

- Applications can be pretty weak but unlike the other pieces, there are things that can be done to protect them and by doing so it's possible to protect anything downstream from them.

Starting at the application makes sense on several levels. First, it's the application that an attacker is going to go after in order to take over

networks, so protecting the application blocks that vector. Second, by closing this vector it protects anything connected downstream of it. Third, it's possible to lock things down without halting the process or breaking anything and finally, with the applications protected you've n got the time needed to deal with the perimeter and controllers directly.



Increased Protection and Lockdown

The best way to protect applications without disrupting things is to whitelist the system and ensure that only the things the process and operating system needs are allowed to run. Presumable the folks that manage the process controllers and SCADA systems will know exactly which programs need to run and if they don't, a call to the software vendor will get the answers quickly enough. The process of whitelisting is simple and depending on which technology you choose, it can be done quickly and invisibly. Once the process is complete, the system does not need to be messed with again as long as the whitelisting tool is not self contained, meaning that it has to reach out for updates like a blacklisting system. This brings us to the requirements for whitelisting in an ICS network.

1. The whitelist must be local and the system must not require any inbound traffic for updates or management
2. The system must only send data out asynchronously, no ACK packets or anything else that could identify the host as a target
3. The system must not force a reboot of the host
4. The system must not lock or break any files that the control software depends on
5. The system must not whitelist anything unknown or unneeded

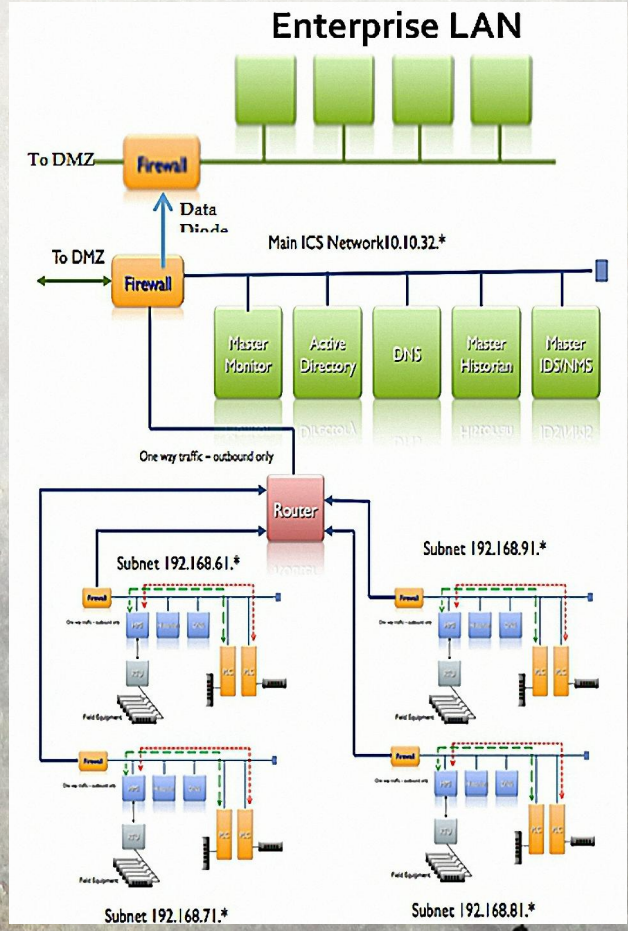
The first two items are to maintain the rules of the Air Gap, which only allows traffic to flow out of the ICS network for things like regulatory data/report feeds.

Under no circumstances should data be sent into the ICS network, and if by some chance it is, the control system must not acknowledge it or act on any commands that it receives. These last two items make the system act more like an individual firewall, and can be changed later when the "big" perimeter and controller changes are made.

So, the lockdown process is install, select and authorize programs, enable protection, move to the next host, rinse and repeat-keeping it up until all the systems are covered.

What Next?

With the applications appropriately protected, the real work begins on restructuring and replacing, but this can only happen because the systems are safe from outside attack.



The choices for moving forward are simple, direct and basic IT best practices:

1. On the Host
    a. Manage user authentication/authorization, eliminating unused or retired items
    b. Install or configure an individual firewall and block all incoming requests
    c. Force attestation of RTUs, PLCs, and other Intelligent Electronic Devices (IED)
    d. Enable stealth mode unless the controllers the host is managing requires ACK
    e. Turn off unused servers e.g. web, telnet, ftp, ssh, nntp, ...
2. On the Network
    a. Scan the entire network at all OSI levels from 2-7 and report.
    b. Generate an overall network diagram and interpose discovered items
    c. Execute a Mark I Eyeball scan of the network to confirm OSI discovered items and any that were hiding, and update diagram
    d. Discover cross network communications dependencies and mitigate
    e. Segment ICS/SCADA and IT networks and firewall (Data Diode)
    f. Segment individual process sub-networks and firewall
3. Develop software upgrade plan
    a. SCADA Components
    b. Maser Control Stations
    c. Operating Systems
    d. Controllers
4. Develop Hardware upgrade plan
    a. Controllers
    b. Hosts

The reconfiguration of the network will by no means be a quick process but it can be broken up into discrete tasks and implemented as time permits. As long as the hosts are whitelisted and protected from inbound traffic and insiders, the overall system will be safe and the worst-case scenarios may be avoided and the process can continue.

Recommendation

Staring from the bottom up, protect exposed systems with the whitelisting of applications. This can be accomplished in a simple manner with existing systems and without disruption. That should be the first priority. With an improved level of protection it is more rationale to then do the planning, re-architecting of the network, authentication of devices, upgrades and the investments necessary to get in a stronger and more secure posture. With a strong layer of protection in place, the longer term effort can be approached in a less frenetic manner. Not taking immediate steps is not an excuse.

References

1. Industrial control systems: UNIFIED APPROACH for improving cybersecurity - ICSJWG 13-Apr-2012
2. Source: The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing. 58:30 -- 59:00
3. Source: 2011 Ponemon Institute survey "State of IT Security: Study of Utilities and Energy Companies"

About The Authors

Peter H. Jenney and Paul Paget

Mr. Jenney is a 30-year veteran in the software development, testing and security space. Both a software developer and product manager, he has developed and managed software at leading edge companies including Dataware Technologies, where he invented CD-Record, the first commercial SCSI CD Recordable system and Rational Software where he drove Rational Testing products to over US$120M while managing technical relationships with Microsoft, IBM and others. In 2005 Mr. Jenney joined Security Innovation, Inc. as Vice President of Strategic Initiatives where he developed relationships and software in partnerships with global government and commercial organizations such as Cisco, Duma (China), CACI, USAF/AFIT, DOT, CERT, et al. Most recently, he entered into a new venture named Resilient Machines where as co-founder and CTO, he creates and deploys novel cyber-defense software specifically focused at Industrial Control Systems and SCADA.

Mr. Paget is a veteran of the information security industry, Paul is known for successfully leading new companies and bringing breakthrough technologies to market, including well known players such as Core Security Technologies, the leader in automated penetration testing and Cybertrust, a leader in identity management. Currently he is CEO of Savant Protection, an emerging leader in the application whitelisting space, focused on protecting sensitive and vulnerable critical infrastructure and organizations. Earlier in his career he held management and executive positions at IBM and Lotus Development.

Feel like a little fish in a big pond?

"When it comes to Internet Privacy, You are Not Alone" David Rosen

Digital First Aid

> “Everything about your digital life is being captured, stored and processed. Your keystrokes, your emails, searches, credit card transactions and bill payments, and your mobile movements through a GPS device are being tracked, captured and possibly reused.”

by David Rosen

Everything about your digital life is being captured, stored and processed. Your keystrokes, your emails, searches, credit card transactions and bill payments, and your mobile movements through a GPS device are being tracked, captured and possibly reused.

Big Government (e.g., federal and local agencies and law enforcement) and Big Business (e.g., telecoms, web sites, smartphone "apps" companies and private data aggregators) to collect tons of information about you that would have been inaccessible a decade ago.

We do not know the full extent to which fellow Americans are being monitored. Both government agencies and corporate entities remain extremely secretive as to the full extent of their data capture, tracking and surveillance activities (e.g., what is captured, how long its kept) as well as how they share the information gathered with each other and 3rd-parties.

But there are still things you can do!

The following four safeguards - a digital first aid kit -- help map out the ways ordinary Americans can resist the encroaching state-corporate information complex. It is not a comprehensive analysis of digital security possibilities, but rather an outline suggesting the scope of vulnerability and some things people can do to protect themselves.

The products mentioned are not being recommended but are suggested as examples of tools available that promote personal privacy.

4 Ways to Protect Yourself Against Tracking & Surveillance

#1 - Protect Your Digital Device

Three digital devices anchor most people's personal and social life -- the mobile communicator (including cellphone, smartphone and/or tablet), the computing device (including desktop, laptop and netbook) and the TV set(s). In addition, many people use a wireless router to link their mobile device or TV set via a wireline connection to the Internet.

Some laptop users often install a laptop lock on their device. Similar to a bike lock, a laptop lock protects the device if you're in coffeehouse and leave it to pick up an order or go to the bathroom. The Targus Defcon comes with a Kevlar reinforced stainless steel cable with a combination lock, a motion sensor and an alarm that can hit 95 decibels.

Once a computing device is up and running, one needs to insure it has strong password protection.

Passwords can be protected through encryption techniques and the most common is known as public-key encryption. It requires two separate "keys," one secret or private, the other public or shared. Encryption preserves the confidentiality of data being transmitted and allows the recipient to verify the identity of the sender.

The leading forms of encryption software are based on what is known as 128-bit or 256-bit ACE (Advanced Encryption Standard) encryption. There are a host of password encryption programs for different computing and communications devices. For example, commercial programs include Norton Identity Safe, 1Password and Password Safe; SafeNotes is for a wireless phone. KeePass and TrueCryp are open sources programs for passwords, bank codes, access codes and PIN numbers. MindWallet is a free program based on a military-grade, 128-bit AES algorithm. MindWallet is a free program based on a military-grade, 128-bit AES algorithm.

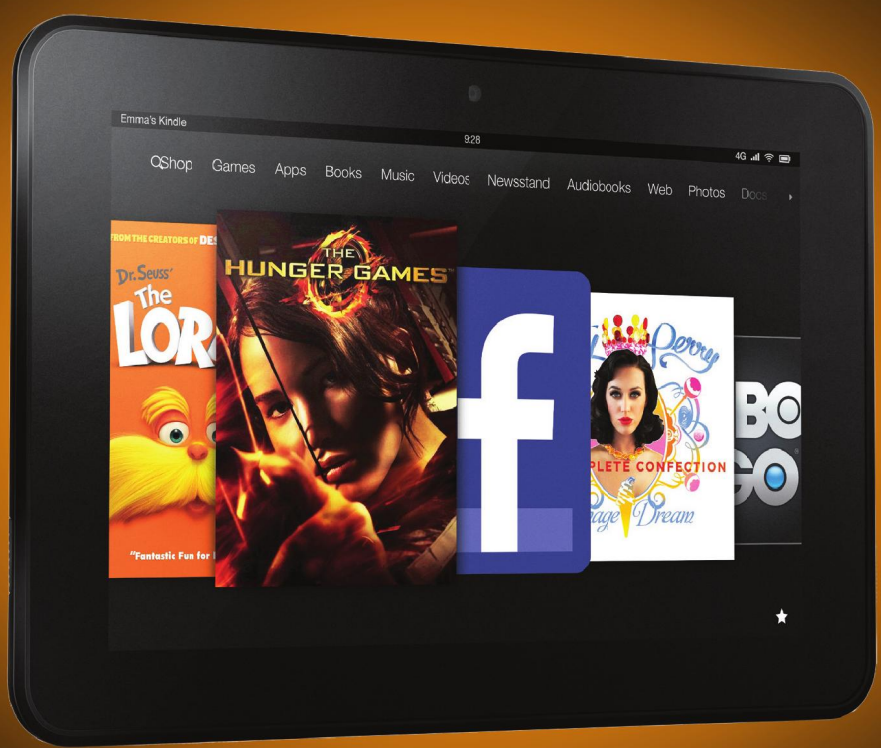
VENAFI

EKCM
ENTERPRISE KEY AND CERTIFICATE MANAGEMENT

Win 1 of 50 kindle fires HD 8.9"

Play EKCM Jeopardy at Booth #1655, and be the lucky winner of a Kindle Fire.

One winner every session, two sessions per hour.
Find out more about Venafi at RSA® Conference 2013.



Kindle fire HD 8.9" devices are available only to full-conference delegates.
You must have your badge scanned, and be present to win.
Qualified attendees are only eligible to win in the first Venafi session they attend with a scanned badge.

venafi.com/RSAC2013

Digital First Aid (cont')

"#2. Protect Your Wireless Router & Use a Firewall"

Most wireless routers come with a program that encrypts data as they are being transmitted through the air. The data can only be deciphered if the wireless router and the wireless device (e.g., the laptop) have the same password. The most common router encryption program is known as Wired Equivalent Privacy (WEP) and has three settings: Off (no security), 64-bit (weak security) and 128-bit (somewhat better security). While WEP is easy to configure, it is not difficult to crack.

Routers come with what is known as the service set identifier (SSID), which is a standard, default ID assigned by the manufacturer. Users should change the ID "name." In addition, users are also encouraged to change the router's default password. Both the ID and password should be 10 characters long using non-sequential letters and numbers.

Users should also considering installing a software or hardware firewall for added protection, a condom's condom. A firewall blocks certain kinds of network traffic, forming a barrier between one's computer and an untrusted network.

It helps protect one's computer from surreptitiously installed malware like viruses, worms, Trojan horses, spyware and spam.

McAfee, Norton and Symantec are among the companies offering firewall and anti-malware programs. Among open source providers are ModSecurity, WebKnight and Smoothwall.

Users should be wary about "free" anti-malware programs. Recently, a rogue anti-virus program called "Windows Malware Firewall" was distributed informing PC uses that malware has been detected on their machine.
For those who downloaded the phony program, it was a nightmare to delete.

Digital First Aid (cont')

“#3 - Protect Your Operating System (OS) & Browser”

Digital connectivity from a device to the Internet and web is facilitated through the device's OS and browser. An OS can be proprietary like Microsoft's Windows and Apple's Mac or open source like Google's Linux-based Android and Firefox's Mozilla. A couple of browsers dominate the market, including MS's Internet Explorer, Apple's Safari and Firefox's Mozilla. Similarly, mobile devices, especially 3G and 4G smartphones, are dominated by a handful of browsers like Apple's iOS (for iPhone and iPad), Google's Chrome and Microsoft's Windows Mobile.

Data tracking is facilitated through communications devices. Advertisers, identity thieves, data miners and spammers track through an online or mobile user's browser. The Federal Trade Commission (FTC) is seeking to establish a "Do Not Track" (DNT) procedure comparable to the "Do Not Call" program. The goal is to allow users to block data tracking.

Three of the larger browser providers, Firefox's Mozilla, Microsoft's Internet Explorer 10 and Google's Chrome (at year's end) will incorporate some form of DNT. In addition, commercial companies (e.g., TrackMeNot and AdBlock) offer what is known as blocklists that are add-ons to leading browsers that block tracking.

Tor seems to be the best browser available. It is a free, open-source program that protects data transport. The data is routed through the Tor network that includes a series of randomly selected relays (run by volunteers) before arriving at the end-user destination. The Tor system thus blocks a user's ISP (Internet Service Provider) and anyone monitoring the network from viewing the websites a user has accessed. In addition, it blocks the website (e.g., Google) from identifying an end-user's IP address and physical location. Even the relays don't know the users who transport data they are routing over the Internet. Finally, all traffic on the Tor network is encrypted.

Tor runs on Foxfire's Mozilla and can be incorporated into Windows, Mac, Android and Linus/Unix OSs. The Tor program can also be used with instant messaging, chat rooms, web forums, remote logins and other functions.

https://www.torproject.org/

Skype, the online phone and video service, was famous for protecting user's privacy. However, since being acquired by Microsoft, it has increasingly opened its doors to policing dictates. It now can access all of a user's information stored on its servers, including profile and credit-card details. According to the company, it keeps instant messages (IMs) "for a maximum of 30 days unless otherwise permitted or required by law. Voicemail messages are currently stored for a maximum of 60 days unless otherwise permitted or required by law."

Digital First Aid (cont')

"#4 - Protect Your Content

"Content is king … and users are becoming digital serfs."

IUsers need to keep in mind that every phone call, every online search, every keystroke, every credit card transaction, etc., etc., is being captured and stored. Equally critical, if a program (e.g., game) is offered free, you'll be robbed.

An online user's response to an advertisement is one of the principles ways people are tracked. Online advertisers, through the online Digital Advertising Alliance (DAA), offer a program to help users to manage tracking. Check out aboutads.info.

Many basic programming services, like email, text message or chat, come with built-in encryption programs or a user can download encryption software or client-server programs like S/MIME (for Secure/Multipurpose Internet Mail Extensions) and OpenPGP (for Pretty Good Privacy). In addition, there are a host of online email encryption programs like JumbleMe, Sendinc and Enlocked from 3rd-parties. The Hacker Daily's Encrypted Messages application is promoted as "the Swiss army knife of encrypted communications and encrypted local note files. Our free small compact app can keep your communications safe from prying eyes."

Be careful about Facebook, MySpace and other social media sites. Under the terms of service conditions of most social networking sites, the companies have free use of all the information or files published through their portal. In addition, Facebook tracks the web pages of each of its 800 million or so members who visited the site over the previous 90 days. It also tracks where millions of nonmembers go on the web when visiting a Facebook user's page.

For those really into protecting their data, you might want to backup your content on a small, external hard drive. One such device is the Rugged Safe that is, in principle, impossible to break into. It comes with a biometric, fingerprint authentication system; up to 10 fingerprints on some programs. It has built in 128-bit AES encryption, which further protects the stored files.

The Federal Trade Commission (FTC) is currently considering new regulations concerning online privacy.

One program involves what is known as Do Not Track function and is conceived to work like FTC's Do Not Call list. Some companies have embraced the program, including Microsoft, Google and Yahoo. If adopted as provisional planned, it will feature a do-not-track button embedded in most Web browsers.

http://www.ftc.gov/opa/reporter/privacy/donottrack.shtml

There are real problems with the Do Not Track program that the online ad industry is adoption. The Electronic Frontier Foundation's (EFF) warning needs to borne in mind: "… we've still got a long way to go. And, unfortunately, it looks like online advertisers are already working to water down the Do Not Track protections."

https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track

The other program involves revisions of the Children's Online Privacy Protection Act (COPPA). The law, originally adopted in 1998, requires websites aimed at kids to get parental consent before gathering information about those users who are under 13 years. Many companies, including a Disney subsidiary, have violated it. The FTC is moving to update COPPA.

About the Author

David Rosen is a Privacy Expert. He writes for CDM as well as the "Media Current" blog for Filmmaker and regularly contributes to AlterNet, CounterPunch, Huffington Post and the Brooklyn Rail. For more information, check out www.DavidRosenWrites.com. He can be reached at drosennyc@verizon.net.

Cyber Intelligence

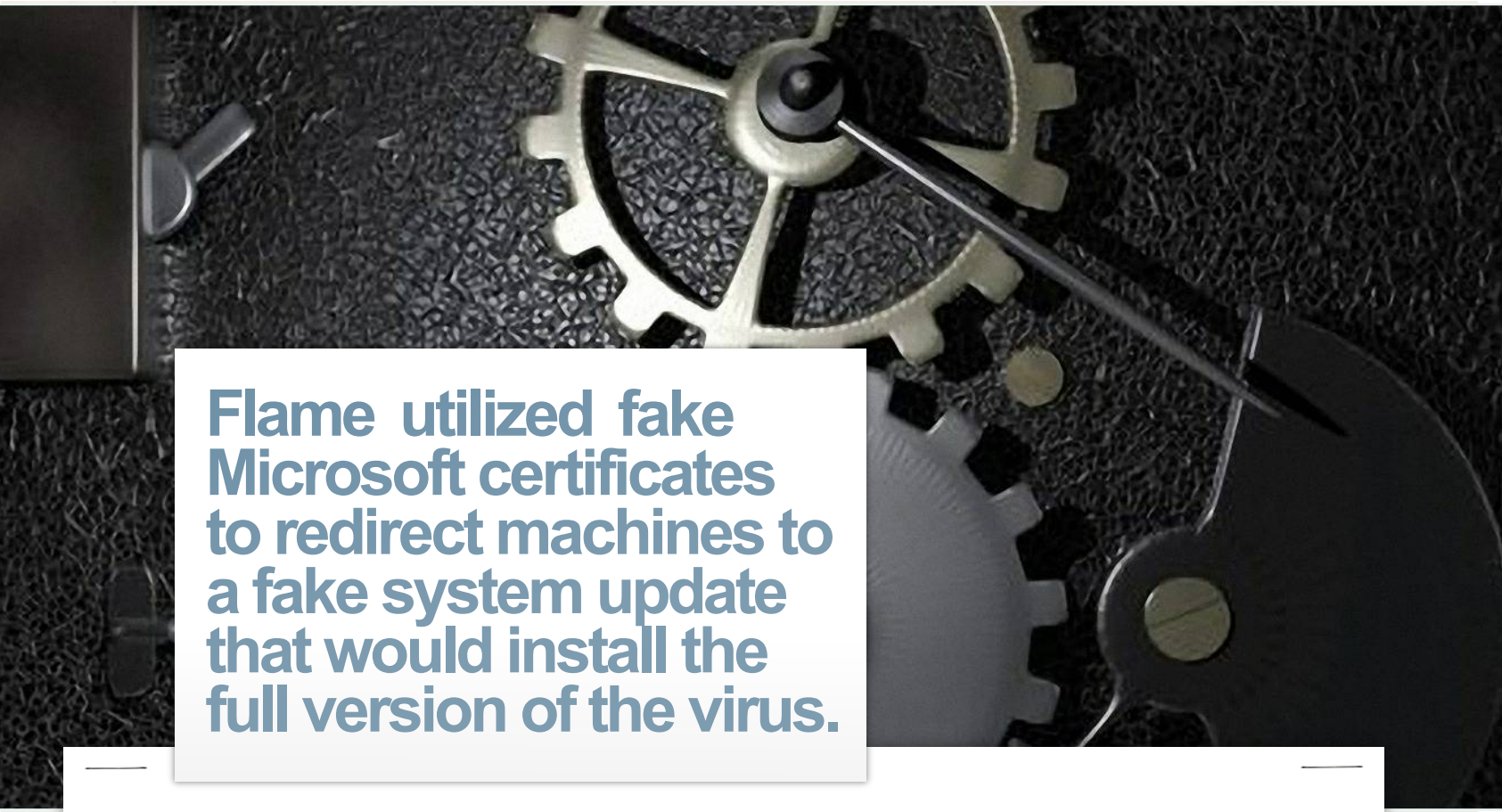
What is needed to execute the payload

by Jeff Bardin

We read in the papers the investigations around malware such as Stuxnet, Flame, Duqu and Mahdi. They are in the news daily with detailed code examples and methods of movement within the target information systems and devices. Anti-virus companies, managed security firms and cyber security consultancies all discuss the capabilities and functions of the malware of the day.

They discuss the technical acumen and unique capabilities of the code marveling at the comprehensive nature of the cyber weapon and the thoroughness of the developers. They and others release the code for open source reviews. They solve the issues with the malware releasing warnings, signatures and engine updates, and new detection and prevention methods all in the name of stopping the highly functional code. The focus is on the technology. The solution, always reported to be a technology. What really needs to be discussed though is the methods of intelligence collection, production, analysis and delivery that lead to such ingenious software to be developed and targeted. Because when you really look at the issue, Stuxnet, Duqu and Mahdi are in and of themselves, nothing more than the payload of the overall program.

Flame has been called a "sophisticated cyber-espionage toolkit." Flame had a command and control or c and c structure with more than 80 different domains. The c and c domains were registered as far back as 2008. With the majority of the domains being registered with GoDaddy. Five of the servers examined were running Ubuntu Linux and had ports 22, 443 and 8080 open. Flame utilized fake Microsoft



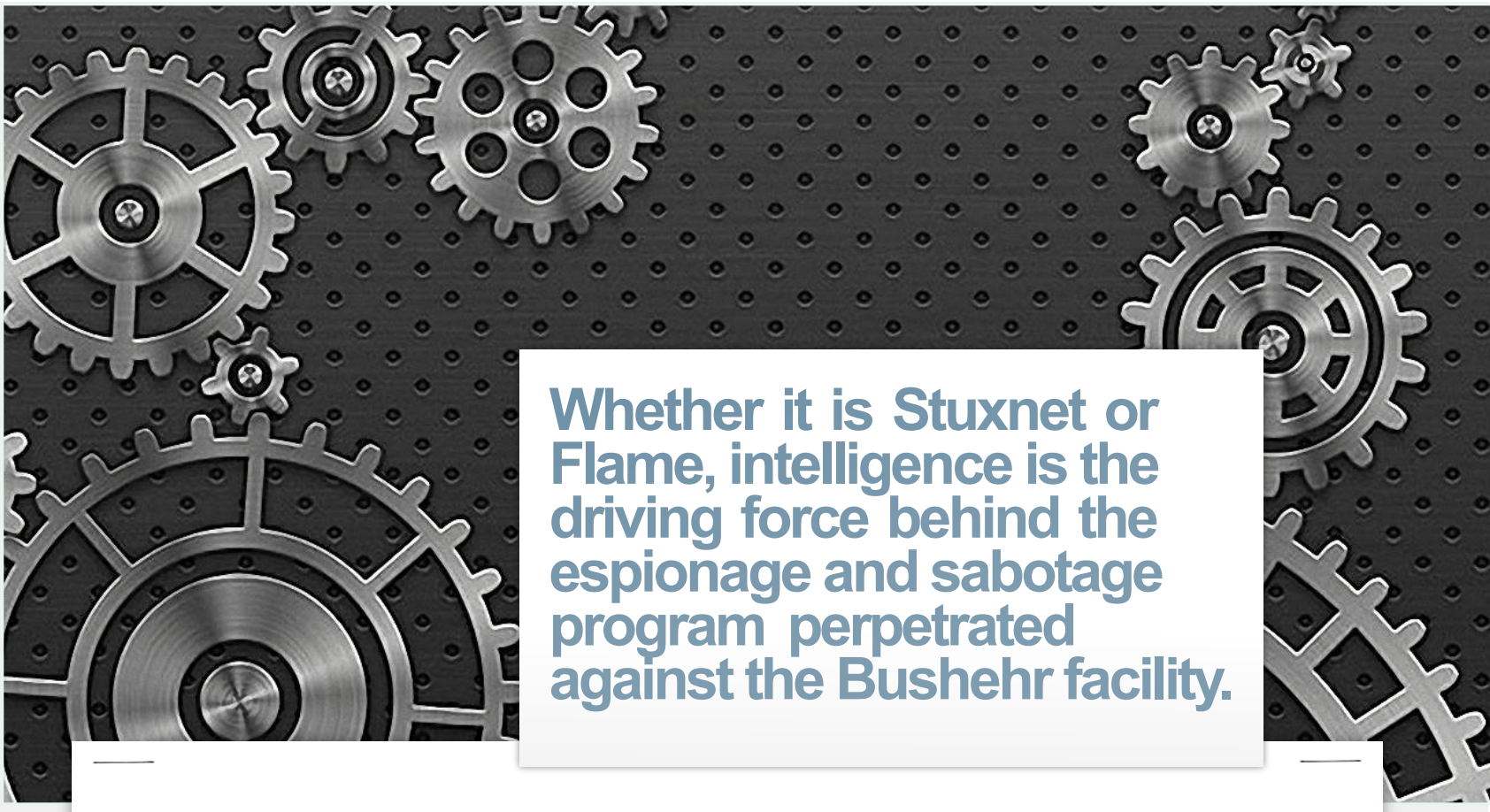
Flame utilized fake Microsoft certificates to redirect machines to a fake system update that would install the full version of the virus.

