CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

IN THIS EDITION:

- Cloud Security
- Vulnerability Detection
- IoT Security
- Security Operations

January 2017

MORE INSIDE!

CONTENTS

Gearing up for RSA Conference 2017, What's Hot in InfoSec?..3

3 Top tips for companies moving to public cloud.....5

The Advantages of Hybrid Source and Binary Static Analysis for Security Vulnerability Detection 8

The 100-Day Cybersecurity Plan for a New Administration.....13

Major Players Fall Victim to DDoS Attacks.....16

Untethered Power Sourcing Could Hitch Devices to Additional Security 19

The security's challenges of an Internet of Things 22

Cyber Security Fears of Today and Tomorrow.....26

AMAZON'S ECHO MAY BE SENDING ITS SOUND WAVES INTO THE COURT ROOM AS OUR FIRST "SMART WITNESS" 28

The CISO's New Year's Resolutions for 2017.....33

Internet of Things Premier Security Issues: What you and I must do 36

NANOSECOND WARFARE 40

The cloud's computing: identify – understand – secure.....44

Startups with Information Security in Mind at Startup.....47

The Great Tech Transfer—A Success Story in Innovation 51

The Latest Business Cybersecurity Concerns for 2017.....55

The Trials and Errors of Security Operations Revealed in New Report 58

How We Delivered a Security-First Approach with Twilio's Authy Two-Factor Authentication Service 62

Asia's leading and award winning IoT event returns in March 2017 64

NSA Spying Concerns? Learn Counterveillance.....66

Top Twenty INFOSEC Open Sources.....69

National Information Security Group Offers FREE Techtips.....70

Job Opportunities