Cyber Intelligence - What is needed to execute the payload (cont')

certificates to redirect machines to a fake system update that would install the full version of the virus. Flame would initially infect a few devices. Once the information obtained was analyzed, Flame would remove itself from devices producing the least valuable information. Targeting would then move on to other devices identifying high value targets. Flame's self-removal and specific information targeting allowed it to go undetected. The c and c structure went offline after an anti-virus firm disclosed the existence of the malware.

Flames's main target was the Middle East. It is estimated there are 185 targets in Iran, 95 in Israel/Palestine, 32 in Sudan, 29 in Syria and 18 in Lebanon. The primary operating system infected was Windows 7 32 bit followed by Windows XP. It was determined that Flame did not run on Windows 7 64 bit. There were several versions of Flame. All the versions observed had the same password. Flame also functioned as a Bluetooth beacon using Bluetooth devices to collect information about discoverable devices. Flame can be related to other versions of malware, namely Stuxnet and Duqu, based on their structures and targets. The data Flame extracted included AutoCAD drawings, summaries of P D F and text files, emails, audio recordings and what was described as "interesting or high value" files. It is suggested that Flame's capture of audio came after other malware targeting email communications made officials conduct more face-to-face meetings to share information. Many of the infected devices were related to Iranian infrastructure, specifically energy. The information captured by Flame was specific and targeted. The significance of targeting AutoCAD files could indicate the intention to collect intelligence about facilities, engineering designs, level of nuclear development, infrastructure design and location of critical elements. Audio recordings could be used to identify persons involved with the planning, design, creation, implementation and maintenance of the facilities and critical elements. Essentially Flame collected information regarding Iran's nuclear capability better and more accurately than other means of intelligence gathering. Had Flame not been detected it would still be collecting and reporting intelligence back to command and control servers. Flame wasn't the first "tool" of its type and it certainly won't be the last.

Stuxnet was primarily a "sabotage" program, whereas Flame was primarily an "espionage" program used for targeting self-determination and collection. Flame can be seen as an extension of the cyber intelligence lifecycle able to determine targets based upon ontologies and machine code that provides a level of artificial intelligence required to seek out data points of value. It follows a strict targeting package determining value while sifting through files (much like the traditional sifting through the papers on someone's desk looking for specific information before moving on to the next drawer or cabinet in the room).



Whether it is Stuxnet or Flame, intelligence is the driving force behind the espionage and sabotage program perpetrated against the Bushehr facility.

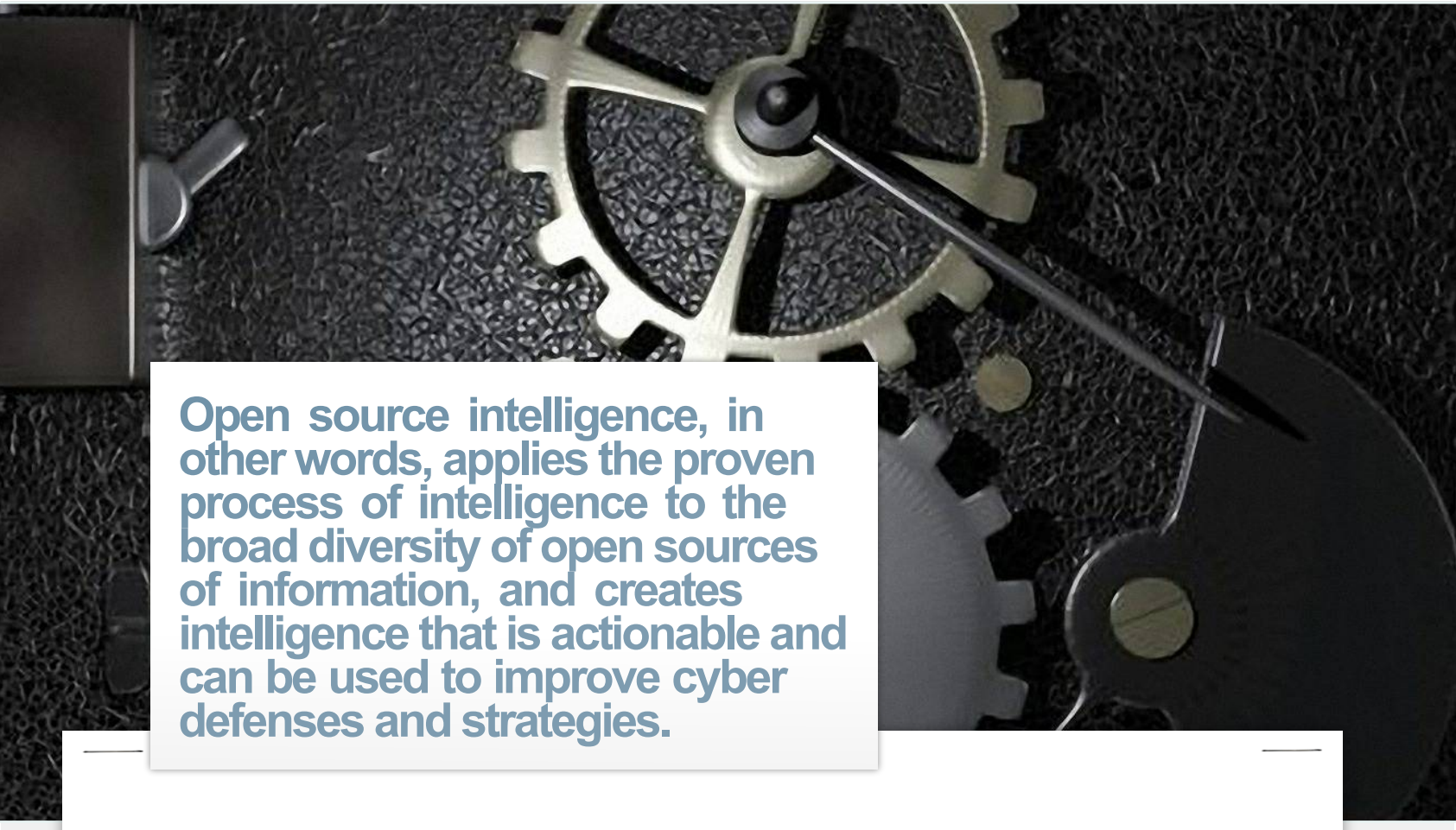
Cyber Intelligence - What is needed to execute the payload (cont')

Once value is determined, data is collected and transmitted back to C&C devices for production, analysis and recommendations and opportunities. These recommendations and opportunities could be additional payloads such as Stuxnet or even physical payloads. Regardless, Flame demonstrates a new level of thinking as in cyber intelligence as we move to the virtual manifestation of the physical tradecraft.

There are years of historical and technical data required to be mined and understood when it comes to Stuxnet. In order to understand what to target and where to direct the payload, the program the created the payload would have to study historical, cultural, technical, architectural, and electrical data points at the very least. Everything about the Bushehr nuclear facility would need to be known starting with its roots in 1974 and the underlying architecture begun by the German contractor Siemens.They would also need to understand the changes proposed in 1995 by Russia when they signed an agreement to provide support to complete the project. They would need to know the ins and outs of the Russian Atoms troi export company and the Leningrad Metallurgy Plant, both associated with providing support, manpower and technologies to complete the Bushehr plant.

We can continue this conversation but I believe you understand this would go one for days as we cover each and every aspect of everything associated with the Bushehr power plant. The idea here is to understand the depth and enormity of the effort required to execute a plan of the magnitude required to surgically create and place the Stuxnet payload. It is all based upon Intelligence. Whether it is Stuxnet or Flame, intelligence is the driving force behind the espionage and sabotage program perpetrated against the Bushehr facility. It is not different from physical activities experience during the Cold War when physical agents would infiltrate foreign countries, penetrate critical facilities subsequently stealing information and sabotaging the target facility or technology.What has changed is the methods of infiltration and penetration as well as the ability to sabotage without physical harm to humans. At least in this case.

Most organizations do not monitor their online postings with cyber OPSEC in mind. Online postings across multiple protocols and web functions might allow your adversaries an opportunity to interpret or piece together critical information. Adversaries use multiple and overlapping collection efforts targeted against all sources of your organizational and employee information. America's enemies scour blogs, forums, chat rooms and personal websites to piece together information that used to harm the government and commercial organizations. Learning about cyber intelligence, open source intelligence and cyber OPSEC effectively equips students with the tools to gather data points, transform these data points into actionable intelligence that prevents target attacks. Students of the craft



Open source intelligence, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence that is actionable and can be used to improve cyber defenses and strategies.

Cyber Intelligence - What is needed to execute the payload (cont')

learn of measures to identify, repel, or neutralize targeted intelligence gathering against organizational assets. Methods of prevention will help reduce your Internet, Web and Web 2 dot zero attack surface.

Open source intelligence is an untapped discipline that can be used to enhance operational security of your organizations online presence while preventing least path of resistance penetration into your organizational environments. In order to protect your online information and reputation, you first must understand the methods of targeting, data gathering and collection, data production, analysis and written delivery. This intense course covers all aspects of the cyber intelligence lifecycle focusing on the use of open source tools to gather readily available Internet and Web 2 dot zero data. The data points are then organized into a profile for analysis into actionable intelligence and used to reduce your attack surface and prevent additional data loss.

The focus is on relevant information that can be obtained legally and ethically from the public and private sector, and that is not classified in its origin or processing. The information may become classified in relation to the students organizational intent or its association with classified information when it is rightly blended into all-source intelligence reports.

Open Source Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual.

Open Source Information is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. Open Source Information is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the open source information world. Open Source Intelligence is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question, in this case organization online OPSEC. Open source intelligence, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence that is actionable and can be used to improve cyber defenses and strategies.

At the end of the course, students are armed with the knowledge and tools necessary to start a Cyber OPSEC program for their organizations. The adversary devotes significant resources to monitor your operations and activities on a daily basis. They can produce reliable information on your capabilities, intentions, and vulnerabilities. Adversaries are also shifting the emphasis in targeting. Foreign targeting of American technology is increasing for economic as well as military reasons. Technology transfer will continue to remain a major concern now and in the future. What you do about it can either make or break your current and future strategies.

Analysts understand the need for patience in executing cyber intelligence and cyber counterintelligence operations.

Cyber Intelligence - What is needed to execute the payload (cont')

Switching Gears - Cyber Counterintelligence (CCI)

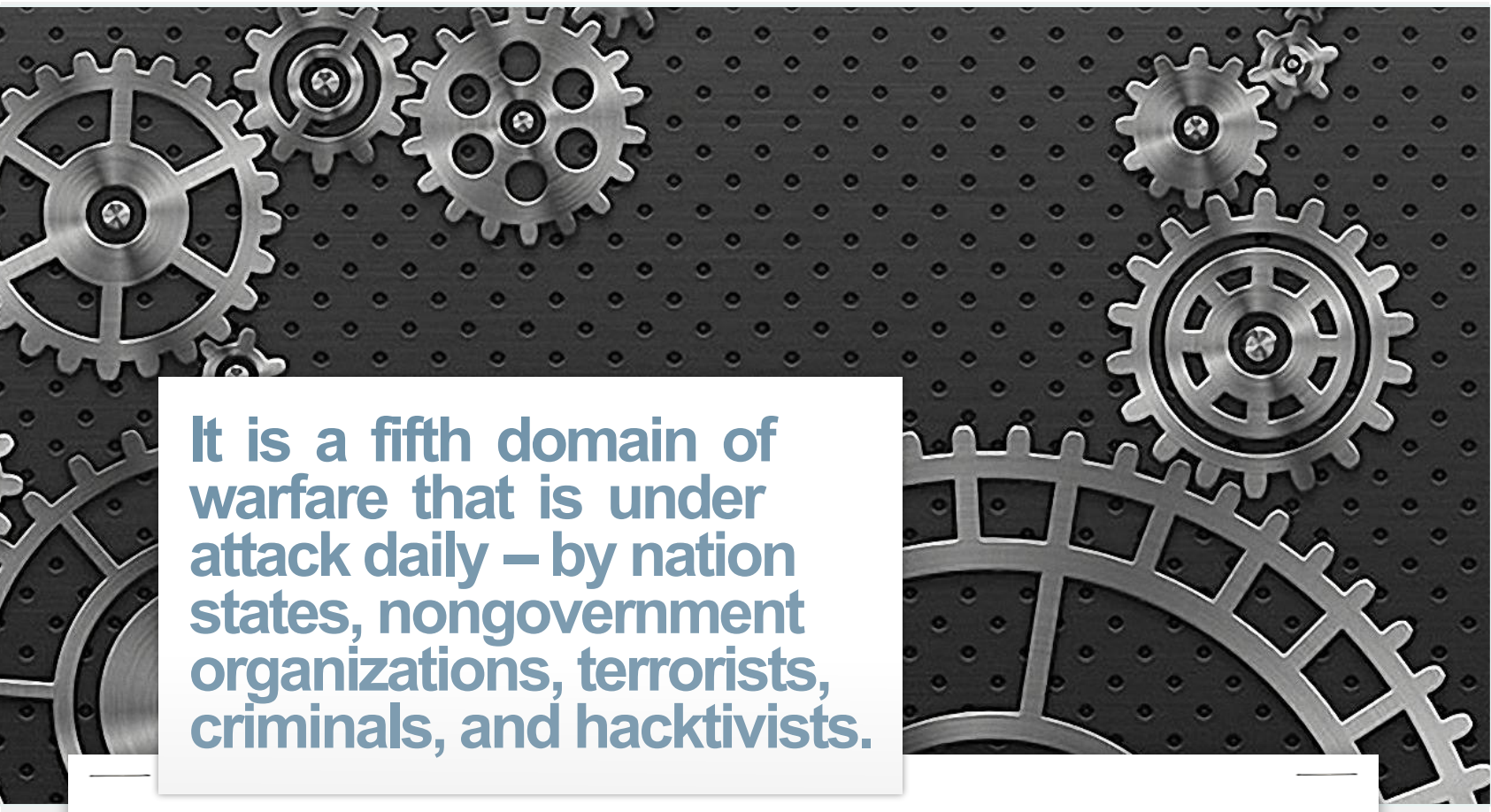
Cyber counterintelligence presents the students of the craft with foundational concepts and processes in the discipline of counterintelligence with a focus on counterintelligence missions, defensive counterintelligence, offensive counterintelligence, and counterespionage as these realms apply to traditional tradecraft, and how they are or will evolve into the cyber domain. By starting with traditional counterintelligence and progressing to cyber counterintelligence, we develop an appreciation for collection efforts, exploitation of potential threats, insider concerns, and the risks and benefits of counterintelligence.

With the expanding importance on comprehensive and timely need for intelligence for nations as well as businesses, we explore the essential elements that make up the intelligence cycle with a focus on how these pivotal points are exploited. Part of this exploration is the continued importance of critical thinking as well as out of the box analysis that is heavily leveraged to improve the critical thinking skills of analysts. As cyber topics continue to evolve, the increased importance of cyber intelligence is growing and as such, the protection of our intelligence cycles expand as well; emphasizing the growing need to ensure our processes are not compromised in a cyber dominated landscape.

Cyber counterintelligence is one aspect and possibly one of the most crucial topics at the core of protecting our collection efforts. Legal, ethical, and privacy issues should be discussed given the inherent nature of the intelligence cycle. The potential for active defense or offensive cyber counterintelligence operations is a critical function. Students of the tradecraft rely heavily on individual research and group discussion to explore the world of cyber counterintelligence, and where applicable, make use of the analysts ability to do independent thinking and analysis of problems.

Students of the craft are able to understand the role and value of counterintelligence in modern organizations, businesses, and governments. They are able to identify key elements of and cyber intelligence targeting and apply the cyber counterintelligence process to mitigate threats of information disclosure for core business processes. Analysts understand the fundamentals behind currently employed computer security technologies relative to cyber counterintelligence, review active defense and issues in offensive cyber operations. Ultimately, analysts are able to examine potential measures to identify, penetrate, or neutralize hostile operations that use cyber means as the primary tradecraft methodology, as well as intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.

From site and source reliability guidelines, analysis writing assessments and intelligence assessment guides to sock puppets, denial, deception, counter denial, and counter deception, anonymity and psychological operations, analysts understand the need for timely and relevant intelligence. These methods are required to



It is a fifth domain of warfare that is under attack daily – by nation states, nongovernment organizations, terrorists, criminals, and hacktivists.

Cyber Intelligence - What is needed to execute the payload (cont')

prepare for programs that can be long term in nature. Analysts understand the need for patience in executing cyber intelligence and cyber counterintelligence operations. In fact, some cyber analysts have been running operations for years. Operations started as a result of training and proper targeting.

My view is that cyberspace is a global domain within the information environment consisting of the independent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors, controllers -- anything connected, or connected devices.

It is a fifth domain of warfare that is under attack daily -- by nation states, nongovernment organizations, terrorists, criminals, and hacktivists.

Since cyberspace is a decentralized domain characterized by increasing global connectivity, ubiquity and mobility, where power can be wielded remotely, instantaneously, inexpensively and anonymously, the threats to global critical infrastructures is [sic] enormous, the challenges unprecedented.

The United States, NATO, the United Kingdom, and other friendly governments and organizations are inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. Cyberspace crosses geographic and jurisdictional boundaries. The expanded use of cyberspace places our interests at greater risk from cyber threats and vulnerabilities; and cyber actors can act globally with[in] their own borders, within the borders of our allies and adversaries.

The complexity and amount of activity in this evolving domain make it difficult to detect, interdict, and attribute malicious activities. Our approach for several years has been that of a defensive posture, one that is reactive and focuses on a "see, detect, and arrest" capability, where the adversary has already emptied the coffers of our most critical information.

This needs to change.

Threats to cyberspace pose one of the most serious economic and security challenges of the 21st century. On the flip side, cyberspace offers us unprecedented opportunities to shape and control the battle space to achieve strategic objectives.

One of the key factors to meeting these challenges is cyber counterintelligence (or CCI). CCI covers the measures to identify, penetrate, or neutralized adversarial operations that use cyber means as a primary tradecraft methodology.

CCI includes activities in cyberspace such as forensics, examinations of information systems, and other approved virtual or online activities to identify, disrupt, neutralize, penetrate, or exploit hostile adversaries.

CCI is composed of both offensive and defensive elements. Offensive CCI includes a cyber penetration and deception of adversary groups, while defensive CCI includes protecting vital information and information systems from

The CCI doctrine expands upon traditional cyber intelligence collection, while pursuing the offensive exploitation and defeat of adversarial intelligence activities directed against our interests.

Cyber Intelligence - What is needed to execute the payload (cont')

being obtained or manipulated by an adversary's cyber intelligence organizations, activities, and operations. This two-pronged approach forms a comprehensive CCI strategy that is informed by collection results, and feeds more comprehensive CCI operations.

I strongly advocate for a more progressive approach to CCI. My doctrine, and I hope that of the United States, includes a collection and processing of technical and intelligence information derived from adversaries by other than an intended recipient. The CCI doctrine expands upon traditional cyber intelligence collection, while pursuing the offensive exploitation and defeat of adversarial intelligence activities directed against our interests. Not only does our doctrine protect the integrity of the government and commercial information and information systems, we believe in the use of incisive, actionable intelligence provided to decision makers at all levels that serve to protect vital assets from adversarial intelligence activities, while neutralizing and exploiting their cyber intelligence capabilities.

We believe that CCI operational activity should:

#1 - Manipulate, disrupt, neutralize, and/or destroy the effectiveness of adversary cyber activities.

#2 - Recruit or induce defection of adversary personnel using cyber personas.

#3 - Leverage denial, deception, counter-denial, counter-deception, information warfare, psychological operations and online media to manipulate, direct, and redirect our adversaries, creating advantages and influencing events that lead to desired outcomes.

#4 - Collect cyber threat information on adversary operations, modus operandi, intelligence requirements, targeting objectives, personalities, communications capabilities, limitations, linguistic focus, efforts to modify, attributable hosting locations, and vulnerabilities.

#5 - Provide information and operations databases to support decision makers.

#6 - Provide CCI support to clandestine human and cyber intelligence operations.

#7 - Identify past, ongoing, or planned cyber espionage.

#8[a] - Leverage all open-source signals, geo-spatial, imagery, measurement, human, financial, and technical intelligence.

#8[b] - Support cyber force protection operations, including, and other than, war and peacekeeping.

#9 - Acquire adversary cyber espionage capabilities for analysis, and countermeasures development.

#10 - develop operational data, threat data, and espionage leads for future CCI operations, investigations and projects, and develop the potential of these leads to enhance cyber security overall.

A direct component of CCI is cyber espionage. It is the act or practice of obtaining secrets via cyber capabilities without the permission of our adversaries. This includes information -- personal, sensitive, proprietary, or of a classified nature -- from individuals, competitors, rivals' groups, governments, and enemies for personal, economic, political, or military advantage, using cyber exploitation methods.

The use of cyber espionage to actively gather information from computers, information systems or networks, or manipulate, disrupt, deny, degrade, or destroy targeted adversary computers, information systems or networks, must be woven into our cyber security strategic plans and operational tactics.

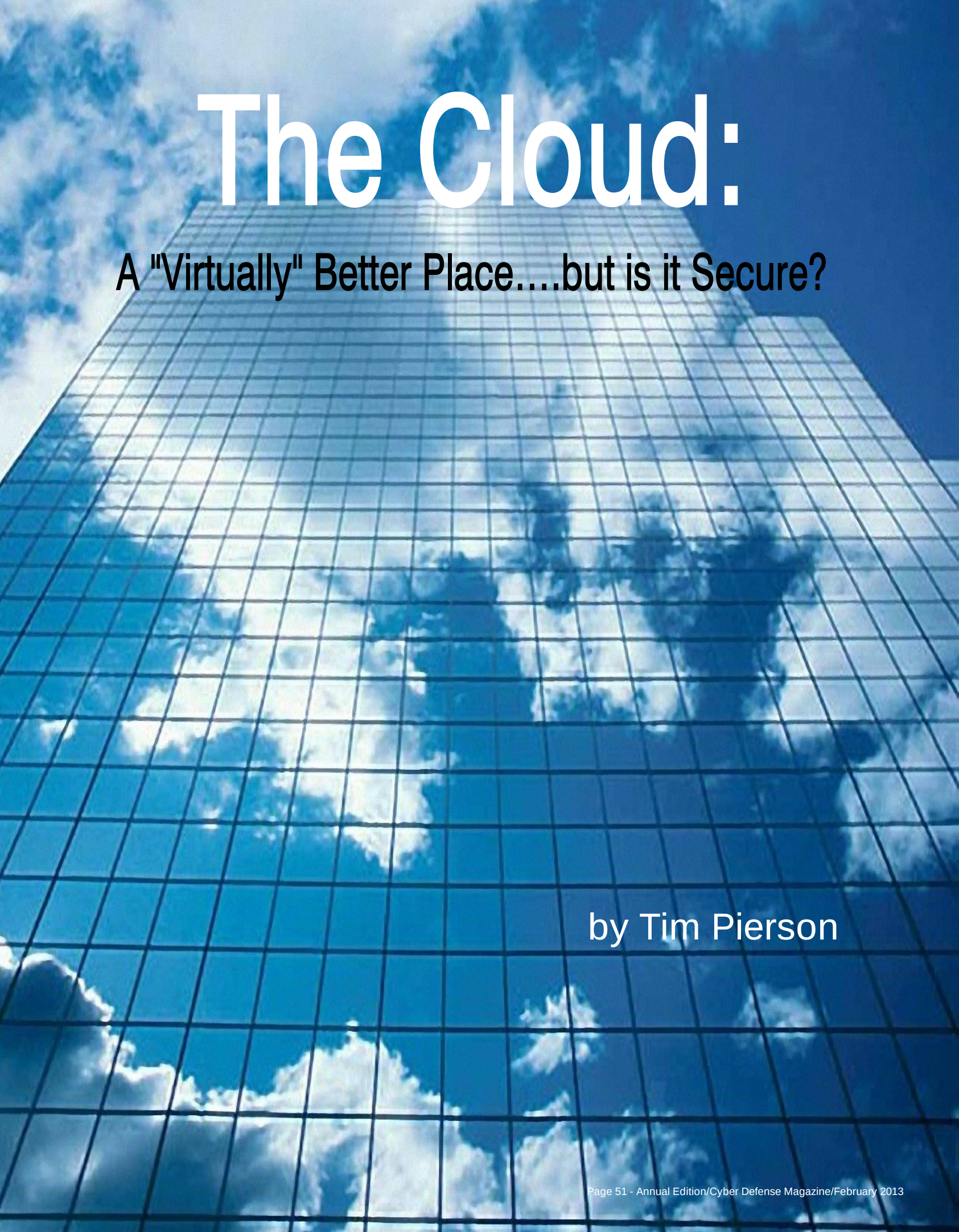
Cyber Intelligence - What is needed to execute the payload (cont')

About The Author

Cyberspace has become a main front -- the fifth domain of warfare in both irregular and traditional conflicts. Adversaries in cyberspace include both states and non-states that range from the unsophisticated amateur to highly trained professional hackers using virtual small arms that are proliferating, while growing enhanced payload and delivery capabilities. Through cyberspace, our adversaries are targeting industry, academia, government, as well as the military, and the sea-air-land and space domains. In much the same way that air power transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield us from the attacks on our critical infrastructures. Indeed, adversaries have taken advantage of computer networks and the power of information technology to not only plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of our governments and population.

In closing, CCI activities, as a component of strong cyber security practices, must be examined, strategically deployed, and operationally delivered -- while being continuously enhanced as a method of both active defense and offense. It is time we expanded our reactionary approach from see, detect and arrest, to one that is proactive and aggressive.

Jeff is the Chief Intelligence Officer for Treadstone 71. In 2007, he was awarded the RSA Conference award for Excellence in the Field of Security Practices. His team also won the 2007 SC Magazine Award - Best Security Team. Jeff sits on the Board Boston Infragard, Content Raven, Potomac Institute for Policy Studies, Journal of Law and Cyber Warfare, and Wisegate and was a founding member of the Cloud Security Alliance. Jeff served in the USAF as a cryptologic linguist, Arabic Language and in the USANG as an armor officer, armored scout platoon leader. He has BA in Special Studies - Middle East Studies & Arabic Language from Trinity College and an MS in Information Assurance from Norwich University. Jeff also attended the Middlebury College Language School for additional Arabic language training. Mr. Bardin has lived and worked in the Mediterranean area and the Kingdom of Saudi Arabic. He is an adjunct instructor of masters programs in cyber intelligence, counterintelligence, cybercrime and cyber terrorism at Utica College. Jeff also holds the CISSP, CISM, C|CISO and NSA-IAM certifications. Jeff has spoken at RSA, NATO CyCon (Estonia), the US Naval Academy, the Air Force Institute of Technology, the Johns Hopkins Research Labs, Hacker Halted, Secureworld Expo, Hacktivity (Budapest), Security Camp (Cairo), and several other conferences and organizations.



The Cloud:

A "Virtually" Better Place....but is it Secure?

by Tim Pierson

We started out with Big Iron, mainframes and the 3270, some 5250 (AS400) then moved to distributed computing. And now with desktop virtualization and cloud we are moving back to housing our machines in the data center of where this author thinks they should have remained all along. This is a fantastic idea. Why can't we just leverage this? Well it turns out we can. Let me explain.

When we were in the midst of distributed computing, it was true that things did indeed go faster because we were distributing the load but one thing you may not know is that our computers are 100,000 times faster than they were just 10 short years ago. What is a person to do with all that excess power? Well I am glad you asked, because this was the dawning age of Virtualization.

Virtualization changed the entire game less than 10 years ago and now with the advent of the cloud it looks to be doing the same thing all over again. You see taking that same concept of excess power namely CPU, Memory, Storage and directing them for mass consumption is how the Cloud was born. But how secure is it, really?

Reducing Internal Risk Exposure - Hosting Data Offsite

If you want to reducing internal risk of exposure to sensitive data, you might ship off backup versions to an Iron Mountain somewhere…that's the same thing you get, in real-time, by hosting the data on a Cloud service provider - not on your internal servers because it's off site. I used to run a training center, and I would interview salespeople often from competitors. I was told once by one: I have a copy of my current employer's database of contacts. I will give it to you if you hire me. Did I hire that person? Of course not because I know that is exactly what would happen to my data if I entrusted it to them. But if the data is not where we are able to steal it, EG no physical access, then there is no problem.

Traditional Network Security is a Three Letter Word (or Acronym)

Now let's discuss Security. You remember that rule back in CISSP the CIA? I call it the CIA triangle, meaning that if it was 3 legs of a stool and one was missing the stool would fall over. Such is the case with CIA. Of course we are referring to the Acronym.

- Confidentiality
- Integrity
- Availability

Ok so with that said, sometimes in the cloud it is much like giving your newborn to someone else to care for. There would have to be a lot of trust in my particular household. My wife is extremely discriminatory of the person who watches the dog while we are away. But not my data? My precious data? Well that is where we have to start our trust.

First off on any trust system you MUST start your trust somewhere. Just like the certificate system in use today to used "trust" various websites. We trust the signing authority that it is indeed that entity. You see when you were very young you were taught who to trust by someone you trusted. Our trust started with our parents or guardians at the time. There are several approaches:

1. Trust No One. This is always and will always be the best approach. You encrypt your data before it enters the cloud and decrypt it on the way out. The only problem with this approach is that when we have to do some type of processing in the cloud that cannot be done on the encrypted data, we have a problem. We must provide trust to someone.

2. Trust With Guarantees - Your Service Level Agreement (SLA): Cloud Service Providers - Cloud Service providers will provide you a SLA or Service Level Agreement that will detail what they will do with your entrusted data. Where it will be replicated for fault tolerance and performance reasons and how they will handle everything. Now I may be being a bit cynical here but that is simply a piece of paper. How do we really know they are doing that? Well we ask them! They will tell us they are. Oh boy, let's see you ask the person who has everything to lose if they don't tell you what they are doing on the SLA, you mean those are the people that are going to tell me if asked they are doing it correctly? Yep! That is exactly what I mean. Ok so isn't that a bit like having the fat kid guard the pie? Come on what do you think they are going to say?

3. Trust - But Verify! Now we are at a crossroads. We must feel comfortable in guarding our data entrusted to us. We have lost physical control of the CIA model. Again we must (if willing) to start our trust somewhere. Well what about compliance? What about Multi-Tenancy? I think President Ronald Regan said it best when he said, Trust but Verify. That means we have to have someone audit our cloud provider. But if you recall when he was referring to Soviet weapons of Mass Destruction we had either ourselves audit or a disinterested 3rd party audit. Regan did not say to the Gorbachav. "Now did you remove all those weapons like we agreed?" "Of course, Comrade, you can trust me!" would have been the answer.

So, now that we've discussed the key issue of TRUST when it comes to the Cloud, you'll have some good questions and talking points for your Cloud provider's security team. If they can't bring one of these INFOSEC guru's to meet with you before you sign the papers, you've come to the wrong Cloud provider. Here's what you should be asking:

4. Make Sure Your Cloud Provider Offers a Full Suite of INFOSEC Services
What kind of INFOSEC tools, products and techniques do they use to 'lock down' your slice of the Cloud? Many Cloud providers can be entrusted to provide security management if they offer things like Auditing, Patch Management, Virus Scanning, Deep packet inspection and the like; again all on the economies of scale model. We don't have the headache; we don't have to provide personnel to do this. So let's make sure they do. Find a Cloud provider who has a really beefed up, next-generation INFOSEC model and service offering that works - if they run old last-generation firewalls, you have to question where they are putting their investments for their customer-base ?

5. Frequently Audit Your Slice of the Cloud
When and how do they audit your slice of the Cloud and what do the reports look like? For me, always living in the camp of Trust No One (aka TNO) is hard for me to do. In order for the Cloud to be completely viable to mission critical data and system there must be a low cost independent audit capability set up and audited by an independent 3rd party. One in which we can push a button and a script will run telling us whether we are in compliance with the SLA provided to us by our provider. This also must be auditable or verified by some mechanism like a Hash to ensure this script has not changed. The advantage of leveraging a slice of a Homogenous Cloud means that we can get economies of scale on Audits. When a 3rd party audits against my SLA they also do that for the same tenants on the same cloud making the cost lower.
Let's look at a few recent examples of failures where cloud providers may have dropped the ball.

Hack a Long Time Coming
According to a recent Blog posting; this attack appears to have begun in mid-May 2012. It appears an account request was sent to Gmail for my personal email address. Google's procedure asks for a number of questions to attempt to verify account ownership. This author is still not clear on how the process works, but it appears those weeks after the process were initiated, the hacker somehow convinced Google's account recovery systems to add a fraudulent recovery email address to my personal Gmail account. For example, the password used on this victim's personal Gmail account was 20+ characters long, highly random, and not used by me on any other services so that says to me it was reset, not dictionary attacked or guessed.
Once the recovery email address was added, the hacker could then reinitiate the password recovery process and get reset instructions sent to the fraudulent email address. Those instructions were then used to reset victim's personal email.
Google Apps and Privilege Escalation
Like thousands of other companies, CloudFlare uses Google Apps for email. When first established CloudFlare.com's email address, the victim listed their personal email address as a recovery email for their account. The hacker was able to use Google's password recovery and have the password reset sent to my personal email for my CloudFlare.com address. Surprisingly, all CloudFlare.com accounts use two-factor authentication. It is my understanding that the victim is still inquiring with Google to understand how the hacker was able to reset the password without providing a valid two-factor authentication token.
Once the attacker had access to my CloudFlare.com email account, the hacker was able to access our Google Apps administrative panel. The hacker appears to have targeted a particular customer, and initiated a password reset request for the customer's CloudFlare.com account. The customer sent a copy of these requests to an administrative email account for debugging purposes and, ironically, to watch for invalid password reset requests. The hacker was able to access this account in Google Apps and verify the password reset. At that point, the attacker was able to log into the customer's CloudFlare account and change DNS settings to temporarily redirect the site.?

Another such incident
A close friend while working at Veritas, did a security audit of a newly-built data center product. A bunch of top line ethical hackers were called in and they found some critical security holes. A few of the issues were found in my friend's code.
The code found was close to the kernel and my friend assumed that it was shielded by the layers of other code on top of it. We remember what happens when we assume? You see he is a new young engineer, full of self-confidence and ego, you know the type, he walked to one of the "so called" ethical hackers/security experts and defended his work by claiming that the software using his work should already be secure and I shouldn't be repeating the same security code in my work. Again where do we start our trust?
I think the ethical hacking group brought in to test the security said it best - "The best security architecture assumes that the layer on the top is already compromised".
Looking back, the year 2011 saw some of the worst cloud security incidents. There were over 535 incidents recorded affecting over 30.4 million sensitive records (source: privacyrights.org report). I guess my favorite spankings was the attack by Anonymous on Sony (details here), primarily because of the "spanking" it provided. As a previous football player I like to use the analogy that sometimes we have to get spanked before we wake up to see what is going on in front of us.
And if you look at what really happened mid-summer 2012 with Drop box, then it's quite applicable to the statement previous. An employee password was compromised and their account had a project file with customer email addresses and details. Was it failure or oversight to believe that these customer email addresses were protected in the cloud? How many of us are doing something similar? Dropbox has probably fell victim to its own popularity and at scale that everything breaks (source: Urs Hölzle, Google). But there is lot to learn from these incidents.
For example this author has a friend who works at Druva where they constantly try and learn from these incidents. They also regularly invite security enthusiasts and audit teams to review their architecture.

Following are a few "spankings" and thus corrections implemented at each level to secure their cloud:

Access/Outer Layer

- Network and At-Rest encryption. Some authors refer to this at rest and in flight.
- Two-Factor authentication of critical users and admins. With today's cell phones this is an easy low cost implementation.

Within the Cloud/ Inner Layer

- Two-Factor encryption (patent pending by Druva) - uses a bank locker like system where neither cloud provider or the user has full access to encryption keys
- It passes the monkey wrench technique like Last Pass ™. Where each holds a portion of the key cannot have the other force-ablily beaten out of them with a monkey wrench.
- Sandbox data for every customer, so a compromised user/customer shouldn't be threat to all
- Establish Employee Access and Control Policies
- Transparently separate the cloud access control - between Design, Architecture and Operations team. The person designing the security should have to not have access to the cloud, and vice versa.
- Data/byte scrambling to avoid any direct access to data

As cloud becomes more affordable, its widespread adoption will be inevitable. But the long term adoption from enterprises will depend upon how it gains the CSO's trust. Ah there is that word again; Trust. Simply encrypting data and getting an audit will not be enough in this author's opinion. As a majority of the cloud service providers use other infrastructure services like AWS, the foundation for secure cloud will depend upon each layer within the cloud to establish security and even redundancy with the underlying layer.

Tim Pierson has been a technical trainer for the past 23 years and is an industry leader in both Security and Virtualization. He has been a notable speaker at many industry events including Novell's Brainshare, Innotech, GISSA and many military venues including the Pentagon and numerous nuclear facilities addressing security both in the US and Europe. He is contributor to Secure Coding best practices and coauthor of Global Knowledge Windows 2000 bootcamp. Current projects include contributing author of "VMware Virtual Infrastructure Security:- Securing ESX and The Virtual Environment" released in April 2009 by Pearson Publishing and has done work for the bimonthly Virtualization Security Roundtable Podcast available as a download on iTunes and Talk Shoe. Tim is one of the EC-Council's Master Instructors.

THE BEST DEFENSE IS OUR DEFENSE

With AppRiver, you can build layers of protection against hackers, spammers, scammers and online crooks. AppRiver's services are easy, effective and affordable. Plus, all of them come with a 30-day free trial and 24/ US-based Phenomenal Care.

Spam & Virus Protection • Web Security • Email Encryption • Secure Exchange Hosting

appriver®
Email & Web Security Experts™

www.appriver.com
sales@appriver.com
(866) 223-4645

Cyber Defense Test Labs: Spotlight

SG2124: Next Generation Security Switches

Security teams usually use internal Security Information Event Management (SIEMs) to be their watchdog for alarming them about threats and risks behind their firewall. Many have started to deploy complex Network Access Control (NAC) solutions and enhanced Endpoint Security software to detect, alert and block high risk internal network access. However, most of these alerts happen a little too late. At CDM, we've only seen a few proactive security solutions focused on the actual physical port that the user plugs their Desktops or Laptops into to gain Local Area Network (LAN) access. The HanDreamnet SG2124 is one of the first line-speed, security centric managed switches we've seen on the market and part of the SG2000 family. Yes, we actually had to spin the globe and reach far into Asia - South Korea to be exact, to find these innovative switches. They are now just coming to market in the US and Canada - in fact, Solantus, Inc. - whom you may already know as one of the very few bold and innovative infosec distributors has recently introduced this product line. Some of the key reasons that we also like this switch fabric is as follows:

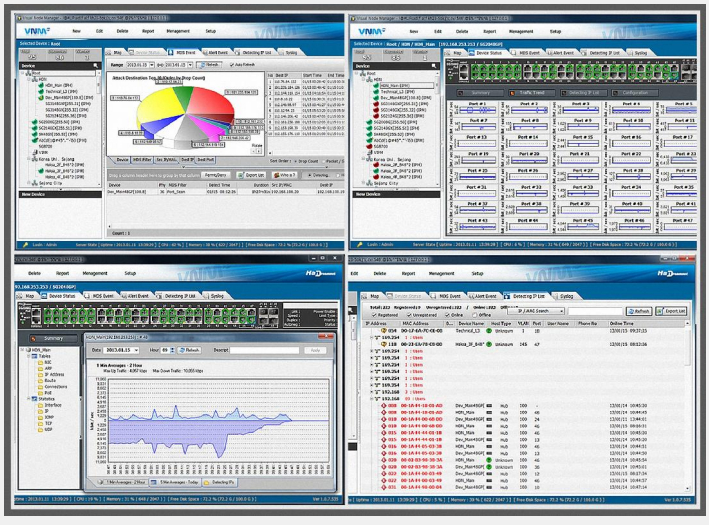
1. Lower total cost of ownership (TCO) than Cisco, Juniper or Extreme, among others.
2. No agent-based software to install so you transparently deploy them or replace aging switches.
3. No affect on the network and in fact, these switches are performing at speeds we didn't expect to see, while security functions are all enabled, by default.
4. Real-time detection and blocking of high risk security events at the physical port level.

How beneficial is an internal threat and denial of service protecting switch? Here are some real-world examples of recent deployments in Asia by end-customers of HanDreamnet:

Electronic Semiconductor Manufacturer - Experienced a flooding attack, which occurred internally. Whole manufacturing lines were stopped. All of production material and goods were scrapped. After deploying SG2124 managed switches, the problem was solved and hasn't happened again…one infected system goes instantly offline at the physical switch port level when this kind of problem flares up again. They re-image the system and try to 're-educate' the employee about mal-behavior leading to installation of malware.

Very Large Corporation - Experienced a spreading worm by mobile user's laptop which caused a huge amount of internal traffic flooding. They had difficulty tracking it down to the source and lost an entire day at corporate headquarters because of this fast and wide spreading worm. After deploying SG2124 managed switches, future worm outbreaks were instantly mitigated at the specific ports where they began, before causing peers on the VLANs to become infected or go offline.

Large University - One of the student labs caused a Distributed Denial of Service attack which caused the firewall to lock-up from bulk traffic sessions and they lost internet access for an entire day and evening. Once they replaced their 'big brand name' switches with the SG2124 series they have not encountered any downtime, since, while experiencing frequent 'troublesome' student traffic. This 'troublesome' traffic gets blocked nearly immediately at the physical switch port, protecting the rest of the network.



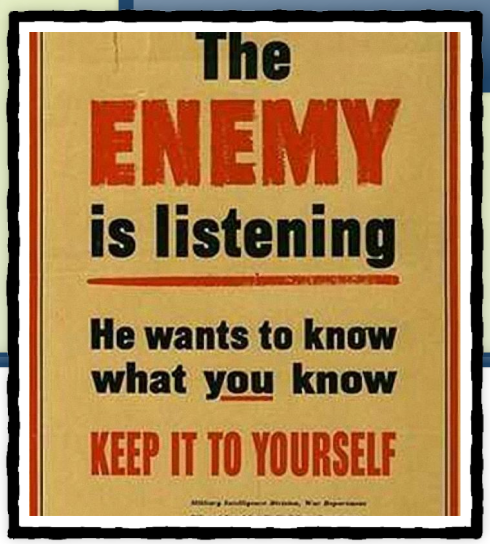
How does the SG2124 do this? Through innovative layer 2 security management:

- Secure Wire Speed "Clean-zone"
- Scanning, Flooding, DoS and DDoS protection up to Layer 4 without Signature Updates.
- Real-time Security from built-in ASIC-based Multi-dimensional traffic security engines.
- Internal Network Access Traffic Control with monitoring and metering down to the port.
- An Integrated Observation System offering real-time monitoring and history reporting.

…and it does all this at a very economical price point for SMBs to very large enterprises. For more than one SG2124 deployment, you can get the Virtual Node Manager up and running in a matter of minutes to keep an eye on your 'intranet' similar to a SIEM but watching ports and VLANs in real-time including infection analysis but also remote traffic control functionality. To learn more about the SG2124 or to see a demo of the Virtual Node Manager, contact Solantus through email at sales@solantus.com.

CYBER ESPIONAGE: DATA EXFILTRATION IN 2013 AND BEYOND

by Dave Porcello



Learn how to detect and block data exfiltration and covert channels

Ok, so you've set up a powerful firewall for your organization. You've locked down all high risk ports. You've only left a few outbound ports open for must-run protocols - SNMP, POP3, HTTP, HTTPS, DNS.

Your network is locked down and you've even added a content proxy to make sure employees don't browse inappropriate site and scrubbing their emails to make sure no junk mail, viruses or other risks come and go through your firewall.

Is your internal network safe and secure from data exfiltration and data leakage over covert channels? Not likely.

Defining Data Exfiltration

Data exfiltration is the leakage of sensitive information such as company secrets, source code, customer records and personally identifiable information (PII). After an attack, cyber criminals can have access to this data in your environment, but to better analyze your sensitive data, they often take files out of your environment and into their own.

Data leakage can have a huge impact on your organization - from the risk of government fines to brand reputation damage and lost revenues. While data can be exfiltrated via physical methods (USB Stick, shoulder surfing, etc), we'll focus on the most prevalent threat facing organizations today, network-based exfiltration by external or internal parties.

Before Its Exfiltrated, Data Must Be Gathered

To better understand current data exfiltration techniques - both by automated and manual techniques, we must understand how data flows in your environment and what tools are available to an attacker in that environment. A point of access must first be established - this is what is traditionally referred to as a "security breach." This can occur via a client-side exploit, weak system credentials, SQL injection or other methods. The most commonly used technique today by sentient attackers is via your own remote access applications - RDP or a VPN.

Data Leakage Starts from Behind Your Firewall

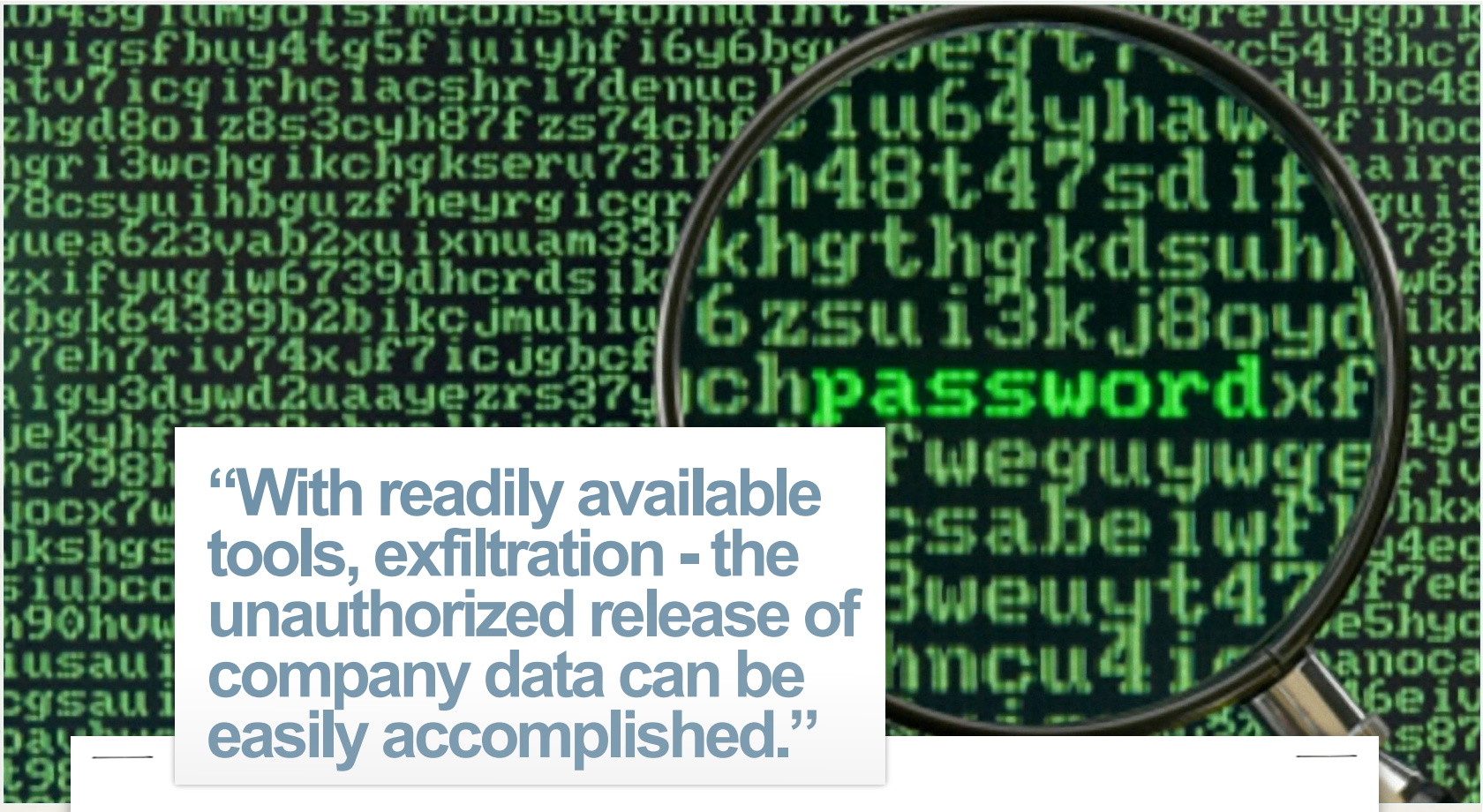
Once that point of access is obtained, the attacker then goes looking for interesting data in the environment. Data at rest is often gathered via built-in Windows shares or FTP clients, and data in transit is gathered with a variety of techniques, the most common of which is parsing memory, where data is unencrypted and available for the taking.

Getting Data Out

Once the attacker has your data, they need to get it out of your environment.

Attackers are likely to use your own built-in tools - RDP or VPN solutions. Because these remote access tools are typically encrypted, and traditionally hard to inspect, this is an easy way for the attacker to pull data out of the environment without detection. One of the best things you can do to protect yourself is monitor usage of the channels, and watch for anomalies.

Malware analysis tells a story of common internet protocols being abused to send your data out. Partially because of the complexity of automating remote access solutions, and in part due to the availability HTTPS, FTP and SMTP libraries, these network protocols are often used by malware to send data out of the environment.



> **"With readily available tools, exfiltration - the unauthorized release of company data can be easily accomplished."**

Advanced Data Exfiltration with Covert Channels

Since you're already filtering inbound and outbound connections, you might be able to catch the attacker connecting to your VPN from Romania but attackers are already moving toward more advanced data exfiltration.

Using a technique called "tunneling," data can be encrypted in archives or in transit, limiting the ability to inspect it at a proxying firewall - It just looks like traffic over HTTP/S, or DNS, or ICMP, among others. These are commonly referred to as "covert channels." With covert channels, attackers can hide what they are saying or passing by writing a message inside a message, much like stenography can hide a picture inside a picture.

Testing covert channels

Using tools like HttpTunnel and STunnel, publicly available open source programs, users can tunnel traffic through most HTTP and HTTPS proxy servers.

Combined with features of SSH such as port forwarding, this can allow many types of services to be run securely over the SSH via HTTP connections.

But this is only the beginning. With even more open source tools that are out on the free market, you can run the Secure Shell (SSH) protocol in many unexpected ways, allowing exfiltration – the unauthorized release of company data, from the inside of your corporate network, right over your 'secure' firewall.

Common and easy-to-test techniques include:

- SSH over any TCP port
- SSH over HTTP requests (appears as standard HTTP traffic)
- SSH over SSL (appears as HTTPS)
- SSH over DNS queries (appears as DNS traffic)
- SSH over ICMP (appears as outbound pings)
- Out-of-band SSH over 3G/4G/GSM cellular

If you are the corporate security professional, maybe that would be ok for remote access to the office but what if an malicious insider decides to send your corporate secrets to their home network? How would you catch them from leaking confidential corporate data if they were to use these tools and techniques?

Killing Cellular and Wireless Covert Channels the Old Fashioned Way

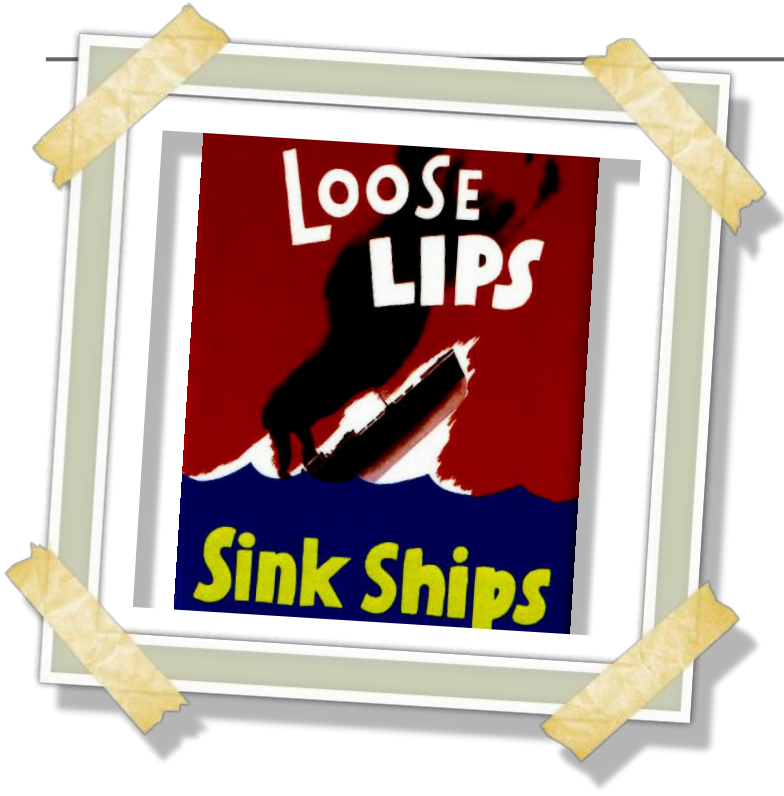
Before we get into detection and/or stopping network traffic-based covert channels, what can we do about 3G/4G/GSM cellular or even wireless? If a malicious insider sets up a covert channel and decides to use one of these protocols, data leakage can occur over the airwaves and you might never notice. Without even having to sniff the airwaves, let's talk about the easiest method that the NSA and CIA use - tinting materials placed on the corporate office windows that block all forms of cellular and wireless traffic. That's the easiest way to deal with this problem and it's done physically - by obtaining radio-signal blocking window film. Just google "signal block window film" and you'll find one of the vendors who sells this kind of product.

Detecting and Blocking Network-Traffic-Based Covert Channels

Now we get into the really hard part - the heavy lifting. This is a multi-pronged process. There's no simple product or answer. Here's my list of things you should do to mitigate the risk of ongoing network-traffic-based covert channels and unknown data leakage by malicious insiders:

1. Do the basics - Proxy Traffic, Review Firewall Logs and Look For Network Anomalies

Now, you'll need to deeply inspect packets and review traffic. To detect basic data exfiltration, you'll want to inspect outgoing traffic for patterns of sensitive data - credit card numbers, social security numbers, whatever patterns you can reliably detect.



Ensure you're proxying as many of your outgoing protocols as possible, and in many cases, you'll want to block them entirely. Is there really any need to allow outgoing ICMP? Can users systems connect to an external DNS server? Why? If you can prevent traffic to external servers altogether, you'll block all exfiltration, covert or not.

With covert channels, you'll want to look for encrypted data over a well known protocol on an open port. This would be the quickest way to detect protocols such as SSH running over HTTP or ICMP or other non-encrypted protocols.

Much of network defense comes down to being aware of anomalies on the network. If your defenders see large amounts of ICMP or DNS traffic being sent to a new host, will they detect it? Using the open source tools detailed above, or the Pwnie Express products, you can set up a test for your defenders. By simply opening a channel and sending random data through it, you can prepare your team for these threats. As they say, if you can see it, you can react to it.

2. Adding Signatures to Your Firewall, IDS or IPS

The good news here is that there are special rules you can write yourself or you can find pre-canned rules, for example, for SNORT to detect the SSH protocol as 'payload' in other protocol network traffic. Even if you are not running a SNORT compatible deep packet inspector, IDS or IPS, you can still look at the sample rules folks have written and then either ask your firewall manufacturer if they have this kind of rule they can send you or find out how to write your own rule to handle this risk.

3. Setup a Network Access Control Solution

The fact that so many employees are bringing their own devices in your organization, puts you at incredible risk - the risk of infections but ultimately data leakage. To ensure they don't bring personal devices onto your corporate network, you'll need to deploy a NAC solution like the open source PacketFence or one of the commercial products from folks like Cisco, Juniper, Forescout, NetClarity or others. Getting your internal network device

"There is a very good reason to test covert channels - IT Security staff needs to stay one step ahead of the upcoming threat."

management under control is a crucial part of detection and blocking of covert channels.

4. Employee Background Checks and Frequent Screening

First, it starts with employee screening and frequent employee reviews. You need to make sure your employees are honest, ethical, trustworthy and also don't have such incredible financial problems that they become a high risk to your organization. When the FBI or CIA does a background check, they consider a person's credit health one of the top issues related to their ability to be corrupted or subverted. Now just because your receptionist and her family are under water financially and their credit score is very low doesn't mean they will become a malicious insider but it does place your organization at risk that this individual - with the keys to the castle, could be bribed to bring in a USB stick, plug it in and run an executable in return for enough money to pay off her family debts. This kind of incident has happened at US Banks so don't think it can't happen to you. By doing permission-based screening, you can get employee background information, financial information and other information including criminal records and have a better understanding about employee risk. Doing this once, twice or four times a year might save you from having a malicious insider. You'll quickly know when someone suffers financially that they need to be observed more closely.

As we continue to face global economic challenges, the 'trickle down' effect of this causes people we might usually trust to take actions we would never expect…just watch the 2005 Jim Carrey movie entitled "Fun with Dick and Jane" and then read your local newspaper's police blog and you'll see some of your neighbors might have taken this movie as a roadmap on getting out of financial troubles. You'd be worse off if they were one of your trusted insiders on your corporate network. Stay vigilant!

I hope you enjoyed this article and will start to look for and block unwarranted covert channels. When it comes to IT Security staff using covert channels, there's a good reason to test - for penetration testing of your own network and staying one step ahead of the threat. Please read my next article where I show you how to build a very low cost 'eavesdropper' using a USB TV tuner and a few parts from your local electronic supply store such as Radio Shack. We'll build 'next generation' software-defined radio to test other lesser-known parts of the RF spectrum, such as pager traffic and GPS. Could these also be covert channels? Find out more in the next edition of Cyber Defense Magazine.

ABOUT THE AUTHOR

Dave Porcello, Founder & CEO of PWNIE EXPRESS.

Dave is an INFOSEC expert who has developed industry leading penetration testing tools and techniques. He frequently speaks at major cyber security events about best practices in penetration testing and system hardening.

He founded PWNIE EXPRESS, to deploy the 'coolest and most innovative' penetration testing drop boxes for persistent penetration testing with remote access by corporate IT security staff.

To learn more about Dave, visit him online at www.pwnieexpress.com.

WELCOME

THANK YOU FOR JOINING MY BOTNET

CYBER DEFENSE TEST LABS (CDTL)

After three months in our test labs, we've reviewed dozens of the most advanced, next generation anti-virus solutions. Only those that received an overall rating of five out of five stars made it into the following pages. Read on and learn more about these anti-virus solutions that deliver the goods. We've taken the heavy lifting out of the review process, so you can choose the solution that best fits your needs.

Emsisoft Anti-Malware v7.0 Review

Cyber Defense Test Labs Review:

EMSISOFT ANTI-MALWARE 7.0

Introduction

Cyber Defense Magazine (CDM) launched the Cyber Defense Test Labs (CDTL) to test and highlight some of the lesser known anti-virus players and next generation anti-malware solutions on the market. While some are much less significant in size, like Emsisoft, who prides themselves on being one of the leading 'virtual' companies in INFOSEC, with engineers spread throughout the globe, they remain lesser known brands like Symantec and McAfee, yet their products outperform and outshine these bigger brands. What we like most about Emsisoft is how easy the product installs, how quickly it runs and how little 'footprint' it takes during scanning and malware blocking operations. Please read on and learn more about Emsisoft in their award winning product review.

Company Snapshot

Emsisoft was founded in 2003 with lots of anti-trojan, anti-keylogger and firewalling experience including the acquisition of the Online Armor firewall. The company has been growing slowly and organically through revenues only, with no sources of outside funding. This is our Editor's favorite model - sweat equity and gaining happy customers who then spread the news via word of mouth. Same model we are using to build Cyber Defense Magazine. This is only one of the many reasons this product suite has been selected as Editor's Choice. The company is registered in Salzburg, Austria, however, leveraging the 'virtual office' model and telecommuting so popular in Europe, Emsisoft employees are spread around the world. With full-timers, freelancers, part-timers and contractors, Emsisoft has 22 team members. With slow and steady growth, Emsisoft has millions of downloads of their software in 2012. While they are still one of the smallest vendors and the underdog, they have done things that companies with thousands of employees in the INFOSEC space have been unable to accomplish.

Customer Service

They offer customer service in 10 different languages (English, German, Russian, Spanish, French, Italian, Portuguese, Greek, Polish and Romanian) via email, but also via phone and remote connection on demand. They guarantee within 24 hours response time and their customer satisfaction level is very high. When it comes to "EMERGENCY" malware infection removal, they do a wonderful job - they passionately enjoy helping folks get rid of infections (and learning how to improve their product in the process), so Emsisoft also offers a free of charge service on our support forum to help getting rid of any infection. Emsisoft actually believes that it is wrong to charge people in such high stress level situations. If they are convinced by the capabilities of the support team and the malware removal products and services, Emsisoft believes good potential customers will purchase a license afterwards anyway - this is also another reason why they have made Editor's Choice this year. What a wonderful philosophy they've put into action. Talk about a 'positive' charma approach to cleaning up malware. As a result, they have very passionate customer reviews and testimonials throughout the web. If you just search 'Emsisoft positive reviews' you'll see many.

> "By living up to their promise of blocking all malware, both known and unknown...they receive our Editor's Choice Anti-virus Solution Award for 2013."

Customer References

While they won't name any customers, they are mostly focused on the CONSUMER and are just now expanding into the small to medium size (SMB) market with the beta version of their centralized command center, called the Emsisoft Enterprise Console. Many of their consumers who have experienced an infection found that they did not have to wipe the hard-drive to remove the malware using Emsisoft and throughout the web you will find very positive reviews, comments and feedback.

Malware Database, Updates, Scanning and Blocking

Emsisoft Anti-Malware uses two scanner engines. One is licensed from Bitdefender and the other is now officially their own scanner engine that specializes in detecting the harder malware traces to find and remove while the Bitdefender engine does a great job finding and catching the more popular malware infections. On top of Bitdefender's MD5 hashed malware signature

Emsisoft Anti-Malware v7.0 Review

> “We think Emsisoft has a cutting-edge anti-malware solution. Emsisoft Anti-Malware has earned Five out of Five Stars and our coveted Editor’s Choice Award.”

database, Emsisoft has over 10 million additional unique malware patterns - this is one of the reasons they run so efficiently. They use patterns to detect malware so if you have one of the 100,000 possible derivatives of W32 for example, they only need a few pattern samples to detect all of these variants. On top of that, Emsisoft updates their database every hour, if there are any changes or improvements, you'll have them very quickly.

Zero-day Malware Detection and Blocking - Strong Multi-scanner Protection

Emsisoft offers frequent, on-demand cloud-based updates, on an hourly schedule. They make claims that this solution can stop all malware including zero-day and it turns out that if you use their product as documented, they may actually be able to hold up to this claim. One of the challenges they face in their attempt to reach this goal is the 'noisiness' of their product in the sense that it can operate in a nearly-paranoid mode, warning you about all malicious behavior including that which we all find acceptable today - such as SKYPE opening ports and operating like covert-channel malware, which technically is mal-behavior. On the bright side, they blocked all the malware we threw at them including many nasty zero-day variants.

Dealing with False Positives - Might Keep You A Bit Busy

You really need to deal with what some might call "paranoid" popups but by doing so, your system remains secure and if you are a geek who enjoys knowing exactly what is happening with your system, Emsisoft knows and tells you, every time. On the scanner and cleanup side you have to be careful quarantining or removing components of trusted applications that trigger alarms with Emsisoft, based on mal behavior. You may trust the program but it may hook the keyboard or install a wierd driver or like SKYPE, open ports without your permission. If a piece of the program ends up in the quarantine, it won't work anymore. You can remove it from the quarantine and you can submit the file directly to Emsisoft so they will review it and decide if they feel that it is a false positive and in one of their frequent updates they will let you know that they agree with you and will offer to unquarantine the file or files. Because they have millions of users, this happens frequently so you'll get some files optionally unquarantined even if you weren't the one to submit them to Emsisoft for review.

Innovation, Uniqueness and Next Generation

We think Emsisoft has a cutting-edge anti-malware solution. Add the Emsisoft Online Armor firewall to the mix and you have a very "BlackICE" like HIPS engine. Now here's where it can get noisy but it's always to your benefit - it monitors all system areas that might be subject for attacks. If something is changed by unknown software, users will see an alert and can decide how to proceed and store a rule for that decision. However it must be clearly said that HIPS technology is ideal for advanced users by design. The best alert system doesn't help if a novice user just clicks "allow" on each of those 'nasty' alert boxes.

As a result, Emsisoft focused on development of a behavior blocking technology, very early in the game. Emsisoft was one of the first vendors that offered a 'working' behavior blocker in Emsisoft Anti-Malware back in 2005 and they also offer a pure behavior blocker product called "Mamutu Behavior Blocker" in parallel. The idea is simple: Each malware behaves in a malicious way, no matter how it does that in technical aspects. A Trojan always sends data, a keylogger always logs keyboard input, a backdoor always open a back door. Their software watches all running programs for such activities in realtime and alerts if something suspicious is done. However the biggest challenge was to reduce the number of wrong alerts caused by good programs that behave very similar to malware to an absolute minimum. After many years of fine tuning Emsisoft claims to have actually cracked the problem and today they have earned other lab test awards with their behavior blocker when classic signature based detection reaches its limit on zero-day malware attacks.

Free Trials, Platforms, Pricing and Availability

We love free tools, although the hyperlink is subject to change, here is where you will find Emsisoft's trials and free tools: http://www.emsisoft.com/en/software/download/

Their solutions run on most Windows-only platforms and their pricing is set at market rates.

Product Effectiveness:	ê ê ê ê ê
Customer Support:	ê ê ê ê ê
Platforms and Pricing:	ê ê ê ê ê
Installation and Documentation:	ê ê ê ê ê
User Interface and Ease of Use:	ê ê ê ê ê
Overall Rating:	ê ê ê ê ê

Summary

By living up to their promise of blocking all malware, both known and unknown, combining two best-of-breed multiple anti-malware scanner engines with the constantly updated Online Armor firewall, with a complex graphical user interface (GUI), exposing lots of features and functions, they receive our **Editor's Choice Anti-virus Solution Award for 2013.**

Cyber Defense Test Labs Review:

LUMENSION® ENDPOINT MANAGEMENT AND SECURITY SUITE

Introduction

Cyber Defense Magazine (CDM) launched the Cyber Defense Test Labs (CDTL) to test and highlight some of the lesser known anti-virus players and next generation anti-malware solutions on the market. While some like Lumension have hundreds of employees, they remain lesser known brands compared with Symantec or McAfee, yet their products outperform and outshine these bigger brands. What we like most about Lumension is how feature rich this solution is as an endpoint security offering. From malware blocking to application control, from data port control to system hardening, they've created an Enterprise class endpoint management solution. Please read on and learn more about Lumension in their award winning product suite review.

Company Snapshot

Lumension was formed by the merger of Patchlink (founded in 1991) and SecureWave (founded in 1999), along with some other acquisition and is privately venture funded. Lumension is headquartered in Scottsdale, AZ, with additional offices in Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the UK, and Australia with approximately 270 employees, globally. Over the past several years, Lumension has proven its ability to serve the largest and most demanding customers worldwide by exhibiting significant growth in the mid- and large-enterprise market segments.

Customer Service

Lumension is known for providing world-class customer support and services 24 hours a day, 365 days a year. Lumension provides its 5,100 customers worldwide with service at any time, via phone and email. Coverage is provided by three (3) regional support centers in the US (Arizona), EMEA (Ireland) and APAC (Singapore). Lumension also has a comprehensive customer portal (Lumension® Customer Portal) which includes access to an extensive Knowledge Base, all product documentation, and binary downloads (if needed). In addition, customers have 24x365 access to our online learning center (Lumension® Learning) which has video-based training for all product modules. Finally, they offer an online end-user community (Lumension® Connect), where customers can join forums and groups, share media and reach out to other customers.

Customer References

Lumension provided CDTL with references in health care and other markets. They have some marquee accounts including ING, Barclays, Salvation Army, Virgin Atlantic and many others. Feedback from all references was extremely positive. While the whitelisting capability is a strength, the only minor concern of end-users is the lack of a client firewall.

Malware Database, Updates, Scanning and Blocking

Lumension licenses their anti-virus engine from Norman ASA, who is one of the pioneers in the AV industry. Norman was founded in 1984 and is a well-recognized leader in the space, especially in the OEM business where they supply their AV engine to some of the biggest names in the industry. They hold many innovative patents, including the SandBox emulator / behavioral analysis technology which detects and stops novel unknown malware (zero-days). The best way to test malware samples and help rapidly develop signatures is through this SandBox technology. The application whitelisting module was developed by Lumension. It is updated frequently and has a poweful scanner and sandboxing technology to detect and block malware.

"From malware blocking to application control, from data port control to system hardening, they've created an Enterprise class endpoint management solution."

Lumension collects malware samples from a wide variety of sources, including approximately 100 customer submitted samples per day, over 20,000 "wild" collections from sources such as VirusTotal, NSIC and honeynets per day and sample collection exchanges with other AV vendors of about 20,000 per day.

In all, they have confirmed to CDTL that they see about 30,000 new and unique files per day, which are then processed and the signatures added to the database. The signature update files are pushed to customers twice-a-day; customers have the ability to manage how

Lumension® Endpoint Management and Security Suite Review

> "By combining blacklisting, whitelisting and the powerful sandbox capabilities of their anti-virus engine, they have a very solid anti-malware offering."

customers twice-a-day; customers have the ability to manage how and when these are then pushed to endpoints under their control.

Zero-day Malware Detection and Blocking

Lumension® AntiVirus identifies malware on a "family" basis instead of the common practice of counting each individual malware variant; in today's sophisticated threat environment with rapidly mutating (polymorphic) malware, the practice of counting each individual malware variant leads to some spectacular numbers but which ultimately is not terribly useful.

That said, the current malware database contains approximately 15M samples at this time; efforts are made to dedupe and leverage the DNA Matching (partial signature matching) technology to minimize the size of signature files and thus reduce negative endpoint performance impact.

Lumension is constantly updating the malware database based on inputs from a large variety of sources; these updates are pushed to customers twice-a-day. Lumension has multiple capabilities which detect and block zero-day (unknown) malware.

These include the various heuristic capabilities mentioned above especially the SandBox behavioral analysis tool and the whitelisting capabilities which prevent unknown, unauthorized, and/or unwanted executables from running in the environment.

Together with their patch & configuration solution (Lumension® Patch and Remediation), these form a solid defense-in-depth approach to security. Note that all of thier solutions (Lumension® AntiVirus, Lumension® Application Control, Lumension® Device Control, Lumension® Patch and Remediation are also delivered as integrated modules in their Lumension® Endpoint Management and Security Suite for improved security. CDTL believes the entire suite works best at detecting and blocking zero-day malware.

Dealing with False Positives

Occasionally Lumension sees some false positive reports on non-critical files. The SandBox emulator technology - which has been in market for over 7 years - is by design a stringent assessment tool aimed at blocking unknown malware (zero-day) and can sometimes return false positives.

Considerable effort is put into preventing false positives by improving routines and processes as well building up a good, clean dataset.

There are several ways of handling false positives including submission to Lumension, add to the exclude list, whitelist them or run them in the SandBox.

Innovation, Uniqueness and Next Generation

By combining blacklisting, whitelisting and the powerful sandbox capabilities of their anti-virus engine, they have a very solid anti-malware offering.

In addition, Lumension uses a unique approach to truly integrated defense-in-depth approach for endpoint security and management, covering anti-virus, application whitelisting, port and device control, data encryption, configuration management, patch management and vulnerability remediation all in one endpoint security suite.

Free Trials, Platforms, Pricing and Availability

Lumension does not offer a consumer product suite. However, for SMBs and larger Enterprises, free trials are available through a variety of trial options, including their "easy track" virtual hosted trial and "total track" full installation trial.

To learn more, visit:
http://www.lumension.com/Products/Evaluation-Request.aspx

This solution runs on most Windows platforms and their pricing is based on volume seat licensing - the more seats and the longer the license, the deeper the discount.

The complete package for a three year license can range anywhere from approximately $150 per seat down to $65 per seat for 1,000 to 10,000 seats.

Product Effectiveness:	ê ê ê ê ê
Customer Support:	ê ê ê ê ê
Platforms and Pricing:	ê ê ê ê ê
Installation and Documentation:	ê ê ê ê ê
User Interface and Ease of Use:	ê ê ê ê ê
Overall Rating:	ê ê ê ê ê

Summary

It's exciting to see a combination of blocking and data leakage protection technology with system hardening all wrapped up into a wonderful Enterprise solution.

For their broad array of powerful, defense-in-depth features and functions, as well as a very clean and easy to use graphical user interface (GUI), an excellent customer service offering, clean documentation and competitive pricing, we give Lumension our Best Endpoint Security Suite Award for 2013..

Comodo Internet Security 2013 Review

Cyber Defense Test Labs Review:

COMODO INTERNET SECURITY 2013

Introduction

Cyber Defense Magazine (CDM) launched the Cyber Defense Test Labs (CDTL) to test and highlight some of the lesser known anti-virus players and next generation anti-malware solutions on the market. While some are significant in size, like Comodo, they remain lesser known brands like Symantec and McAfee, yet their products outperform and outshine these bigger brands. What we like most about Comodo is how proactive the company has been at advancing their preemptive nature, providing more proactive protection with a clean graphical user interface (GUI) and the most powerful detection, blocking and cleanup technology we've found in the industry. Please read on and learn more about Comodo in their award winning product review.

> "...the most powerful detection, blocking and cleanup technology we've found in the industry."

Company Snapshot

Comodo Group, Inc. was founded in 1998, is privately held and is headquartered in Jersey City, NJ. Comodo has offices in UK, China, Japan, Israel, India, Romania and Ukraine, with over 600 employees, globally. Comodo has over 25 million installations of their security software, growing monthly by hundreds of thousands of new installs.

Customer Service

Comodo has a strong customer service offering via email, phone, and they have their own very cool proprietary chat tool called GeekBuddy, which is a lot like SKYPE and Webex or Logmein all wrapped in one. It allows them to remotely diagnose and help cleanup some of the nastiest malware infections, anywhere their customers are located as long as their internet connection is still functioning. Most malware likes a live connection so this gives Comodo a unique advantage with this GeekBuddy offering. They work very diligently to resolve issues within an hour and provide the following support options:

http://www.comodo.com/support/comodo-support.php

For business customers the local reseller or service partner is always the first line of contact but Comodo is very flexible in providing support and solving problems.

Customer References

While we were unable to find a published list of anti-virus customers, as one of the oldest SSL certificate providers in the globe, they have a blue chip list of these customers, many of which we would assume have purchased the business version of their anti-virus product suite. This is the page we found the customer list:

http://www.instantssl.com/ssl-certificate-corporate/ssl-certificate-customers.html

Malware Database, Updates, Scanning and Blocking

They have the most powerful, single anti-virus engine in the market, built by their own team. With over 81,000,000 samples of malware, they have one of the largest database in the market, and growing daily with a cloud-update feed. To ensure they maintain a powerful lead against new malware, they generate an Anti-virus database update every two hours. Samples come from end-users, crawlers, honeypots, online scanners like virustotal and through exchanges with third parties.

After testing most of the leading (and a few bleeding edge) anti-virus products, we found the combination of a very large and growing signature database with a built-in heuristic engine makes Comodo's anti-virus suite hard to beat at catching a majority of malware, including zero-day. Their heuristic scanner analyzes structure and attributes of PE files and is also looking for similarities with files from known malware families. When such similarities has been found - "file looks like malware" - the heuristic scanner makes the assumption it is a malware file. The criteria that Comodo checks highly depend on the malware family. They can be relatively simple - like "same custom cryptor has been used for all known files from same malware family" or more complex, for example, virtual execution of all files from the malware family use the same sequence of key system calls, or actions. Similar patterns of mal-behavior become

Comodo Internet Security 2013 Review

> "On-top of the most powerful anti-virus system, a combination of HIPS, scanning and Default Deny engines, Comodo has wrapped one of the cleanest and easiest to use graphical interfaces (GUI) we've seen."

Common and this helps Comodo's engine stay on top of these variants.

Zero-day Malware Detection and Blocking

As to Zero-day, Comodo's anti-virus solution has two subsystems for protection against this kind of nasty: Automatic sandboxing and Default Deny HIPS.

Automatic sandboxing puts untrusted executable file in restricted virtual operating environment. Any changes (files, registry, etc.) made by an untrusted file is limited to the sandbox and has no effect on the actual user system. In this way any new virus or other malicious software are completely isolated from the user system and absolutely harmless.

Dealing with False Positives - Rare Occurrences

Comodo's INFOSEC team works hard at reducing false positives.

They check every new signature against a set of known safe files from different vendors to help reduce the risk of false positives and based upon feedback by users through email, geekbuddy support and on their online forum, they have reduced the 'noise' of false positive detection to the lowest we've seen in most anti-virus solutions.

If a signature is incorrect, the updates are so frequent that most users might not even notice this is being done on their behalf.

Innovation, Uniqueness and Next Generation

Uniquely, because of the belief in the strength and power of their offering, Comodo offers a $500 guarantee per licensed computer with thier anti-virus product. Included in the purchase is expert malware removal support as well.

What's most impressive about Comodo is thier Host-based Intrusion Prevention (HIPS) engine. They came up with the concept of a Default Deny strategy that watches actions performed by applications and allow it only when it appears in their white list. Unlike most behavior blocking systems, these actions are checked before execution, so if it is denied, the malware is unable to fully function and therefore cannot harm an end-user's system.

This Default Deny strategy along with the automatic quarantine features in Comodo's product suite 'defanged' all the malware we tested it against.Both of these malware blocking engines are able to intercept low level operating system calls, almost in the same fashion that a keylogger works, but to the end-users benefit.

Like most anti-virus products, we expected the scanning process to be quite resource intensive. However, Comodo Internet Security 2013 offers several improvements we like including a more intelligent resource usage and background mode that lowers the priority of the scanning process, allowing us to be more productive, in parallel.

Free Trials, Platforms, Pricing and Availability

Comodo offers free trials of their consumer, enterprise and mobile platform as well as many free tools. We love free tools, although the hyperlink is subject to change, here is where you will find Comodo's free tools:

http://www.comodo.com/products/free-products.php

They also have support for Linux, Mac, Windows and the Android Operating Systems for anti-virus protection. Pricing is highly competitive and Comodo frequently offers discounts.

Product Effectiveness:	ê ê ê ê ê
Customer Support:	ê ê ê ê ê
Platforms and Pricing:	ê ê ê ê ê
Installation and Documentation:	ê ê ê ê ê
User Interface and Ease of Use:	ê ê ê ê ê

Overall Rating: ê ê ê ê ê

Summary

On-top of the most powerful anti-virus system, a combination of HIPS, scanning and Default Deny engines, Comodo has wrapped one of the cleanest and easiest to use graphical interfaces (GUI) we've seen. However, it's the sheer power at catching everything we could throw at them that makes them our choice for **Most Powerful Anti-virus Solution Award**

F-Secure Internet Security 2013 Review

Cyber Defense Test Labs Review:

F-SECURE INTERNET SECURITY 2013

Introduction

Cyber Defense Magazine (CDM) launched the Cyber Defense Test Labs (CDTL) to test and highlight some of the lesser known anti-virus players and next generation anti-malware solutions on the market. While some are significant in size, like F-Secure, they remain lesser known brands like Symantec and McAfee, yet their products outperform and outshine these bigger brands. What we like most about F-Secure is how easy the product installs, how quickly it runs and how little 'footprint' it takes during scanning and malware blocking operations. Please read on and learn more about F-Secure in their award winning product review.

Company Snapshot

One of the longest standing anti-virus companies, who has consistently built a solid product suite is F-Secure, which was founded in 1988. They are a privately held company but have been listed on NASDAQ QMX Helsinki Ltd. since 1999. Their headquarters are in Helsinki, Finland. They have offices in the USA, Finland, Belgium, Poland Denmark, Italy, Germany, France, Spain, The Netherlands, Norway, Brazil, Malaysia, Australia, Hong Kong, India, Japan and in Singapore with almost 1,000 employees. Even during a very difficult global economic meltdown, their revenues have continued to grow in the double digits, reaching almost 40m USD by Q2 of 2012 with significant positive cash flow of a healthy, positive 6.7m USD.

Customer Service

F-Secure has a strong customer service offering as one of the more mature players in the industry. They offer customer service by phone, email, chat and Community forum. Customer Service varies by country. They have phone support in 16 different countries and English support available for other countries. For example in the USA they offer 24/7 support including phone, chat and email. Resellers and partners have their own partner support. We found a very detailed table for country specific support by phone here:

http://www.f-secure.com/en/web/business_global/support/contact/call-f-secure-support

For business customers the local reseller or service partner is always the first line of contact.

Customer References

While they don't offer big brand name customer references, for stated security reasons, F-Secure has a nice page on some case studies they have done:

http://www.f-secure.com/en/web/business_global/references/case-studies

Malware Database, Updates, Scanning and Blocking

F-Secure has a comprehensive, malware sample collection database contains over 100 million unique samples. Online engine is utilizing this database for detections and the database is stored in the cloud. Local signature database consists of some millions of signatures which contains also heuristic and generic detections. A heuristic and generic detection can detect from hundreds to hundreds of thousands of unique samples.

"One of the longest standing anti-virus companies, who has consistently built a solid product suite is F-Secure, which was founded in 1988."

While their Cloud database is updated every few seconds. Local signature databases are updated at least three times per day but often updates happen more frequently when important detections are released due to increased threat activity. F-Secure has dedicated people and automation that looks for new and unseen malware that is used and distributed in the wild. In addition to this we get samples from our customers and from trusted partners.

F-Secure has been making their own AVS scanners for years plus they made a smart decision to OEM the Bitdefender scanner, as well, which helped boost them in our tests to extremely high detection and block rating, one of our highest ever. Their scanners are named, Aquarius, Hydra, Gemini, Deep Guard and Online. Only Aquarius comes from Bitdefender. Their Windows client products use these engines: Aquarius, Hydra, Gemini, Deep Guard, Online, while Windows server products use these engines: Aquarius, Hydra, Gemini, Deep Guard. Their Linux products use these engines: Aquarius and Hydra, Mac products use this engine:

F-Secure Internet Security 2013 Review

> "Their Deep Guard engine is one of the strongest HIPs engines on the market. They were one of the first to leverage reputation data to provide protection against malware."

Hydra, Android Mobile products use these engines: Hydra, Online and other Mobile products use this engine: Hydra.. They have both signature and heuristics malware detection capabilities. Their HIPS engine is called Deep Guard. Deep Guard monitors the behavior of samples while they are being executed and utilizes both file reputation data and malicious patterns in its detections. Deep Guard is designed to be user friendly and it will bother the user only when malware is being detected.

Zero-day Malware Detection and Blocking

F-Secure suggests using a combination of multiple engines and layered protection to catch and block new malware. F-Secure solutions utilize heuristic, behavioral and reputation based detections that can and will detect zero-day malware. Also, F-Secure solutions scan possible attack patterns in multiple layers starting from network traffic all the way to the point when an application is being executed. At Cyber Defense Test Labs we have no qualms about other competitive test labs. We think the more testing the better so we're happy to say that F-Secure has also been tested by other independent and professional AV test labs including AV-Test and AV-Comparatives, among others.

Dealing with False Positives - Rare Occurrences

In rare occasions, F-Secure has blocked an application which is not truly malware (but behaves in a similar fashion to malware) such as Microsoft's Instant Messenger and SKYPE which will roam firewall ports looking for ways out, move traffic without user permission and perform file transfers, some of which end up including malware which exploit operating system vulnerabilities such as jpeg rendering flaws. While blocking these file transfers is not a false positive, some users will want to enable Microsoft IM or SKYPE, knowing that they are not behaving properly.

F-Secure has taken this into account and in addition, they always release a cloud based whitelisting first before local database signatures are released. This allows them to quickly provide a resolution for a false positive, literally in a matter of seconds.

ınnovation, Uniqueness and Next Generation

While F-Secure has been around for a long time, they continue to stay on the top both in price, performance and ease of use. This is attributed to a creative executive team that is always embracing change and challenges. Their Deep Guard engine is one of the strongest HIPs engines on the market. They were one of the first to leverage reputation data to provide protection against malware, which by the way, Symantec has recently done to improve their scores over McAfee and others. This just goes to show you that F-Secure is an innovator that competition considers worthy of following.

While they continue to innovate with Mobile Security offerings, they also plan to add additional levels of protection against new exploits in their corporate service portfolio offerings.

Free Trials, Platforms, Pricing and Availability

F-Secure offers free trials of their consumer, enterprise and mobile platforms as well as some free tools. We love free tools, although the hyperlink is subject to change, here is where you will find F-Secure's free tools:

http://www.f-secure.com/en/web/home_us/free-tools

Their solutions run on Windows PC and Servers, Mac, Linux, Android, Windows mobile, Symbian, Blackberry, and Apple's iOS. While they won't publish pricing, they use a channel-based sales model so you can find pricing online at one of their many resellers covering your region.

Product Effectiveness:	ê ê ê ê ê
Customer Support:	ê ê ê ê ê
Platforms and Pricing:	ê ê ê ê ê
Installation and Documentation:	ê ê ê ê ê
User Interface and Ease of Use:	ê ê ê ê ê

Overall Rating: ê ê ê ê ê

Summary

For their consistent product quality, frequent innovations and powerful host-based intrusion prevention engine, coupled with their reputaton-based protection capabilities, with ability to stop most zero-day malware, we give them our **Most Comprehensive Anti-virus Solution Award for 2013.**

Avast! Free Version 7.0 Review

Cyber Defense Test Labs Review:

AVAST! FREE VERSION 7.0

Introduction

Cyber Defense Magazine (CDM) launched the Cyber Defense Test Labs (CDTL) to test and highlight some of the lesser known anti-virus players and next generation anti-malware solutions on the market. While some are less significant in size, like Avast!, they remain lesser known brands like Symantec and McAfee, yet their products outperform and outshine these bigger brands and their deployments are global.

What we like most about Avast! is that it is a free, lightweight, easy to install and use, anti-malware solution that is available in more than 42 languages and able to detect and block all the malware we could throw at it. Please read on and learn more about Avast! in their award winning product review.

Company Snapshot

Avast! was founded in 1991 by two entrepreneurs and private owners, Eduard Ku?era and Pavel Baudiš, continues to be privately held and with over 240 employees, has offices in Prague, Austria, Germany and the USA. The Avast! headquarters are located in Prague. Avast! has 162 million active users and claims, because of their always free version, to have the world's largest install base. They have been tested elsewhere as well by many respected labs including the VB100 by VirusBulletin and the Advanced+ rating they received from AV Comparatives. If you checkout their free download at CNET's download.com, you'll see they receive 4 and 5 star ratings consistently from user reviews and have over 2m Facebook fans. We found the full list of these here: http://www.avast.com/awards-certifications

> "Avast! has 162 million active users and claims, because of their always free version, to have the world's largest install base."

Customer Service

Avast! has grown creatively or should we say 'virally' by these reviews, social media, free downloads and word of mouth. With a simple, clean and easy to use graphical user interface (GUI), the need for user support is minimal. However, they offer a support forum and for their paid version, they train their resellers who then offer support for them, plus they have recently added Free Phone Support:

http://www.avast.com/en-us/support

For business customers the local reseller is the recommended first line of contact but Avast! is very flexible in providing support and solving problems.

Customer References

Avast! does not provide customer references, however, they recommend potential customers read the reviews of users at Download.com and join their Facebook page.

Malware Database, Updates, Scanning and Blocking

Avast! has their own scanning engine. They developed it themselves to be low-bandwidth and function in the traditional signature detection model with a little bit of heuristics to run more efficiently, based on more than 150,000 unique incoming samples they receive each day.

Avast! updates their malware database at least twice a day but will serve up to twenty to thirty streaming updates with fresh detection. They actually call this their new Streaming Updates feature and it does keep them one step ahead of most threats, without the user having to worry about checking to see if they have the latest

Avast! Free Version 7.0 Review

> "What we like most about Avast! is that it is a free, lightweight, easy to install and use, anti-malware solution that is available in more than 42 languages."

software or database running.

Avast! gets their samples for review, testing and updates from more than 40 different sources including their own CommunityIQ feature as well as other anti-virus vendors, security organizations and malware enthusiasts.

The Avast! scanning engine uses a layered approach to catch and stop malware. Statical analysis comes in the first place - the code is analyzed and stopped when malicious markers are found. Avast! also test samples at their own controlled malware lab environment once it has been classified as suspicious by the statical analysis.

That's the second layer where they analyze the isolated activity performed by the executable - without any changes to the system itself. The sample is stopped from running once Avast! decide it's malicious. The last level is their behavioral shield that monitors suspicious changes to the system and suspicious activities.

Zero-day Malware Detection and Blocking

In addition to the methods described above, Avast! has a File Reputation module which enables them to detect and block Zero-day malware, ie, previously unseen samples.

Dealing with False Positives - Rare Occurrences

To ensure reduced false positives, they constantly run tests against a huge set of clean files so they can spot any major false positives before releasing an update through the Streaming Updates feed.

In the event a false positive does happen, Avast! leverages the CommunityIQ, their internal testing and their Stream Updates to resolve it quickly, most likely without end-users even noticing.

Innovation, Uniqueness and Next Generation

In addition to a wonderful, pure play free anti-virus product, Avast! offers consumer and business versions for reasonable pricing that offer many more features such as Remote, Sandbox, SafeZone, Firewall and Anti-spam add on features.

The Pro version includes the anti-virus engine, Remote, Sandbox and SafeZone, while the Internet Security is their complete suite edition which also includes Firewall and Anti-spam features.

The Remote feature is similar to only one other in our test suite, known as Geekbuddy, however you can have your own friend help you with the Remote remediation process or resellers can offer this to their customers. It's a great way to reduce end-user support overhead.

Free Trials, Platforms, Pricing and Availability

Avast! does offer a 30 day free trial of their paid products and the free version is free with no strings attached. To grab your copy of their latest free version and free trials of paid versions, please visit:

http://www.avast.com/en-us/download-software

They run on Windows, Apple's OSX platform and the Android OS. Pricing for Pro is $39.99 USD and Internet Security is $49.99 for one PC for a one year subscription.

Product Effectiveness:	ê ê ê ê ê
Customer Support:	ê ê ê ê ê
Platforms and Pricing:	ê ê ê ê ê
Installation and Documentation:	ê ê ê ê ê
User Interface and Ease of Use:	ê ê ê ê ê

Overall Rating: ê ê ê ê ê

Summary

Avast! Free Version 7.0 is easy to install, easy to use and requires very little bandwidth. It's one of the most lightweight products we've tested.

For being a great free product, lightweight, easy to install and use, available in more than 42 languages and able to detect and block all the malware we could throw at it, we give Avast! Free Version 7.0 our **Best Free Anti-virus Product Award for 2013.**

DO YOU KNOW WHO IS ON YOUR NETWORK?

WE DO.

(Well, actually it's our award winning Network Access Control solutions that do.)

Want to gain control over the BYOD dilemma in a matter of minutes?

www.netclarity.net

email: sales@netclarity.net

Call: 1-800-874-2133, Option #2 for a FREE trial

IT'S IDENTITY, STUPID

.id

Photo courtesy of Brian Snow,
Senior Technical Director, NSA.gov (Retired)

By Richard Thieme

We know that identity is a critical issue for security practitioners, but have we really grasped that identity has become THE existential issue for life in the early 21st century?

Academics write scholarly tomes on morphing personas and juggling online personalities;

counter-cultural spokesfolk like Jacob Applebaum in his 29C3 keynote articulate a perceived need for learning how to erase tracks that linger in the snows of cyberspace; traffic analysis and those from whom and to whom the traffic moves requires more and more storage, faster and faster processing.

But it's deeper than that.

The fact is, we live among a multiplicity of nested identities that are linked and simultaneously morphing, identities that we determine at the comment of both contemplation and action because the decisions we make about being and thinking and doing determine the clusters of thoughts and actions that in turn determine HOW WE ARE PERCEIVED by Others - and the other may be Big Brother, or one of many little brothers gathering, parsing and selling our data, or casual friends who interpret who they think we are unselfconsciously as they engage with our symbolic presence - also on the fly - and assume and presume us to be who they think we are (see: phishing).

"But it's worse than that."

Identity - from that of "the individual," a social construction, post-renaissance, post printing press - to the citizenship we reference as our primary source of being-in-the-world - is on the move. And because those levels are nested and linked, a change in one means a change in the others, the way pulling a side of a rhomboid on a computer monitor alters the area and the shape, yes, but above all, the relationships of the parts to each other and to the perceived whole. And it is relationships that determine the whole, even more than what is related. Relationships frame what we think we see, more than the things we thinn we see, and those who know this and achieve mastery and control over most behaviors in that regard, rule the identity space - which is now the space of offensive and defensive activities alike.

But it's worse than that.

Implicit ethical and moral dimensions emerge from new social and cultural structures as a result of ongoing technological transformations, so any discussion of ethics - that is, the right or appropriate behavior in any given context - in relationship to the implementation of new technologies, must take into account these multiple dimensions. The philosophical and religious systems that permeate society are also undergoing transformation, which means that prior paradigms have become chaotic seas of uncorrelated data in transitional cognitive spaces. The frames in which emergent properties, new patterns of data, and new emergent selves - beyond "individuality" - all live and move and have their being, are not yet clear, nor do they have names we can use as if we all mean the same things by our words. We still call these vehicles for self-expression "horseless carriages," as it were, using terms that are fading from sight, and have not yet found a way to talk about "driving" and "automobiles."
All this is most evident in the world of security and professional intelligence.

Post WorldWar II, R&D in the intelligence community and military spheres have shared responsibility for creating technological engines that have transformed human identity and therefore the Kuhnian paradigm in which we frame possibilities for action. Action means options, and options mean ethics. (As I said, I define "ethics" as options that are most congruent with our core notions of identity, self, integrity, and "the right thing to do.")

Definitions of everyday reality-privacy, security - continue to be transformed by technologies of surveillance, information, and communication. Those technologies are invisible frames because we live inside the picture, so if we define ethical issues in the context created by prior technologies then we derive familiar recognizable and comforting concepts as a result, but ones that no longer fit the real-life context created by new technologies. Our ethical decisions are inauthentic. We deceive others, yes, but first we deceive ourselves. That is the heart of the problem.

Between times, we live in the fog of war. In a world which posits terrorists (i.e., enemies of social and economic order) as the Other, the mind of society is the battlefield. Images and ideas are the primary weapons, and the means by which they come into being and move through human networks is the subtext of all security. The paradigms we use determine the questions we are capable of thinking and asking. The formulation of relevant questions may be more important than the answers.

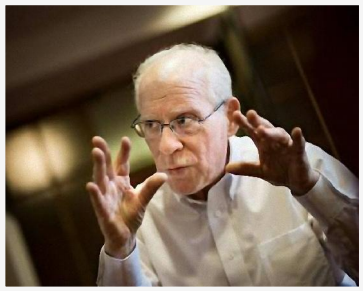
Let me highlight a few key concepts:

(1) Information security as one task, both offensive and defensive, of the intelligence community sanctions breaking foreign laws while prohibiting similar activities on American soil. We have no friends or allies "out there," only targets (and maybe "in here," too). But simple distinctions of "foreign" and "domestic" no longer hold. The convergence of enabling technologies of intrusion, interception, and panoptic reach, combined with a sense of urgency about the counterterror imperative and a clear mandate from our leaders to do everything possible to defeat an amorphous non-state entity defined by behaviors rather than boundaries, borders, or even a clear ideological allegiance, has created an ominous but invisible set of conditions that undermine the previous cornerstones of law, ethics, and even religious traditions.

(2) Identity is a function of boundaries. An "individual self" defined by a boundary around biological processes and the complex of energy and information radiated by those processes is undermined by the erosion of those boundaries by the use of connective technologies.

(3) Security, privacy, and intelligence gathering are corollaries of individual and national identities and how they relate to one another.

(4) Security is a function of boundaries. Boundaries define the "other" that threatens "us" and "us" is a felt experience of clan, tribal, and societal kinship still. Prior to the emergence of writing and the religions it facilitated, the "enemy" was the "Other." Ancient societies defined enemies as non-members of our tribe. After writing, the enemy became - e.g. in Christianity- that in ourselves which must be fought, resisted, or transcended. This shift in consciousness was a result of emergent technologies of writing.



(5) When the enemy is "within" the body politic, defined as an element that threatens societal order and economic well-being, defined no longer as a nation-state that threatens our political existence as a nation state, then the distinction between criminals and terrorists or religious/political dissenters and supporters of terrorism blurs. Accordingly the tools considered appropriate to their identification and neutralization will blur.

We continue to speak of ethical norms in relationship to the cultural past as if it is still the context of our beliefs and actions. We speak of individuals as primary moral agents. We speak of nation states as primary determinants of our collective identities. We speak of the intelligence mission as if "we" who live inside one nation are intercepting or penetrating or subverting the technical processes and social dynamics of others who are also "inside" the boundary of a nation state that defines them.

Those distinctions no longer hold.

“ We continue to speak of ethical norms in relationship to the cultural past as if it is still the context of our beliefs and actions. ”

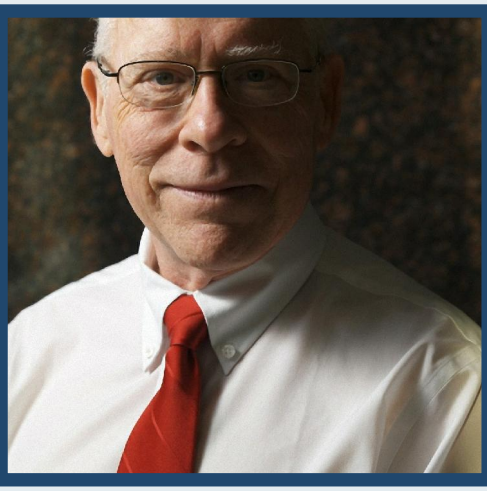
(6) Current technologies make speaking of interception obsolete. Boundaries between elements of the network, between the networks that make up the network, are arbitrary and porous. We live in a world without walls. Every attribute of a process or structure that broadcasts or transmits information about itself by any means can be detected, often at the source. Often enough, those who built the system in the first place engineer information to come to them. "Here" and "there" are distinctions without a difference.

“Our identities exist as potentialities made actual by our intention at the moment of action. They are the equivalent of quantum states, fixed only when expressed.”

(7) Identity at a fundamental level is therefore transformed. Digital identities can be appropriated, yes, but more than that, we invent them on the fly and determine at the moment of thought or action or execution to which matrix of equally transitory and transitional attributes we are related as a node in the network. Our identities exist as potentialities made actual by our intention at the moment of action. They are the equivalent of quantum states, fixed only when expressed.

Identity in relationship to security is a matter of observation and not assertion. Only multi-level observation penetrates the skin sufficiently to reach the meta-level determined by actions which may support or contradict identity-assertions.

(8) As boundaries go liquid, the task of defining appropriate behaviors in relationship to moral norms becomes difficult because the phrase "moral norms" is a metaphor for the context that is generally invisible to members of a society but not to sophisticated security professionals, an elite sanctioned to manipulate those underlying norms on behalf of ends considered important enough to justify a variety of means to achieve them.



ABOUT THE AUTHOR

Richard Thieme (www.thiemeworks.com) is an author and professional speaker focused on the deeper implications of technology, religion, and science for twenty-first century life. He has published hundreds of articles, dozens of short stories, three books with more coming, and has delivered over one thousand speeches. A novel, FOAM, is in progress and A Richard Thieme Reader, collecting fiction and non-fiction, interviews and book reviews, will be published in 2013.

He speaks professionally about the challenges posed by new technologies and the future and how to reinvent ourselves to meet them. Clients range from GE, Medtronic, and Microsoft to the NSA, FBI, and US Secret Service, plus dozens of security and hacker conferences including 17 years at Def Con & Black Hat.

He has keynoted conferences in Sydney & Brisbane, Wellington & Auckland, Dublin, Berlin, & Heidelberg, Amsterdam Rotterdam & The Hague, Dubai & Kuala Lumpur, Eilat Israel, Johannesburg SA and Lodz (Poland), and all over Canada & the USA.

Therefore:

Security professionals exercise an implicit, de facto thought leadership because they create structures that bind and inform society and civilization. They create frames of human behavior that determine how we think about ourselves as possibilities for action. Their real implicit charge is no longer "to defend and protect a nation" but to stabilize a world.

The dire possibility of societal disintegration elevates the moral responsibility of the security and intelligence communities to a higher level. Linked in cooperative activity, they are responsible for maintaining social and global order at a level of understanding far beyond that formulated in the past by any one nation. These communities in the aggregate constitute a global community of practitioners who share an ethos and modalities of operation not available to ordinary citizens; they have thereby created for themselves an intrinsic vocation or calling to maintain global order in a way that is consistent with the ethical norms and moral order articulated by the great cultural traditions even as those traditions are also transformed by diverse technologies-and even though they and we recognize that in practice that moral order and those ethical norms are often violated as a matter of practice.

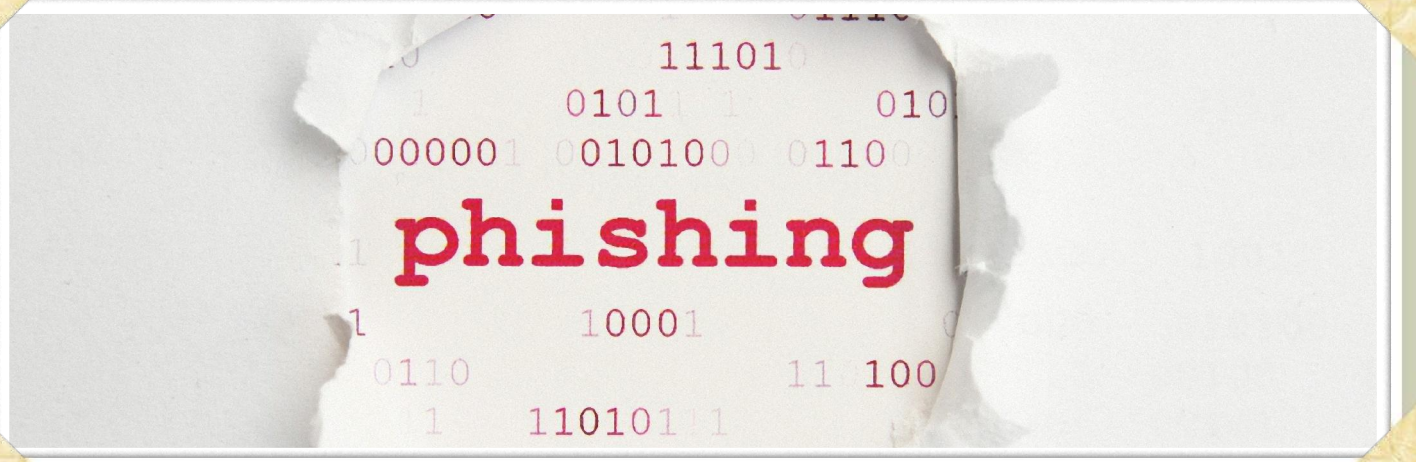
Well, this is but the beginning of a conversation. No one said it would be easy, did they?

“Security professionals exercise an implicit, de facto thought leadership because they create structures that bind and inform society and civilization. They create frames of human behavior that determine how we think about ourselves as possibilities for action. Their real implicit charge is no longer "to defend and protect a nation" but to stabilize a world.”

Welcome to the frontline…

www.nationalccdc.org

CIAS



Reasonable Suspicion - Best Practices for Recognizing Phishing

by Aaron Higbee, PhishMe CTO

With phishing attacks constantly evolving and taking on more sophisticated forms, making sure employees can recognize and react appropriately to threats is of increasing importance. But what can you do to ensure employees are prepared for the moment when a phishing email arrives in their inbox? PhishMe CTO Aaron Higbee has identified best practices that employees should follow to avoid being snared by a phishing attack.

Keep Your Emotions in Check

Many phishing scams will attempt to elicit an emotion from the reader. As we all know, when our emotions are high we tend to do things we normally wouldn't, like click on an unknown URL. Some of the most effective phishing emails are ones that take an authoritative tone to threaten the user with unwanted consequences. For instance, an email may pose as the IT department and command a user to reset password and login information, threatening to lock the user's account unless that information is entered by a certain deadline. A legitimate IT department will never ask for you login information, so don't allow the perceived threat of account lockout bait you in to revealing your information.

Phishers also try to tempt us. Yes, we would all love to win an all-expenses paid vacation simply by clicking a link, but the old adage that if something seems too good to be true, it probably is, applies here. Be wary of any email promising you something. Don't let your emotions get the better of you. Learn to recognize, and be suspicious, when an email is trying to evoke emotions such as fear, curiosity, or urgency.

Best-practices for recognizing:

Phishing

Don’t get snared!

Paranoia, within reason, is a good thing

Learning when to be suspicious of email is an important element of effectively preventing phishing attacks. Chances are you get a lot of email through the day. Understanding that reporting suspicious email is critical to the defense of your organization, you want to make smart decisions about what is reasonable to report and what is probably benign. When you examine the email in your inbox much of it is ongoing conversational threads or emails that you were otherwise expecting. It's the small percentage of unexpected or unsolicited emails that you need to be wary of. For instance, you just attended a project planning meeting where the coordinator told everyone at the end of the meeting, "I'm going to email out notes from the meeting" and within the hour you get a notes.docx.zip attachment from that person, open it! On the flipside if you get a notes.docx.zip claiming to be meeting notes for a meeting you didn't attend, be suspicious. Report it.

A reasonable level of paranoia is appropriate for dealing with links in emails too. Whenever possible, type URLs into your browser rather than following links in emails. If you do follow a link, double-check and make sure you know where it's going before clicking. Hovering over a link allows you to see the path it will follow, and a common trick phishers use to disguise malicious links is to prefix them with a legitimate web address (e.g., google.com/maliciousssite). Get in the habit of reading links from right to left to distinguish between safe and unsafe links. If you can't identify a link, don't follow it!

Respect the Program

Most companies have IT security programs in place, so follow them! First off, don't uninstall or tamper with organizational security software, and don't go around security controls, rather, ask for help or file for an exception.

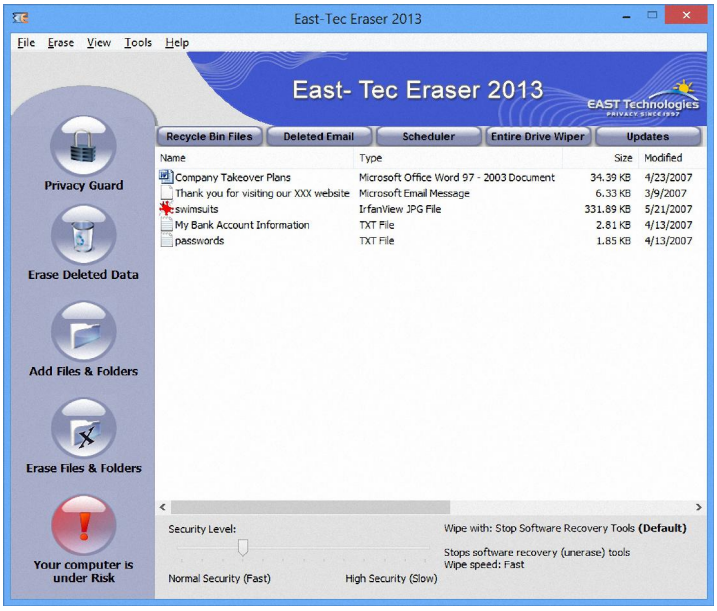
Although there are security controls in place, don't assume that they will prevent all malicious emails from making it to your inbox. If you receive a suspicious email, follow your organization's process and report it to the proper authority. Even more importantly, if you think you may have fallen for a phishing scam, report it immediately, as a swift response to a phishing infiltration can significantly reduce the adverse impact on an enterprise.

Preparing employees to react properly to phishing emails may seem daunting, but raising awareness and training employees to follow these best practices is a relatively simple way to reduce your organization's risk of being exploited through a phishing attack.

About The Author

Aaron is the Co-Founder and CTO of PhishMe, Inc. directing all aspects of development and research that drives the feature set of this market leading solution. Before PhishMe and Intrepidus Group, Aaron served as Principal Consultant for McAfee's Foundstone division where he was a lead instructor and known for his ability to mentor and develop junior consultants into expert penetration testers. Prior to his seven years of consulting experience, Aaron's biggest achievement is building industry recognized Intrepidus Group and incubating PhishMe out of it. His creative touch is evident in the unique way he recruits and retains talent and his style further extends itself into his leadership role at PhishMe. Aaron is a speaker at regional conferences and associations as well large conferences such as BlackHat, DefCon, Shmoocon, etc. His expert opinion is a valuable resource for many media outlets interested in security.

EAST Technologies: East-Tec Eraser 2013



Protects Your Privacy and Identity

East-Tec Eraser 2013 completely destroys information stored without your knowledge or approval: Internet history, Web pages and pictures from sites visited on the Internet, unwanted cookies, chatroom conversations, deleted e-mail messages and files, temporary files, the Windows swap file, the Recycle Bin, etc.

Real Deletion

Normal deletion is not secure: when you delete a file, its contents and information about it remain on disk. East-Tec Eraser 2013 makes sure deleted files are really deleted, so that previously deleted files like valuable corporate trade secrets, business plans, personal files, photos or confidential letters will not fall into the wrong hands.

Cleans Your Favorite Browsers

East-Tec Eraser 2013 works with all your favorite browsers (Internet Explorer, Mozilla Firefox, Google Chrome, America Online, MSN Explorer, Opera, Safari, Netscape Navigator) and securely deletes all your Internet history, visited web pages and images (Temporary Internet Files or cache), address bar locations, unwanted cookies, and more.

Cleans Your Favorite Programs

East-Tec Eraser 2013 cleans Yahoo Messenger, MSN Messenger, AOL Messenger, ICQ, Outlook and Outlook Express, Mozilla Thunderbird, Eudora, Limewire, Morpheus, Kazaa, Windows Media Player, RealPlayer, Winamp, Google Toolbar, Microsoft Office, Norton Antivirus, ZoneAlarm, WinZip, WinRar, Download Accelerator, and many more.

Improves System Performance

East-Tec Eraser 2013 speeds up your computer and programs, deletes thousands of unnecessary and temporary files and frees up a lot of valuable disk space.

Permanent Erasing

East-Tec Eraser 2013 meets and exceeds government and industry standards for the permanent erasure of digital information, Russian and German security standards, and industry standards like the Bruce Schneier Algorithm or the Peter Gutmann Method.

Automatic Protection

You can set East-Tec Eraser 2013 to automatically clean your computer at specified intervals, like when you close your Internet browser, when the computer is not used, at a certain date and time, once a day, or you can set longer cleaning operations to run once a week.

Entire Drive Wiper

East-Tec Eraser 2013 can securely erase entire CD/DVD disks, USB drives or hard disk drives with all files and folders. Use this option if you share, give away or sell disks to other people and you don't want them to see what data you used to have on those disks.

The Anti-Surprise (Anti-Boss or Panic) Key

Automatically close all open windows and immediately run East-Tec Eraser 2013 with preselected options (e.g. erase your Internet traces in stealth mode) with just a combination of keys. Use it in emergency situations to protect your privacy.

Very Easy to Use

East-Tec Eraser 2013 has an intuitive interface and wizards that guide you through all the necessary steps required to protect yourself. You can also erase files and folders with one click directly from Windows, or drag and drop them in East-Tec Eraser 2013.

Flexible and Personalized Protection

East-Tec Eraser 2013 fully supports your personal privacy needs and allows you to define your own sensitive information, cookies you approve and want to keep, and even your own erase methods.

Advanced Features for Professional Use

East-Tec Eraser 2013 features running in stealth mode completely invisible to the user, preventing specific data from being erased based on filters, granting different permissions to users, password protection, processor usage priority settings, command line parameters to allow advanced automation or running from batch files, etc.

Cyber Defense Magazine Exclusive:

Free copies of last year's edition can be found here:
http://customer.east-tec.com/transfer/press/cdm/etecdm.exe

Then, CDM readers can register here:
http://offers.east-tec.com/cdm/2013/eraser/

then, you will receive a one time discount for 2013 edition.

Meeting the Application Security Requirements of PCI-DSS (Payment Card Industry Data Security Standard)

Challenges with Application Security and PCI

Let's talk about Application Security and PCI. I've got three agenda items to discuss in this article, however, the second one in particular is quite meaty and we're going to go rather deep into five of the 12 requirements:

1. The challenges of application security in general
2. Requirements 3, 4, 6, 11, and 12, how they relate to application security (along the way I'll discuss not only how they relate, but also what you can do to make sure that your development teams understand those requirements and know the actionable steps they need to take in order to comply.)
3. Integrating PCI requirements and software development best practices into your software development lifecycle.

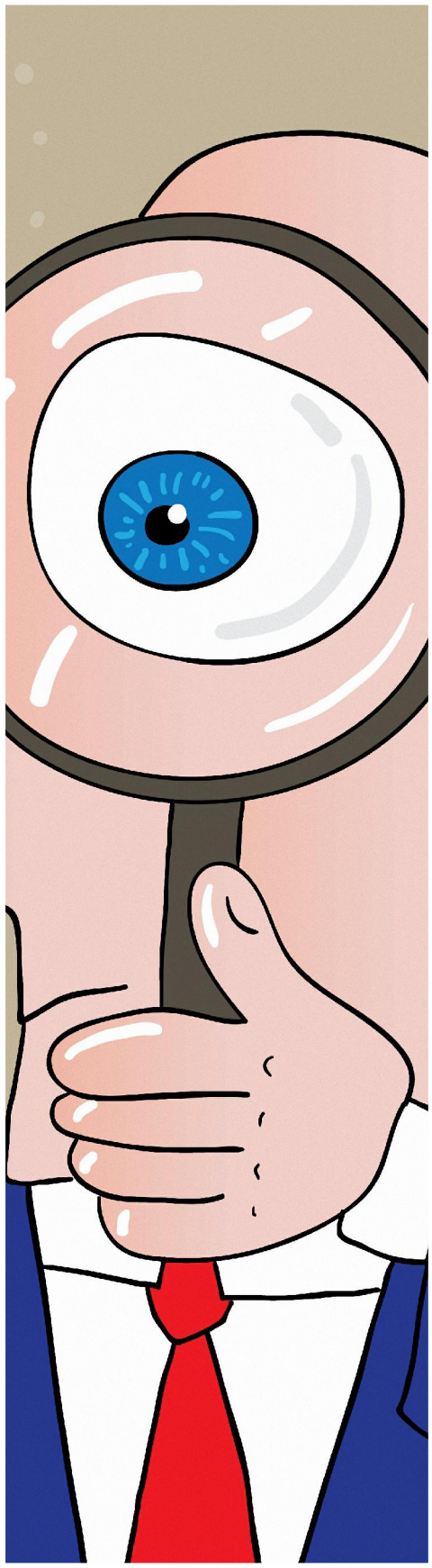
And thus we begin, starting with application security requirements of the payment card industry data security standards. Now a lot of organizations do tend to struggle with this, and for good reason. First of all, the PCI-DSS, in my opinion, is one of the best standards out there. It is more prescriptive than any other security standard I can think of. However, there is still a lot of genericism that has crept into those twelve requirements. Even in the testing procedures - now, for those of you not familiar with the PCI DSS, there are generally three columns for each of the twelve requirements:

- The first is just what the requirement states.
- The next column goes a little bit deeper and explains some rationale behind it, and
- The last column talks about testing procedures: how you can validate whether or not you're complying with the standard.

So you get the "what", the "why", and then the "how". Unfortunately, even the "how" is often very generic. The second reason that application security requirements in PCI DSS tend to be a little bit hairy is, the standard was written by security professionals, for security professionals. Yet, three out of the twelve address application security specifically, and as you'll see in this article, five out of the twelve have quite direct implications for software developers. In a couple of paragraphs below you'll see some data from The Ponemon Institute that supports the fact that software development teams and Information Security teams usually don't see eye to eye. The requirements of the PCI can also be remarkably general, e.g., "you must protect cardholder data". Well duh! That's what the whole standard is about! But what you really need to deliver to your software developers is: what does that mean to them? And how do they protect cardholder data in their specific role? And we're going to get into that in quite a lot of detail a little bit later on. You've also got requirements in the PCI-DSS that state, "develop software applications according to industry best practice." Well great, but what is "industry best practice"? In some instances, the PCI DSS does give specific examples; it'll call out things like OWASP top Ten, and CWE from MITRE. Very good stuff. However, a couple of requirements just stop at "industry best practice". And of course, if you go looking for industry best practices on the Internet (as an example search for "Cross Site Scripting" which is one of the vulnerabilities which the PCI DSS says you need to code to defend against) you end up with about 4,850,000 results. Which one of those are you going to take a look at? Maybe the first, and maybe the second, but most of those are probably just wiki entries that explain what cross site scripting is but contain nothing prescriptive that a developer can take as actionable.

Let's consider some additional reasons why application security is so challenging in PCI DSS. Security teams (which for the sake of this paper include IT risk teams, compliance teams, enterprise risk management teams, governance teams, and the like) typically speak in terms of risk, and use terms like "vulnerabilities" and "business continuity." None of those terms exist in the software development world. Software developers think in terms of bugs, defects, features, functions, and due dates. The two groups have very different languages they speak. And historically, most IT security standards and regulations are focused on network and endpoint security, which makes sense. Install and configure firewalls, make sure antivirus is turned on and up to date, install the latest patches on your laptop and your mobile phone. That's all great, but when you start to introduce application security, you're now entering into the world of software development. And software development and IT security - specifically network and endpoint security - are two very different worlds.

> *And all those nasty data breaches from 2011 that hit Sony, Lockheed Martin, RSA, and others? Well over 90% of them exploited software vulnerabilities.*



According to Forrester's "State of Application Security" report in 2011, attackers recognize that software applications are where sensitive data is most vulnerable, and that's where they're attacking. Quoting the report directly, "Today, the "money" is in software applications - that's where companies process their most sensitive data from credit card numbers to customer and employee information as well as trade secrets." And all those nasty data breaches from 2011 that hit Sony, Lockheed Martin, RSA, and others? Well over 90% of them exploited software vulnerabilities. Earlier I mentioned the Ponemon Institute and some research they had done. Earlier this year, they published the "Application Security Maturity" research report, in which they asked a bunch of very interesting questions. The samples went out to something like ten or twelve thousand individuals, and they asked the same questions of InfoSec teams and software development teams in the same organizations. One of the questions that they asked was around collaboration between the two groups. If you look at the PCI DSS you would think "there's got to be some collaboration because at least three - and (as we're going to see) five out of the twelve requirements have direct implications for application security. There's got to be some collaboration, right? Well, not so much. 43% of security personnel said there was little or no collaboration, and in the development world, nearly 60% said there was little or no collaboration between the two teams. Some of these numbers are way too large, and should be a much much smaller number. And it's interesting to note the difference between the two numbers -a lot of this comes down to the fact that security teams will often generate a security policy which will have security controls. And those controls might relate to application security; yet, it's not nearly as thorough or sufficient or contextual to mean anything to a developer. So security personnel might think "sure, we've got a written policy and the policy states we have to build applications so they're not susceptible to the OWASP Top Ten - my job's done!" And of course developers look at that and say "well that's a very high level security requirement, it doesn't mean anything to me as a Java developer as I sit here on a Wednesday afternoon trying to hit my deadlines." Let's look at another question from the Ponemon survey. The next one asked about security being integrated into the software development lifecycle. Again, security personnel and developers were surveyed. What percentage stated that they had no process at all, or an inconsistent, ad hoc process for building security into software applications? Security personnel say 64%. Wow. Pretty big numbers. 64 percent of security professionals state there is no process for building security into their applications. What do you think of the development community? Nearly 80%! This is a very disturbing statistic, sitting here, at the end of 2012. 80% of developers surveyed still think there is no process or an inefficient ad-hoc process for building security into software applications. That is just woefully insufficient and once again, you notice the difference between security personnel and developers. More security folks think that there is a process for building security into their applications. Once again, a major difference of understanding here is related to the policy not providing contextual, actionable steps that developers need. Okay, we'll find out a little bit more later. Now let's get back to what we've been talking about which is PCI DSS. Most of you folks will recognize the six functional groups or control objectives. That is how the PCI DSS is organized, and then those six groups are further broken down into the twelve requirements. The twelve requirements are then further broken down into sub-requirements. But if you look at the groups:

- Build and maintain a secure network
- Protect cardholder data
- Regularly monitor and test networks, and
- Maintain an information security policy

That looks an awful lot like those good information security practices. And in fact, it is. It's really IT risk management, or Information Technology Risk Management, and that shouldn't be surprising, because

as I mentioned earlier, the PCI DSS was written for security professionals, by security professionals. And the fact that it's just specific to credit card information and payment transactions doesn't mean it's not a good information security framework. It is. And for most of the controls in PCI DSS, if you swap out "cardholder data" for "sensitive data" or "electronically protected healthcare information" you'll notice a lot of similarities between things like ISO 270x, HIPAA, and other security frameworks. One theme that you'll notice throughout this paper is that I recommend that you strive for repeatable, secure software development -- and you will achieve compliance along the way. Many organizations tackle this in reverse. They take a specific compliance mandate, like PCI DSS, and let that drive what they're doing or how they're measuring themselves with respect to security. Then they'll repeat the same thing for ISO and repeat the same thing for HIPPA, and it ends up becoming a lot of work, and a lot of redundant work; therefore, striving for repeatable, secure developments and security best practices, you will achieve compliance along the way, not to mention you'll be more efficient, you'll be able to develop software faster. A common misconception that it takes longer to write secure code than it does to write insecure code - not true! And also, you'll be able to gain leverage across multiple compliance frameworks. BUT, the place to start is ironically, the very last requirement in the PCI DSS, which is number twelve: Maintain an information security policy that addresses information security for all personnel. This is what drives everything else. Every single security control, every piece of developer guidance will be driven from your security policies. And pieces that are often overlooked are things like a policy that addresses security for ALL personnel. Now what this means in the PCI DSS framework, is all personnel that are in scope. That means anyone that is involved in the storage, transmission, or processing of credit card data. And if you build an application that is in scope, those developers are in scope. Now information security policies and awareness training that come with it have to be contextual - relevant to that group of software developers. If you delivered information security policy to a janitor, and you deliver the same one to a software developer, do you really think it is going to be equally understandable and actionable for both of their jobs? In most cases, the answer is no.

"...as I mentioned earlier, the PCI DSS was written for security professionals, by security professionals. And the fact that it's just specific to credit card information and payment transactions doesn't mean it's not a good information security framework. It is."

Understanding and meeting application security requirements in PCI DSS.

As I mentioned, we're going to be talking about 5 of the 12 requirements: #3, 4, 6, 11 and 12. In numerical order, not necessarily in order of importance. In fact if you know anything about PCI DSS, you realize that requirement six is very heavy with application security controls because it talks about building and maintaining secure system. So we'll start with requirement 3. Requirement 3 states "protect cardholder data". Very generic, but then we start to dive deeper. 3.2: "don't store sensitive authentication data after authorization." 3.3: "mask PAN data when displayed." PAN of course being information that's stored in mag strips in plastic credit cards, for example. 3.4: "render PAN data unreadable, anywhere it's stored." All right, well, again, fantastic security controls. However, when translating that to a developer, you've got to give them a bit more guidance. How do you make sure that you're not storing sensitive authentication data? Well, you have to make sure you're implementing cryptography correctly. And, not only that, you have to make sure you're following best practices for logging data in databases. And making sure that database encryption is turned on, and you have to sanitize input of users. When talking about masking PAN data, a developer can use techniques such as source code review to look for data in the form of PAN. This helps the developer identify all the places in code where data that looks like a PAN might be getting stored and/or encrypted. And there are plenty of good automated tools that can help with this, static analysis security test tools or whitebox testing tools, specifically, many of which have built-in PCI-DSS patterns to search against. In 3.4 - rendering PAN unreadable anywhere it is stored - things like hashing, truncation, strong cryptography, and good key management procedures are required. This is that next level of abstraction that a software development team needs. You don't need to give them information on how to implement, necessarily; but, the security controls in your policies need to be more explicit, as shown in the examples above.

Now let's talk about some good, bad, and ugly practices regarding 3.2, 3.3, and 3.4 . Efficient organizations, or organizations following best practices, are protecting cardholder data using encryption. They use higher order symmetric cryptography such as AES 256. Now we're talking about encrypting data at rest in requirement 3. Requirement 4 talks about encrypting data in transmission. So when you're talking about encrypting data at rest, you're talking about symmetric cryptography. Things like AES and use of hashes. You're not talking about public key crypto such as RSA and elliptic curve and Ntru. Another best practice that forward-thinking organizations use is enable database encryption. Any database worth its weight in salt has automated encryption that you can turn on for any data types. So do it and don't ignore the connection to the databases. What's that? Well, very commonly, data is encrypted in the database, but sent there in clear text by the application. Because software applications, when they are accessing and managing data, need to do so in unencrypted format, very often, a software

> *Good practice is encrypting sensitive data transmission EVERYWHERE - the PCI standard calls for transmission data being encrypted over open public networks.*

developer will open a direct path to a database, and send that data in there, allowing the database to do the encryption. Not a good practice; setting yourself up for man-in-the-middle attacks, and not leveraging best practices in application security. Also, using older hashes and algorithms. Technically you can use AES 128, no problem with that! However, when you've got 256 available, and you've got 192 available; they're stronger, they're better, when you're talking about storing data at rest, you don't really have to worry too much about performance, so using older but still approved hashed algorithms is not a good practice. Standards will catch up, but they'll always be behind the latest and greatest best practices; it's just the nature of standards. One of the ugliest examples -- writing your own crypto algorithms. Way too many times we've seen this; something that should not be done. Crypto algorithms are very tough to get right, and there's a lot of really good crypto algorithms out there! And they've been out there for 15 or 20 years, so use them! Another ugly practice is hanging on to that authentication data, storing it in a "safe place" for future transactions. Don't keep it! If you don't have to keep it, don't keep it. That is the rule of thumb when it comes to any PCI data, whether it's authentication data, cardholder data, PAN data: if you don't have to keep it, don't.

Next, requirement 4. Use strong cryptography.

This is talking about data in transmission. Now requirement 4 does talk directly about data across open public networks. 4.1 talks about strong cryptography and security protocols over open networks. 4.2 - never send unencrypted PANs by end-user messaging technologies like email and instant messaging. Well fine, again, the same types of techniques that you could apply for requirement three can apply for requirement four. Source code review, looking for PAN-type data. Any time you are transmitting, sending data outside of the bounds of that application, make sure it is encrypted. And now because you're talking about transmission, you are talking about public key, or asymmetric cryptography. You need to use RSA or Elliptic Curve or Ntru.

That gets us right into the Good, Bad, and the Ugly for requirement 4.

Good practice is encrypting sensitive data transmission EVERYWHERE - the PCI standard calls for transmission data being encrypted over open public networks. Just do it everywhere and you're safer; you also remove ambiguity as far as where and when to encrypt. This is one place where organizations get into trouble, because when you're selectively encrypting data, there's a lot more information to track, and a lot more potential attack vectors. More importantly, make sure you have requirements and design specifications for secure data transmissions. Developers are very good at implementing requirements; that's how they get measured, that's how they get paid. So if you put security requirements with respect to data transmission into the spec, and it will get implemented. And if it doesn't get implemented, you're forcing the developer to now go and seek out how to meet that requirement - that's what you want to do. Here's a bad practice: and this actually comes right out of the PCI DSS - it's one of their testing procedures. It's asking you to verify that "https" appears in the browser URL. That doesn't mean that SSL is implemented properly. In fact, if that's your testing procedure, you're really testing pretty lightly - that's not a verification. It's only verification that those five letters show in the url - very very easy to spoof that. Absolutely does not mean that SSL is being implemented properly. And the ugly practice - I am shocked that they even had to put into the standard "don't send the sensitive data over instant messaging chat." Why would you ever do that?! Its crazy, so don't do it. And also, another testing procedure: verify that only trusted keys and/or certificates are accepted. Oh great, it sounds wonderful. How do you do it? In fact, this is a very common man-in-the-middle attack that we conduct all the time for mobile applications or web applications because it's pretty easy to spoof things like certificates. It's a good control, however, you've got to make sure it's done properly. And this is one of those examples where you really need to provide the development team a lot more context than "do this".

Now let's talk about requirement 6. We're going to change it up a little bit in requirement six, because this is the one that goes really deep into application security. The top level requirement says develop and maintain secure systems and applications. Why? Because there are bad people out there, because many vulnerabilities can be fixed by vendor-provided patches, and because all systems should have all of these patches and be protected against exploitations by insiders and outsiders and viruses. Okay, great. Everyone agrees, yes, we should do it. What do we do, and how? And I'm going to jump to 6.2, which talks about establishing a process to identify newly discovered vulnerabilities. Great idea. How do they recommend doing it? How do they verify that it's done, how do they test? Well, the requirement states you should interview the responsible personnel to verify that the process is being implemented. It also states you need to verify the processes to identify new security vulnerabilities include the use of outside sources for security vulnerability information. What does that mean? Well first of all, that means that the internal auditor or the QSA needs to go ask the development team "Do you implement a process for identifying new security vulnerabilities?" "Do you have a risk rating for each one?" "Did you create this yourself, or are you using external sources to make sure that you've got multiple points of this risk-ranking and security vulnerability understanding?" That's the testing procedure. Again, the testing procedure here is pretty weak. Interview people? Really?! Very easy for someone to shake their head and say "Sure, yeah! We've got a risk-ranking process." A good organization documents their vulnerability management procedures. Let me see it! Document it! Vulnerability management procedures - they're not difficult to document, and the act of documenting it will force the development team to start thinking about security vulnerabilities, because most of them don't. You saw in the data

points of the Ponemon study earlier, developers think in terms of bugs, well, you know what, a security vulnerability is a bug, so integrate it into their defect management process. Vulnerability management is nothing different from defect management, and that's what you need to communicate to development organizations.

So what are some good external or outside resources for security vulnerability information?

There are quite a few, and I've named two of these already today. One is CWE, which stands from the Common Weakness Enumeration Project. Comes out of MITRE - it's a government-funded project with wonderful information that talks about weaknesses of software applications. And an organization near and dear to my heart, OWASP, or the Open Web Application Security Project - it's an open-source community of security professionals and developers around the planet. They generate projects and one of the projects is called the OWASP Top Ten, which lists the top ten risks to web applications. It used to be called vulnerabilities, they've since moved on - they're getting more of a business sense; I love it. Now they're talking about risk instead of vulnerabilities. Some bad practices: Using an automated tool's default risk ranking feature - almost every one will have one, too. I'm going to talk about AppScan Standard, a common web vulnerability scanning product from IBM Rational. Not because I love AppScan or I hate AppScan, but because it happens to be the one that popped into my head as I was writing this article. It's a fine tool, there are many different versions of it, source editions, standard, enterprise. AppScan, just like many tools, right out of the box will have a risk-ranking feature for vulnerabilities it discovers. Don't depend on it! Why? Because AppScan has no idea what a particular vulnerability means to your business. What you really need to do is understand what a particular vulnerability could mean in terms of business impact - not tracing that vulnerability to impact potential is a bad practice that we see repeated time and time again. Now what is an ugly practice here? An ugly practice is just getting caught in the madness of vulnerability management without taking time to analyze vulnerabilities and identify potential root causes. One of the biggest reasons and biggest costs that we see in an organization is the same vulnerability showing up in assessment after assessment after assessment, because the organization hasn't done its diligence in understanding what the root cause is and putting preventative measures in place. I can't tell you how many times that we run a consecutive scans or have done a manual assessment on the same application and keep finding the same vulnerabilities pop up. And that is the reason that's a practice you want to avoid - it's a huge cost and time tax.

Next is requirement 6.3 - one of my favorites!

Why is it my favorite? Because it mandates that you are to develop software applications based on "industry best practices" and incorporate security throughout the SDLC. Great! I would love it if this were actually implemented! However, as you saw from the two data points in the Ponemon Institute, 79% of developers don't think this is implemented! How can that be the case? So many organizations are required to comply with PCI DSS. Well, the reason it's not the case, is because so often, we think of it's on either just the development implementation phase of software development, or we stop at the very high level security control that says "build applications so they're not susceptible to OWASP Top Ten" and we think we're done. That is not integrating security through an SDLC. If you look at this chevron diagram below, you will see different phases of software development in green. Requirements, design, implementation, verification, release. This is no different than building a house or building a car. First you define what you're going to do, then you design it, then you build it, then you test it, then you release it, then off you go - and you maintain it. For every one of those phases, there are security activities that need to be done. And if your architect and business analyst and developer and QA professional and IT staff

don't know what they are, they won't get them done! Fortunately, there are lots of good sources of information, and much of it's free. Again, you can look to OWASP here, used by plenty of organizations around the world. They've got great cheat sheets and secure coding documents that can be used. DISA, which is the Defense Information Security Agency, they produce what's called a STIG, or a Software Technical Implementation Guide, that talks about developer awareness, but it's a very good and it has some good guidance on application security. I picked on AppScan in the last slide, so I'll give them some kudos here. AppScan and other tools, most of them will map findings to OWASP Top Ten, which is called out in the PCI DSS as a good framework to follow. I've mentioned CWE before. CERT also has some great coding standards. Microsoft has the SDL, which is the Secure Development Lifecycle. In fact, this chevron above is borrowed directly from the Microsoft SDL. And then there are also commercial offerings - things like Security Innovation's TeamMentor, which is a massive collection of secure coding checklists and code samples, but it's not just for developers. It's for the analysts who define requirements, the architects who design, the testers who verify, and the IT teams who manage those applications once they're in production. And oh, by the way, all of these activities, if you expect your teams to do them, you have to train them on how to do them. If you expect them to use tools to help automate, you have to train them on not just how to use the tools, but what the heck this tool does in the first place.

Let's talk about some good, bad, and ugly on Requirement 6.3. The testing procedures - code reviews according to secure coding guidelines. Great, sounds wonderful. Where can I get those secure coding guidelines? Again, go to OWASP, or look at TeamMentor. In fact there is a TeamMentor OWASP Edition, that is free and open source. So if you only have to worry about web applications, go grab it. Another testing procedure: examine written software development to verify that processes are based on industry standards and best practices, ensuring that information security is included throughout the lifecycle, and software applications are developed in accordance with PCI DSS. This "testing procedure" is nothing more than the requirements restated. Another example of how sometimes "verification procedures" can be relatively useless. You need actionable steps to take here. So let's look at some of the good, bad and the ugly of what organizations have done.

"Incorporate security at each phase of the SDLC." Technically, that is a requirement of PCI DSS. However, it's very often overlooked by QSAs or internal ISAs. It is a requirement - if you were to look at the PCI DSS requirements, by the letter, you need to incorporate security in every phase of the SDLC. Period. In black and white, it's very clear. It's not done and organizations typically are not held accountable for it … so they don't get hung up over it, which is a shame. Chances are the auditors (QSA, ISA) are security professionals who don't understand software development or application security. Therefore, it is easy for them to ignore requirements they don't fully understand or gloss over the testing procedures too lightly. Let's pick some bad activities - again, AppScan is back! This time showing its bad side. Thinking that using AppScan constitutes "industry best practice" is bad. It doesn't. Using any tool does not constitute "industry best practice". AppScan, like any other high quality (and it is a fine product) just helps you automate and scan for known vulnerabilities, and it doesn't catch them all. So over reliance on tools and gaining a false sense of security is definitely a "bad practice" you've got to watch out for. And here's the ugly. This goes back to the interview process, telling your QSAs "Sure we practice secure code. Don't worry about it!" Or taking your developer's word that a code review has been done. Show me! Document it! Code reviews have reports that get generated from them. Show it to me.

"Chances are the auditors (QSA, ISA) are security professionals who don't understand software development or application security. Therefore, it is easy for them to ignore requirements they don't fully understand or gloss over the testing procedures too lightly."

Requirement 6.5 - this is going to sound very familiar. Develop applications based on secure coding guidelines. It then further goes on to reference OWASP Top Ten. It used to do so specifically, now it does it indirectly. So you'll notice 6.5.1 is injection flaw, and they're asking you to code defensively to make sure that you're applications are not susceptible to injection flaws, particularly SQL injection. Then it goes on to talk about overflow vulnerabilities, and bad communication protocols, and a whole bunch of others that we'll get into. What I want to do here is talk about these vulnerabilities - I'm going to talk about several of them below - and talk about some best practices (one for each.) There are multiple ways that you can facilitate compliance for 6.5.x, with plenty of complicated controls, so I want to talk about a best practice for each one. And keep in mind as we're going through this what the testing procedures are for 6.5. The first one states that you are to verify that processes require training in secure coding techniques for developers based on industry best practice. Think about that. You're asking your development team to avoid SQL injection, cross-site scripting, and buffer overflows. How can they do that if they don't know what they are and how to code defensively? Can you expect that they're going to want to go out and source that information by themselves and learn all that stuff? You better not depend on that. Plenty of good developers will go ahead and do that, but you can't depend on it. In fact, most of the developers that we end up working with aren't exposed to the security controls or security compliance mandate of their organization at all.

So let's talk about some of these.

1. The first is injection, particularly SQL injection (and that's taken straight out of the PCI DSS). Well one great way to avoid SQL injection is to sanitize and validate any input. Basically you can't trust any input that a user gives you; you have to assume it's malicious. There's a lot more behind that, and we'll get to it in a couple of minutes, because once you decide to sanitize and validate input, a developer needs to determine, "how do I do that?" and "how do I do it in a specific language, such as ASP.NET?"
2. Buffer overflows: avoiding buffer overflows can be simplified to validating what the boundaries are and truncating input strings so you're not putting too much data into a buffer. Pretty straightforward. A buffer is just a placeholder, and you have to define the size of the placeholder. If you stuff too much information into that placeholder, you can get into trouble.
3. Insecure communications: we've talked a little bit about this earlier. Properly encrypt all authenticated and sensitive communications. Well, how do you do it? If it's at rest, use AES 256. If it's in transmission, use one of the PCA algorithms. Okay, how do I implement that? Again, just because you have a control, doesn't mean the developer knows what to do. You've got to give them additional guidance, and that' where things like OWASP and TeamMentor really come into play.
4. Improper error handling - this is very common. An application that gets input it doesn't understand, and it gives information back to the user, trying to be helpful, "I am a sequel server database,

and we require queries in this format: XXXX." Well great, why don't you just tell me how to hack you?! You've got to be sensitive not to leak information in error messages. Give the minimum amount required without giving too much information, in particular, information that names database tables or provides format for query format.

5. Cross site scripting, one of the most popular still, and one of the most rampant in web applications. This vulnerability has caused more damage than anything but SQL injection, in my opinion, in the last ten years. So validating parameters for web applications sessions before you include it in your transaction is one of the best practices to avoid cross site scripting.

6. Cross site request forgery - a newer vulnerability that came on the scene several years ago. To avoid this, is all about not relying on credentials or information that's automatically generated by the browsers. What what ends up happening is you have malware or a man in the middle that is generating these things and you can't trust it.

Okay, the good and the bad and the ugly for requirement 6.5 which talks about building applications on secure coding practices. First of all, adopt things like OWASP coding documents, or other trusted sources like Microsoft SDL or TeamMentor. These are maintained by professionals independently for your good. So use them. Also, map security controls to actionable steps for developers. This takes work, it takes effort. We can't just tell a developer "make sure that you're not susceptible to SQL injection" we've got to educate them. We've got to lead them down the path of what that means, and provide them training. If we can't educate them, we've got to give them access to training so they can self-educate or get educated by a subject matter expert. Some bad practices here, just doing the minimum to be compliant. This is very common, and I completely understand the motivation for this. Your mandate says to be compliant with "this" security standard, and most organizations don't want to spend a lot of money on security or compliance, they just want to do the least amount they can to be compliant and be done with it. Well, even if your goal was just to be compliant, this can still come to bite you in the butt. The reason being, is you can end up spending and wasting, five, six, or ten times more money and time because you're trying to meet specific security objectives one at a time, as opposed to writing secure applications and then determining how much leverage you get across not just PCI DSS but maybe also ISO, and HIPPA, and other security frameworks. And of course, the ugly: you want to believe that experienced, talented developers who write highly functional code and good performing code, and know how to write secure code. It's not true. It might be true, but you can't count that it is; you can't rely on it. You also can't rely that developers will self-learn, or self-manage everything they need to do. You've got to bring this particular horse to the water, so to speak. Next up is PCI requirement PCI 6.6. Probably the most prescriptive and also most frustrating for those of us in the security profession, it specifies that web-facing applications need to undergo either one of two things on a regular basis: either a vulnerability assessment OR have a web application firewall in front of them. Now, you ask any security professional, they're going to tell you that those two things are not equal. In fact, they're extremely different. And each one of them brings pros and cons with it, and we'll analyze that a little bit further on. Why the PCI Security Council decided that these two were equivalent compensating controls I'll never understand, but it is what it is. It's been this way since June 2008 so we have to deal with it. Another interesting and most frustrating sub-control here is that after you've conducted a security vulnerability assessment, you're required to verify that all vulnerabilities have been corrected. This is impossible, as anyone who has tried to do it can attest. Let me paraphrase this requirement a little bit more. What it says is for public-facing web applications, you have to have a security assessment OR a web application firewall. Okay, that's fine. What is a security assessment? Well it could be a code review, or a web application vulnerability scan. Again, that's fine. Use static analysis tools, use dynamic analysis tools, or you can also do it manually - in fact, best practices is that you use manual techniques to detect vulnerabilities that automated scanning technology can't. OR if you don't want to deal with that, just go buy a web application firewall. But make sure it's configured properly - a misconfigured web application firewall can easily block ALL traffic, and that's not good for business. You'll also need to question how many web application firewalls you'll need, and what the cost of that is when you're purchasing it, because the cost of web application firewalls can pile up pretty quickly and if you're comparing that to the purchase of a static or dynamic analysis tool; plus, you need the expertise in-house to run and operate that tool properly, so you've got to make that a consideration. OK, a little bit deeper. You've got multiple options for requirement 6.6.(a) - you can outsource a web vulnerability scan, or you can do a web vulnerability scan internally. You can outsource a code review, or do a code review internally. You can use automated tools, or you can do it manually. It's one of the more flexible requirements, and again, unfortunately, these are not all equal measures. If you have an application security professional conduct a manually code review and compare those results to an automated web vulnerability scan, you're going to find dramatically different results. You're most likely going to find a lot more vulnerabilities with a web vulnerability scan, the majority of them will probably be false-positives, and you're not going to find the most damaging vulnerabilities that end up getting caught with manual reviews, things like business logic and compound-attack vulnerabilities. But you've got flexibility. So again, by the letter of the law, internal or external, code review or web vulnerability scan -- up to you. Just keep in mind, if you're using automated tools (and here we go again IBM AppScan) they're terrific -- they can find a lot of common web vulnerabilities much faster than a human can; but, you've got to be careful with false positives, even worse false negatives (vulnerabilities they didn't find, that are actually there.) Keep in mind, the products relying on pattern matching. They have a set of vulnerability patterns, and they look for those patterns, either in your code or in your web traffic. There's no real good prioritization, and it's difficult for them or any automated tool to find vulnerabilities that are caused by applications interacting with their environment. Applications don't exist in isolation; they're always rooted in hardware, and network connectivity and dependent on other software, so don't become over reliant on tools.

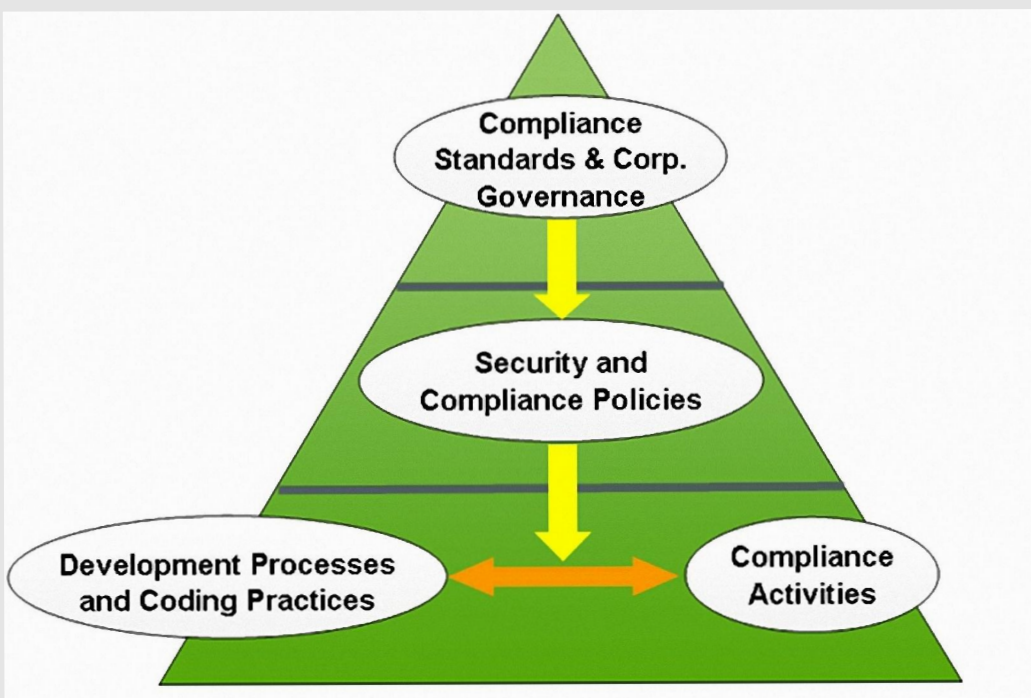
and dependent on other software, so don't become over reliant on tools. Let's talk about some good practices: Internal and external code reviews and web vulnerability scanning. We've found that highly mature organizations do both internal and external security assessment, and they do so at the source code level and at the as-built level. This was verified by The Ponemon Institue's Application Security Maturity study, as well as maturity studies that have been done previously by organizations like Security Innovation. It's a best practice, just like hiring a CPA to do your taxes. You can do them yourself, most of us probably do them ourselves, but you want an independent auditor to check, especially for critical assets and transactions. Using manual techniques to make sure that you're covering or hitting the gaps that the automated tools can't cover is another good practice. A bad practice is thinking that you can meet that one requirement that the PCI DSS that says that once you identify vulnerabilities, make sure you correct them all. Impossibility. And if your QSA is dinging you on this, kick them out, get a different one. Another bad practice is running AppScan once a year and thinking it's sufficient. I've bashed on these tools enough, so I won't go any further. As I mentioned, we use them every single day in our consulting practice. We love automated tools, so by no means am I saying "don't use them" -- but use them with prudence. And ugly practices: not realizing that you need skills to do code reviews and web vulnerability testing. I can't tell you how many organizations we've seen that have bought a tool like AppScan only to realize that a year later and a quarter million dollars into it, their developers don't know how to interpret the results, their security team doesn't know how to run the tool, they're not getting the value out that they'd expected, they start to get depressed and stop using the tool, and it's just a vicious cycle. Education is the key there. Also, don't rely on web application firewalls as your sole source of application security protection. They're good, again, at finding very specific vulnerabilities in traffic, not necessarily in application code, in fact, not at all.

Let's talk about requirement 11 now. Requirement 11 started out as just a network penetration test, and over the years it has morphed into now being a requirement to perform external AND internal penetration testing at least once a year, at both the network and application layers. Well that's terrific, however, keep in mind that what you do in requirement 6.6, which is a web vulnerability assessment or code review, can absolutely constitute an application layer penetration test. That is another example of one of the activities that you're doing giving you leverage over multiple security controls and requirements. Now it won't necessarily help you with the network penetration test; that's something you still have to do. Now the good, the bad and the ugly: It's good to realize that this is a complement to 6.5 or building applications according to best practice; it's also partly overlapping with 6.6. Another good practice is using penetration testing as a verification point. It really should be a backstop. It's verifying that you've done things right; it should not be the beginning and end of all of your testing efforts. If you're doing penetration testing specifically to find vulnerabilities, you're way behind the curve. You should be doing penetration testing to make sure that attackers cannot be successful and that you've architected and coded things correctly. A bad practice is running a vulnerability scanner, and I'll stop picking on AppScan, and I'll use Rapid7 NexPose - again, a fine product which we use all the time - but using those vulnerability scanners and assuming that you've got complete coverage is a no-no. No tool can give you complete coverage; a tool is just a tool - it helps you automate and do things a little bit faster. And ugly, as I mentioned, is depending on your penetration testing as your test and verification activities.

Next let's talk about requirement 12.6. This talks about building an information security policy and educating your employees. It calls out that you need to educate your employees upon hire and at least annually. Good practices realize that "educate all employees" means that you have to train by role. As I mentioned earlier, security awareness training for a janitor that comes in after hours when no-one is at your office is very different than training a java programmer who is sitting there from 9-5 needs. You can be proactive like leading organization in terms of security awareness -- regular reminders in different forms of media, e.g., stickers on bathroom mirrors, posters in the hallway - those kinds of things proactive organizations do very well. Some bad practices: getting together as a staff once a year and holding an awareness session with Sally the Security Professional. Also, using the same awareness content year after year. Technically you're not supposed to do it! 50% of organizations we've seen do exactly that - not a good practice. Attacks change, security awareness tactics change; keep up with the times. And of course, the worst thing you can do is just send an email pointing your staff to a couple of security resources and thinking you're done training. Not going to cut it.

Integrating PCI Requirements into your Development Process and Policies

This is about mapping application security to PCI. And I want to start with a typical compliance workflow:



At the top of the pyramid you've got legal requirement and customer requirement and compliance requirements. You take those and the executive team typically will develop corporate governance - corporate standards - that get passed onto the information risk management or information security team. What does that team do? It generates security policies and compliance policies, and then they dole them out to all the individual people in the organization, and from that (now you're at the bottom of the period) you've got compliance activities that you need to be able to map to software development best practices. Most organizations don't do that - they stop at the two yellow arrows, and they don't do the orange. But the orange arrows are the most important part. This is where you're going to be able to request and enable your software architect developers and testers to do what they need to do. And keep in mind you need to define activities for each phase and each team member in software development. It incorporates tools, it incorporates training, it incorporates new processes. You need to be able to work hand in hand with those development organizations.

We saw in the data point earlier that majority of development teams don't think that they work in collaboration with security professionals, and it's incumbent upon us to change that. And how do you change that? Well, first of all you can do some simple mapping of PCI requirements of application security to security activities. I'm going to show you some examples below. Secondly, you can take advantage of the fact that hacking is cool. Monitor attack trends. Developers don't necessarily want to do security activities, but they want to do cool, interesting things. So help them take advantage of the fact that hacking is cool and bring in a subject matter expert, show them how their particular application might be exploited, and then remind them that doing a single security activity, such as a code review, can get you leverage over multiple requirements. And expose the requirements to them. Developers want to know that what they're doing is useful, so expose the requirements to them.

Take a look at activities like threat modeling and security code reviews. Exposing your testers to OWASP Top Ten can enable them to learn how to adopt some of these activities. These are the types of tools and activities that your software development teams need to be doing. Let's consider that SQL injection example that we alluded to earlier. This is where we talked about connecting the dots. PCI requirement 6.5.1 says "build applications that are not susceptible to injection flaws, particularly SQL injection". Okay, great. Is your job done as a security professional once you've handed that off to your development team? Heck no. A developer has to understand "Okay, what is SQL injection?" And once they understand what SQL injection is, they need to answer, "How do I code defensively to prevent SQL injection?" What are some steps you want them to take? One might be sanitizing user input. That's good. Next the developer needs to learn "How do I sanitize user input?" What guidelines can you provide to help them do that? Take it a step further: the developer then needs to consider, "Well, I'm writing an ASP.NET application - how do I sanitize user input in ASP.NET?" That's how far we've got to take it! And typically we stop very short of that. But, resources like OWASP and TeamMentor will allow us to get there.

Use a spreadsheet - put all of your security controls on one column, and then security coding activities or application security best practices along the rows, and you'll see the overlap. It's a pretty straightforward thing to do, and for those of you that use UCF (Unified Compliance Framework), it does this for you. Here's a typical mapping of the PCI requirements and the OWASP Top Ten. Very straightforward. 6.5.7 is OWASP Top Ten #2, 6.5.1, OWASP Top Ten #1.

Okay, these are some things to keep in mind: how will you fail your PCI audit? Well, you'll fail your PCI audit if all members of the development team don't know basic software security principles. You'll also fail if your team is not properly trained on tools and what the tools are doing: looking for web vulnerabilities, scanning source code for vulnerabilities. And you'll also fail if compliance professionals don't at least have a high understanding of what application security best practices are.

We've talked about tools plenty in this webcast; you really need to understand how the tools apply before you buy it, and certainly before you use it. I don't know how to use a jack hammer. If I see one, I'll probably just leave it alone. I won't want to touch it, I won't try to turn it on, and I certainly won't try to create a hole with it because I'll most likely just take off my foot. Best practices yield leverage. Everyone knows that if you want to have good heart health, eat fruits and vegetables, avoid food with high saturated fat content, and exercise regularly. Well you know what, those are best practices not just for good heart health, but to avoid diabetes, to avoid stroke, to avoid high cholesterol. It's the same in application security: you follow the best practices; you'll get leverage across compliance and don't think about it in the reverse way.

Okay, some concluding recommendations:

1. Adopt and document application security best practices. There's plenty of documentation out there for you to leverage and use - go grab it.
2. Educate your teams. I can't stress this enough; it's the most leverage you're going to get - educate your teams. Not just on what PCI DSS means, but on application security fundamentals and best practices. There's lots of good training available out there.
3. Align your SDLC with corporate policies and compliance requirements.

About the Author

Ed Adams is a software executive with successful leadership experience in various-sized organizations that serve the IT security and quality assurance industries. As CEO, Mr. Adams applies his security and business skills, as well as his pervasive industry experience in the software quality space, to direct application security experts to help organizations understand the risks in their software systems and develop programs to mitigate those risks. The company has delivered high-quality risk solutions to the most recognizable companies in the world including Microsoft, IBM, Fedex, ING, Nationwide and HP.

Mr. Adams is a Ponemon Institute Fellow and founded the Application Security Industry Consortium, Inc. (AppSIC), a non-profit association of industry analysts, enterprise technologists, and security leaders established to define cross-industry application security metrics and best practices that eventually morphed into SAFECode at which point Mr. Adams got more engaged with other industry initiatives, including OWASP. Mr. Adams is on the board of the National Association of Information Security Groups (NAISG), and the International Secure Software Engineering Council (ISSECO).

No stranger to the podium, Mr. Adams has presented to thousands at numerous seminars, software industry conferences, and private companies. He has contributed written and oral commentary for business and technology media outlets such as New England Cable News, CSO Magazine, SC Magazine, CIO Update, Investor's Business Daily, Optimize and CFO Magazine. Mr. Adams earned his MBA degree with honors from Boston College.

Cyber Crime and Cyber War Predictions

by Gary S. Miliefsky & Pierluigi Paganini

PREDICTION #1 - MOBILE MALWARE TAKES OVER

REMOTE EAVESDROPPING. COVERT DATA THEFT. WORMS AND BOTNETS ARE COMING

The technologies characterized by the largest penetration level with the most contribution to the distribution of new cyber threats are social media and mobile computing. Mobile devices are powerful tools, often unprotected and their owners, and in a majority of cases, their owners completely ignore the risk of applets being cyber threats and they miss the basic measures to mitigate them. Most users trust first and never verify later. This is bad. Very bad.

Mobility, in both private and business environments, have pushed technologic changes without compensating with a proper optimization within a perspective of holistic security, which has, of course, led to new and more powerful vectors of attack methodologies, including undetectable covert channels for data and identity theft as well as the deployment of new remotely controlled botnets on mobile for SMS and other purposes, yet to be determined, leveraged daily, by cyber criminals and hackers.

The Android OS will be the most attacked mobile platform, with more of 100 million Android devices having shipped in Q2 2012 alone with a 52.2% market share, lack of defense systems and user awareness on cyber threats make them easy, privileged targets for cybercrime and state-sponsored hackers. In a recent report by the Sophos security team, they revealed that in Australia and the U.S., Android threat exposure rates are now far exceeding those of PCs, showing the urgency to implement proper countermeasures.

To aggravate the scenario, we have the uncontrolled introduction of mobile use in workspace that enlarged the surface of attack to include small to large enterprises and governments. To reduce this risk, it is fundamental to define and implement "bring your own device" (BYOD) policies to address the ways in which employees could use these devices both in and out of the workplace - this should include the mechanisms of access protection to be adopted, data encryption, data accessible by the mobile platform, and limiting the execution of applications that can be run outside the company (e.g., email client or data mining applications).

Android isn't a lonely, unique platform hit by cyber threats, as the changing nature of all endpoint devices and the presence of multiple operating systems (OS) in the same environments has already produced as effect, the diffusion of new multi-platform malware that targeting governments and private businesses, the trend is in constant, explosive growth.

Our prediction is that the year 2013 will be characterized by the diffusion of new malicious agents designed to exploit mobile smartphone, tablet and other new platforms, with the principal attacker categories to be both cyber-criminal organizations and governments. Many governments may be using these platforms for cyber-espionage on their own citizens as well as rogue nation victims. This problem will not be solved by traditional firewall and anti-virus countermeasures.

PREDICTION #2- ROGUE NATIONS UNLEASH CYBER WEAPONS

IN RESPONSE TO THE USA AND ISRAEL. OTHERS JOIN THE FIGHT

Governments from all around the world are conscious of the strategic importance of cyberspace and are concerned about the risks related to cyber attacks against their critical infrastructures. Over 100 independent nations, according to official sources, are developing cyber weapons - and the number of cyber warfare operations, taking place over the Internet, has dramatically increased. It has been estimated that thousands of attacks are conducted daily against government systems all over the world and they are principally conducted by foreign governments mainly for cyber espionage but also for offensive purposes. In this scenario, it is easy to predict a rapid and dramatic increase of the number of state-sponsored attacks during 2013, most of them exploiting 0-day ('zero-day') vulnerabilities to compromise the networks of the adversaries. One of the principal problems approaching cyber weapon development and their use in warfare context is the total absence of a globally recognized "common law" framework that evaluates the legal and political responsibility of the aggressor and the real level of threat made. Also, spillover into civilian life is happening without measure - many new cyber weapons traverse the Internet through vulnerabilities in civilian private and business computers and mobile devices. This year, 2013, and the following few years, will be characterized by the intensification of the cyber operations, governments such as the US have demonstrated a great interest in attacking enemies rather than simply defending against them. In fact, the unclassified PLAN X program launched in October 2012 by the Defense Advanced Research Projects Agency (DARPA) expresses the will to design new revolutionary technologies for cyber warfare operations. Meanwhile the US, Israel, Russia and China will continue to invest in the development of new cyber capabilities, governments of North Korea and Iran are considered the most active in the designing of new cyber weapons. Both counties, historically considered hostile, will conduct attacks in cover operations against their enemies. The development of cyber weapons is much easier and cheaper than the creation of conventional weapons and has the great privilege that could grant the anonymity of the attackers. Finally, with so many newly uncovered smartphone, wireless router, USB, universal plug-and-play-protocol implementations and SCADA vulnerabilities, one could imagine a scenario where state-sponsored cyberweapons traverse smartphones over cellular networks then through wireless routers onto critical infrastructure environments and then, uncovering a SCADA vulnerability, exploit a system causing tremendous physical damage - such as what happened to Iran via Stuxnet. While Stuxnet targeted particular Siemens equipment which helped control a nuclear reactor, other new cyber weapons might affect air and train transportation, traditional coal and natural gas power plants and much more. Te risks of backfire and blowback should be seriously taken into account and the consideration for defensive cyber weapons.

PREDICTION #3- BRING YOUR OWN DEVICES OUT OF CONTROL

MANAGEMENT OF THIS BYOD DILEMMA WILL BE A NIGHTMARE

The IT landscape is dominated by the rise of mobile networking - pervasively almost all employees bring their mobile devices into the workspace and access to corporate resources and data from the outside. Most security experts believe that this promiscuous usage has to be regulated to avoid security incidents.

While these new gadgets - smartphones and tablets allow users to be almost always connected, either over wireless or cellular networks, or both (at the same time), the downside is that the attack surface is impressively increased and expose unaware users to serious risks. These risks ripple throughout the enterprise and the Bring Your Own Device (BYOD) dilemma is reaching epic proportions.

A proper BYOD policy must address application assessment and control, data and services accessible, authentication mechanisms and many other aspects such as devices disposal. While BYOD is an opportunity for companies to increase productivity and employee satisfaction, while reducing equipment expenditures, the lack of an efficient approach exposes organizations to security risks and further financial exposure, but it represent also an overload for IT & Infosec sectors of businesses.

Through the adoption of a BYOD policy, companies could improve user's productivity and obtain cost cutting but they must also be willing to reinvest in the improvement of their IT infrastructure introducing new defense systems that could preserve internal networks and client devices.

Unfortunately, many companies ignore completely, the real risks associated with the use of mobile technologies and consider the security as a cost to limit. The effects will be felt in the coming months, cybercrime will vigorously hit the private sector, especially small and medium enterprises (SMBs), easily taking advantage of the absence of adequate security measures.

While the INFOSEC industry has put the word out that “802.1x” is the be-all-end-all answer to the BYOD dilemma, it is not. In fact, 802.1x is a protocol pushed by all the major Network Access Control (NAC) vendors with the exception of one vendor. According to PWNIE EXPRESS, this protocol is easily circumvented. In addition it only works on newer, more expensive managed switches. It also does not work on all VoiP equipment and it does not work across Hubs, also known as ‘unmanaged switches’. In addition, your SmartPhone and Tablet are probably NOT running the 802.1x protocol.

Cybercriminals have found their new trojan horse and it's probably in your front pocket with an infected applet allowing remote control, eavesdropping, data leakage and convert command and control channels. Ring, ring, 2013 shall be a wakeup call for the BYOD dilemma.

PREDICTION #4- CLOUD EXPLOITATION WILL BE FRONT PAGE NEWS

CLOUD AND "VIRTUAL" COMPUTING VULNERABILITIES EXPLOITED BY CYBER CRIMINALS

Cloud computing infrastructures will continue to suffer cyber attacks, as hackers and cybercriminals are well aware of the capabilities that these platform offers. Compromising a cloud infrastructure, public or private, gives to the attackers an impressive amount of resources to use in further attacks. The Security for Business Innovation Council, composed by IT security experts from 19 companies worldwide, include cloud computing exploitation as a major disruptive force for 2013. In its report, "Information Security Shake-Up," the group highlights that many organizations are preparing to move more business processes to the cloud. The trust in could computing model is increasing sensibly, majority of business managers are confident that the cloud is now viable for mission critical business applications, in 2013 "mission-critical applications and regulated data" will be consigned to the cloud,

The report states:

"Middle managers don't want to use their resources on security," the report bluntly says. "They are incentivized by timeline and budget; adding security doesn't fit into their objectives."

The exploit of security holes in software as a service (SaaS), infrastructure as a service (IaaS) or platform as a service (PaaS) is one of the primary targets for attackers that are conscious of the power offered by these architectures and services.

Securing cloud computing architectures will be a major focus of vendor efforts over this year. Corporations that are risk-averse enough to avoid the public cloud should be interested to the deployment of secure private cloud which contains all the security controls usually missed in public environments. Private clouds are usually more efficient, as they are characterized by a more responsive incident management and also detection capabilities and operational capabilities such as patch management are improved. Remember, a vulnerable service within a cloud architecture could expose the entire cloud, which would easily allow the proliferation of malware within the infrastructure.

We believe that principal incidents in the incoming year could affect mainly private clouds for which security procedure in many cases are not adopted correctly. Wrong configurations and improper use of cloud resources could expose cloud hosted applications to serious risks and data loss. Fortunately many instruments, such as data encryption tools, smart key management tools, log management tools, identity and access management systems and virtualization-management tools allow cloud IT managers to prevent and mitigate cyber threats, but they have a cost that businesses have to be ready to pay. Until then, we expect front page news this year on cloud exploitation.

PREDICTION #5- SCADA DOWNTIME WILL AFFECT SOCIETY

SUCCESSFUL SCADA ATTACKS WILL BRING DOWN CRITICAL INFRASTRUCTURE

According to the latest report published by The European Network and Information Security Agency (ENISA) "ENISA Threat Landscape - Responding to the Evolving Threat Environment" that summarizes principal cyber threats, critical infrastructure represents prime targets in the latest wave of cyber warfare and cyber terrorism. Different agents such as terrorists, state-sponsored hackers or hacktivists are very interested in attacking control systems within a critical infrastructure, the possible impact could be considerable under different perspectives (governments, homeland security, society).

Public health, energy production, telecommunication are all sectors exposed to serious risks that have to be protected at any level as described in an efficient cyber strategy. However, most SCADA systems are now getting internet connectivity without any forethought into the network security implications.
Serious hackers - especially cyber terrorists are increasingly targeting critical infrastructure across the board and the world. One proof point is the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) tracking of their responses to cyber incidents against critical infrastructure which uses SCADA. In 2012, they responded to 198 major cyber-incidents against critical infrastructures, which was a significant increase over the incidents of the prior year. The sector that most suffered the attacks in 2012 is the energy, accounting for 41 percent of reported events, followed by water with 15 percent. There are a couple of glaring problems that need to be addressed for the defense of critical infrastructure against cyber attacks:

Level of awareness and government commitment : Before the Stuxnet case, the world wide security community has always underestimated the possible effect of a cyber offensive, in many cases refusing to believe in the concept of a "cyber weapon" of potentially "mass destruction". Fortunately the events of late have changed the perception of cyber threats and all governments are approaching the problem through the definition of a more efficient cyber strategy focused on SCADA and related critical infrastructure protection.

The level of knowledge needed for a cyber attack : contrary to what users might believe - that it is difficult or nearly impossible to attack a SCADA system, it is in fact very easy….there are many techniques that could be adopted to compromise a control system, in several occasions the absence of defense systems, improper configurations, zero-day vulnerabilities and superficial patch management processes, enabling the mission of the attacker.

The main problem is that potentially any professional with no particular knowledge could simply gather information on a target choosing for him already available exploit kits which target SCADA systems. The fact that anyone can get a hold of the Stuxnet source code is a major problem.

Recently the web portal ThreatPost, the Kaspersky news lab service, published an interesting article titled "Shodan Search Engine Project Enumerates Internet-Facing Critical Infrastructure Devices" on the possibility to used publicly available information to identify Critical Infrastructure devices. Two critical infrastructure protection specialists, Bob Radvanovsky and Jacob Brodsky of consultancy InfraCritical, have worked in collaboration with Department of Homeland Security for 9 months to discover all devices presents inside US critical infrastructure and exposed on the web. The results are shocking and the situation is very concerning; the two researchers discovered initially more than 500,000 devices, many of them exposed online without proper security defense, typically protected by poor authentication mechanisms based on published default passwords. Not only critical infrastructures such as communication, energy and water utilities use SCADA devices, also common HVAC systems, traffic control systems and building automation control systems make large use of these devices. SCADA systems are very diffused and DHS tried to restrict the initial list to most relevant systems identifying a final list of 7,200 devices. To select the potential targets the two specialist haven't used specific technologies, it was enough to write scripts to conduct automated searches on Shodan search engine, a popular web portal which lists servers, routers, any other network devices exposed online providing useful information to an attacker such as geographic location and the operating system (OS) versions installed.
Let us not forget the excellent work of a couple of Italian security specialists, Luigi Auriemma and Donato Ferrante, founders of the company ReVuln that published an interesting proof of concept on SCADA systems, "ReVuln - SCADA 0-day vulnerabilities", and related vulnerabilities. The video published by the researchers is a showcase of some SCADA 0-day exploits owned by ReVuln security company, the 0-day vulnerabilities are all server-side and remotely exploitable. This video shows issues affecting the following vendors: General Electric, Schneider Electric, Kaskad, ABB/Rockwell, Eaton, Siemens …in other words, when it comes to SCADA, nobody is secure. Note that many other 0-day vulnerabilities owned by ReVuln affecting other well-known SCADA/HMI vendors have been not included in this video. Demonstration of the great interest on cyber security by the US Government, that fears cyber attacks and their consequences on Homeland Security, is seen in the well known program called "Perfect Citizen". The program has the main purpose to explore national utilities to discover security vulnerabilities that could be exploited in case of attack and this research will go on at least until September 2014. It's fundamental that any governments will improve cyber strategies to protect SCADA systems, requiring the respect of strict regulation under security perspective to ensure their security and prevent external attacks.

Therefore, we predict that 2013 is a critical year, on the one hand we have an army of attackers who may attack at any time SCADA systems deployed everywhere, on the other end there is the IT community aware of the problems that must try to remedy them at all costs to avoid serious consequences in terms of security.

PREDICTION #6- INDIVIDUAL PRIVACY IS OVER THIS YEAR

YOUR IDENTITY AND PRIVACY ARE STOLEN. EAVESDROPPED. BOUGHT AND SOLD.

Every day, we read new stories about cybercriminals that steal user's sensible data and in a majority of cases they pretends to be someone else by assuming victim's identity in the cyber space. Identity theft is just one of the multitude of cyber threats that menace user's identity and their privacy; the frequency of this type of crime is increasing as reported by the last IC3 report and updated daily on http://www.privacyrights.org/ for privacy breaches in the USA.

The Windows, iPhone, Android, BlackBerry and Windows Phone markets are incredibly high risk environments for being spied upon without the end-user's knowledge. With an estimated 60% of BING and over 30% of GOOGLE website links containing drive-by malware, it's no wonder, cyber crime that allows for remote espionage and spyware being easily installed through drive-by downloads is on a tremendous rise and will continue to grow.

Firewall software for these platforms may or may not block port traffic depending upon the end-user setttings. Most users want SKYPE and Microsoft IM to be able to communicate and therefore numerous ports remain open for malware to phone home to callback URLs or for spyware to send their eavedropping information to those who are maliciously eavesdropping.

Phishing, advanced persisent threat (APT) and many other kind of malware based attacks daily menace user's data, coupled with the high penetration level of technologies, such as social networking and mobile, are exposing user's privacy to serious risks. But individual privacy is also menaced by legitimate business, governments and private companies are increasing the monitoring of user's experience on line, obviously for different purposes. Governments and intelligence agencies mainly operate for homeland security reason meanwhile private businesses in many cases ignore user privacy to collect the major number of data on user's habits to be able to provide him a customized offer that match its needs.

Mobile devices that tracks our movements, smart-tv that are able to recognize user's experience to provide the desired programs, browsers that collect user's navigation data, VOIP clients that are subject of eavesdropping are just some examples of possible menace to user's privacy.

Technology is assuming a relevant role in our lives, it is improving the quality of life but it is amplifying our attack surface, in 2013 and in the near future, the concept of privacy will be utopia, internet users will suffer an unprecedented personally identifyable information (PII) exposure … we've probably already passed the point of no return.

PREDICTION #7- THE UNITED NATIONS ATTEMPTS INTERNET TAKEOVER

THE U.N. WILL TRY TO CREATE A RULING INTERNET BODY AND NEW LAWS

Only a few months ago, a UN treaty was approved to update the 24-year-old United Nations telecommunications rules. The agreement states that countries have the right to access international telecommunications services and control them to prevent cybercrimes. The downside is that the UN treaty could open the doors to attitudes of censorship of governments that want to apply a strict control on the Internet. The countries that haven't accepted the UN agreement, such as U.S. and U.K, will continue to be bound by the 1988 release of the communication rules according declaration of a spokeswoman for the International Telecommunication Union, Sarah Parkes. Google representative commented:

"We stand with the countries who refuse to sign this treaty and also with the millions of voices who have joined us to support a free and open web."

Every government is increasingly monitoring and selectively censoring web sites, content and access to the entire Internet, and similar treaties legitimizes it, but do not nourish false illusions, everything on Internet is already being monitored. Monitoring and control of internet are highly debated and contradictory topics, censorship is a multi-billion dollar business in continued exponential rise and many major social media sites are doing tremendous monitoring - and for whom? Is it for marketing purposes or government spying? We know it's happening…the question is for whom and why?

Adopting the standard known as Y.2770 (Approved on 2012-11-20 - Requirements for deep packet inspection in Next Generation Networks) the United Nations' International Telecommunications Union has taken the unprecedented step permitting traffic eavesdropping on a global basis. The UN seeks unprecedented control of global internet traffic which would permit the inspection of Internet traffic analyzing every piece of web content such as emails and any other form communication; with the only defense against this being strong encryption coupled with non-dictionary-based strong passwords. Control of communication channels is a critical question, one also understands the need to protect homeland security through intelligence operations but we cannot ignore the situational differences in every country - based on local and federal laws and the ripple affect on their citizens. In China, Syria, Iran and Russia today opponents of the governments are exposed to risk more serious … at stake there is their survival. It is easy to forecast that the standard approved by UN will be invoked by many countries for eavesdropping of communication, creating outrage among citizens and much of private industry at stake is much more freedom of expression, these treaties hide business logic that ignore human dignity and the possible implications on freedom of expression. And it is reasonable to expect that many will use alternative forms of communication and anonymous technologies to avoid the control of governments. Examples include anonymizing networks and proxy servers, VPN tunnels for 'hiding IP addresses', because slowly, like a frog in a pot of warm water with the temperature rising slowly, the Internet will change, it will never be the same, and we now run the real risk of being in a militarized cyber zone managed by global beaurocrats and their financial backers.

InfoSec Marketplace

Uncovering Innovative Information Security Products and Services

InfoSec Marketplace

Uncovering Innovative Information Security Products and Services

SERVICES

Center for Internet Security

Vendor Neutral – Cost Effective

Security Benchmarks™
A division of Center for Internet Security

Are Your IT Systems Secured according to Industry Best Practice? Find Out Now!

CIS-CAT, a member-only **C**onfiguration **A**ssessment **T**ool, can compare the configuration security of your IT systems against 25 CIS Benchmarks.

For a *FREE* 30-day CIS-CAT Trial, contact members@cisecurity.org.

Gain access to over 70 consensus-based security benchmarks covering 14 technologies...
Microsoft, Red Hat Linux, Oracle, Cisco, IBM, Apple, Apache and more!

Become a CIS member today!
Learn more at: http://benchmarks.cisecurity.org/enroll.
And for a 10% discount off a 1-year membership, enter PROMO CODE: **RSA2013**

http://benchmarks.cisecurity.org

Internationally Recognized – Nonprofit

Widely Used for Compliance with Industry Regulations & Referenced in the PCI Data Security Standard

NAISG

National Information Security Group:
Visit us online at NAISG.org
and signup for free TechTips

CCURE.ORG

Did you know that more than 150,000 people have used the CCCure's resources over the past 12 years to reach their certification and career goals? CCURE.org offers some of the most complete and relevant quizzes for the CISSP® and the CEH® certifications. CCCure.org also has over 1600 questions for the CISSP® and many hundreds of questions for the CEH®. You can track your progress and we also offer the ability to review questions you have missed.

www.cccure.org

InfoSec Marketplace

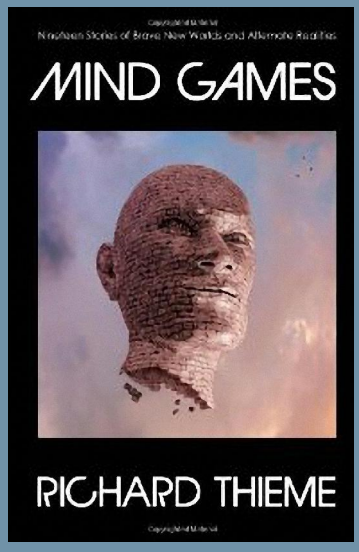
Uncovering Innovative Information Security Products and Services

PRODUCTS AND SERVICES

InfoSec Marketplace

Uncovering Innovative Information Security Products and Services

BOOKS



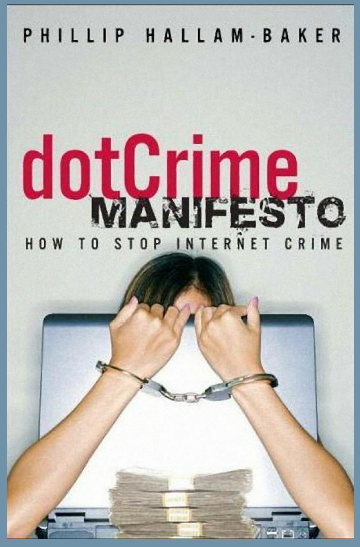
Mind Games - by Richard Thieme

A Unique Collection of 19 Stories of Brave New Worlds and Alternate Realities

Mind Games is a unique collection of 19 stories of brave new worlds and alternate realities - stories of computer hackers, deception and intelligence, puzzling anomalies, spirituality and mysteries of consciousness, the paranormal, UFOs, alien life forms - in short, everyday life in the 21st century. All have been previously published in literary, slipstream, and science fiction magazines and anthologies but have not been available in a single collection - until now.Beautifully illustrated and published by Duncan Long Publications. Available from the author, signed, at retail price, $20 or $23 ($20 + $3 mailing) via mail – pay rthieme@thiemeworks.com at PayPal or by check to:

Richard Thieme
ThiemeWorks
PO Box 170737
Milwaukee WI 53217

http://www.thiemeworks.com/book-mind-games/



The dotCrime Manifesto: How to Stop Internet Crime

By Dr. Hallam-Baker, co-inventor of the World Wide Web

Internet crime keeps getting worse...but it doesn't have to be that way. In this book, Internet security pioneer Phillip Hallam-Baker shows how we can make the Internet far friendlier for honest people–and far less friendly to criminals. The dotCrime Manifesto begins with a revealing new look at the challenge of Internet crime–and a surprising look at today's Internet criminals. You'll discover why the Internet's lack of accountability makes it so vulnerable, and how this can be fixed –technically, politically, and culturally. Hallam-Baker introduces tactical, short-term measures for countering phishing, botnets, spam, and other forms of Internet crime. Even more important, he presents a comprehensive plan for implementing accountability-driven security infrastructure: a plan that draws on tools that are already available, and rapidly emerging standards and products. The result: a safer Internet that doesn't sacrifice what people value most: power, ubiquity, simplicity, flexibility, or privacy.

http://www.dotcrimemanifesto.com/

InfoSec Marketplace

Uncovering Innovative Information Security Products and Services

BOOKS

InfoSec Marketplace

Uncovering Innovative Information Security Products and Services

JOB OPPORTUNITIES

DHS CYBER POSITIONS

DHS is actively recruiting innovative, dynamic, and cutting edge professionals to protect the Nation's cyberspace.

Come join us and apply your knowledge and skills to America's most complex homeland security challenges.

A variety of occupations are available, such as:

- Electrical Engineers (GS-855)
- IT Specialists (INFOSEC) (GS-2210)
- Telecommunications Specialists (GS-391)
- Program Management (GS-343/340) Security (GS-0080)
- Intelligence Analyst (GS-0132)
- Investigative Analyst (GS-1805)
- Investigation/Criminal (GS-1810/11)

Be a part of the cybersecurity solution. **Join DHS today!**

For more information about available career opportunities, go to www.dhs.gov/cybercareers.

You may also search www.usajobs.com and use "cyber" as the agency search term.
DHS is an equal opportunity employer.

U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security

RSA BOOTH #845

NSA
NSA.gov/Careers
APPLY TODAY

WHERE INTELLIGENCE GOES TO WORK®

https://www.cia.gov/careers/

THRIVE

WHAT ON EARTH WILL IT TAKE?

A CLEAR COMPASS MEDIA PRODUCTION Creator and Host: FOSTER GAMBLE Producer: KIMBERLY CARTER GAMBLE Directors: STEPHEN GAGNE and KIMBERLY CARTER GAMBLE Visual Effect Director: GOA LOBAUGH
Visual Effects: LIQUIDBUDDHA STUDIOS Editors: STEPHEN GAGNE and BRENT STREEPER 2-D Animation: MICHELLE ENEMARK Writers: FOSTER GAMBLE, KIMBERLY CARTER GAMBLE, NEAL ROGIN and MARY EARLE CHASE
Co-Producer: JAIME VLASSOPULOS Associate Producers: CLAIRE DARLING, MARSHALL LEFFERTS and LEE WATERWORTH Original Score: GARY MALKIN and DAN ALVAREZ

WWW.THRIVEMOVEMENT.COM

Clear Compass Media

FireHost Cloud Security Hosting Platform

While there's a lot of hype out there about the Cloud, security has been an afterthought. But that is not the case at FireHost, who was designed from scratch to focus on Security and Regulatory Compliance-based hosting on the Cloud - one of the most unique and advanced security-based ISP and MSSP offerings we've seen in the industry and priced right.

Secure Managed Hosting

FireHost makes the benefits of "big IT" initiatives like eCommerce, high-availability, load balancing and virtualization available to small and medium size businesses, for less. They rovide managed hosting solutions that fulfill the needs of businesses with complex hosting requirements on Windows and Linux platforms. Their engineers break down all aspects of your hosting requirements to an understandable level and customize a solution specifically for your needs.

Secure Compliant Hosting

When it comes to PCI DSS, SAS 70 and HIPAA, which are compliance standards that were developed to provide protection for personally identifiable information (PII), protected health information (PHI) and credit card data, FireHost has you covered. If your business requirements include obtaining any of these compliance objectives, FireHost provides secure, compliance ready hosting to clients in healthcare, eCommerce, and financial institutions worldwide. They help online businesses small and large obtain the understanding, confidence, infrastructure, and resources necessary to make their online presence soar to the next level, securely.

PCI 2.0 Compliant Hosting

Secure, PCI 2.0 compliant web hosting allows retailers worldwide to accept, store, and/or process credit cards and sensitive personal data in a responsible way. Their PCI hosting segments public, website files from confidential database files and restricts access to "need to know" personnel only.

HIPAA Compliant Hosting

FireHost helps healthcare organizations achieve and maintain HIPAA (Health Insurance Portability and Accountability Act) security requirements. For many FireHost clients, outsourcing electronic aspects of HIPAA to a secure web host allows them to focus resources on inter-office aspects of HIPAA regulations.

FISMA Compliant Hosting

The need for security embodies the FISMA requirements, and FireHost provides the extremely secure hosting infrastructure to fully support those high standards. From the physical to the network and system layers, FireHost deploys a defense in depth approach that meets or exceeds NIST 800.53 rev3 requirements.

SSAE 16 Compliant Hosting

SSAE 16 sets the new standard for compliance. One of FireHost specialties is helping small and medium-size businesses achieve SSAE 16 certification, which meets the new international service organizations standards for Type I and Type II reporting.

SAS 70 Compliant Hosting

SAS 70 compliant hosting practices allow organizations to achieve compliance for more control objectives. With a secure hosting provider, you inherit some of the FireHost controls to achieve a more extensive and thorough compliance auditor report.

In addition to all of these compliance measures, FireHost has planned for the worst exploitation of Open Source platform hosting such as exploitable WordPress, Drupal and Joomla as well as the risks of exploitation to your hosted MYSQL, Microsoft SQL Server and PostgresSQL databases.

They also take business continuity very seriously and offer solutions for businesses that cannot afford to suffer from as little as a 1-minute hiccup to a more serious, catastrophic event. To learn more, visit them at http://www.firehost.com.

Service Effectiveness:	ê ê ê ê ê
Customer Support:	ê ê ê ê ê
Platforms and Pricing:	ê ê ê ê ê
Installation and Documentation:	ê ê ê ê ê
User Interface and Ease of Use:	ê ê ê ê ê

Overall Rating: ê ê ê ê ê

Summary

For their well defined security posture and strong regulatory compliance offering wrapped around all the features and benefits of Cloud-computing and virtualization, with an affordable pricing model, we give them a well deserved **Most Secure Cloud Hosting Platform Award for 2013.**

Information Security Innovator of the Year

> "Robert Martin is an unsung hero - shaping past, present and future thinking about vulnerabilities and their exploitation."
>
> Pierluigi Paganini, Editor-in-Chief

WHO IS ROBERT A. MARTIN?

Robert A. Martin is a Senior Principal Engineer at The MITRE Corporation, a not-for-profit organization that operates federally funded research and development centers for the government. For the past 20 years, his efforts focused on the interplay of risk management, cyber security, and quality assessment. The majority of this time has been spent working on the CVE, OVAL, MAEC, CAPEC, CybOX, and CWE security standards initiatives in addition to basic quality measurement and management.

He is a frequent speaker on the various security and quality issues surrounding information technology systems and has published numerous papers on these topics. Mr. Martin joined MITRE in 1981 with a BS and MS in Electrical Engineering from RPI, later he earned an MBA from Babson College. He is a member of the ACM, AFCEA, IEEE, and the IEEE Computer Society.

WHY IS THE CVE PROGRAM SO IMPORTANT?

While there may be more than one hundred million samples of malware in the wild, they can each only exploit one or more CVEs. That means if you can find and fix your CVEs, you can worry much less about much more malware. It's the most proactive thing you can do to harden your systems against exploitation.

WHAT DOES OVAL STAND FOR AND WHY SHOULD YOU CARE?

OVAL stands for Open Vulnerability Assessment Language and takes the CVE program to a higher level by wrapping vulnerabilities in a well defined XML schema, enabling the process of alerting, detecting, reporting and removing vulnerabilities to become machine-readable and automated.

WHAT IS MAEC?

MAEC™ is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns. By eliminating the ambiguity and inaccuracy that currently exists in malware descriptions and by reducing reliance on signatures, MAEC aims to improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware; reduce potential duplication of malware analysis efforts by researchers; and allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances.

HOW ABOUT CAPEC?

CAPEC™ is a publicly available, community-developed list of common attack patterns along with a comprehensive schema and classification taxonomy. Attack patterns are descriptions of common methods for exploiting software systems. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples.

To respond effectively, the community needs to think outside of the box and have a firm grasp of the attacker's perspective and the approaches used to exploit software systems. CAPEC provides this information to the community in order to help enhance security throughout the software development lifecycle and to support the needs of developers, testers, and educators.

TELL ME ABOUT CybOX?

CybOX™, the Cyber Observable eXpression, is a standardized schema for the specification, capture, characterization and communication of events or stateful properties that are observable in the operational domain. A wide variety of high-level cyber security use cases rely on such information including: event management/logging, malware characterization, intrusion detection, incident response/management, attack pattern characterization, etc. CybOX provides a common mechanism for addressing cyber observables across and among this full range of use cases improving consistency, efficiency, interoperability and overall situational awareness.

WHAT IS CWE ALL ABOUT?

The Common Weakness Enumeration (CWE) defines a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that detect weaknesses in software. Past Top 25 CWE lists have represented community collaboration efforts to prioritize the most exploitable constructs that make software vulnerable to attack or failure.

SUMMARY

For his humble and consistent passion to make the Common Vulnerabilities and Exposures (CVE) program the global, de facto standard for describing vulnerabilities, helping build the database of CVEs from less then 300 known holes in 1999 to over 54,000 catalogued weaknesses in all major operating systems, applications, Internet software and connected devices, and being an INFOSEC thought leader, we name Robert A. Martin our Information Security Innovator for 2013.

Cyber Defense Magazine
www.cyberdefensemagazine.com

About Our Founder & Executive Producer

Gary S. Miliefsky, FMDHS, CISSP

Gary S. Miliefsky is the Executive Producer of Cyber Defense Magazine (CDM), which he founded after years of being a cover story author and regular contributor to Hakin9 Magazine. In partnership with UMASS, he started the Cyber Defense Test Labs (CDTL) to perform independent lab reviews of next generation INFOSEC products. Years ago, ahead of the BYOD market shift, he founded NetClarity, Inc. (http://www.netclarity.net), the world's first next generation agentless, non-inline network access control (NAC) and bring your own device (BYOD) management appliances vendor based on a patented technology he invented. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. A dynamic speaker, he's presented at two White House Summits on cyber security, the RSA Conference, CSI, and many others.He served as an informal advisor to President Clinton and helped the President's Critical Infrastructure Protection Board, under the Bush Administration, which is now known as the National Infrastructure Advisory Council (NIAC) and operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace.Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), he serves on the advisory board of MITRE on the CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (http:// www.NAISG.org).

Visit Gary online at http://www.cyberdefensemagazine.com.

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.

marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com
Cyber Defense Magazine - rev. date: 2/25/2013

Our Promise:
Electronic Editions of Cyber Warnings Monthly Mini-Magazine and our Annual Edition of Cyber Defense Magazine are FREE, Always.
No strings attached.

Secure the Cure

Donate

IT Security Professionals Tax-Exempt
Non-Profit, helping fund the search for
the cure for Cancer and help those in need.

Tel: 1-210-639-8652
Twitter: @securethecure
Web: www.securethecure.org

SECURETHECURE.ORG IS DEDICATED TO HELPING FIND THE CURE FOR CANCER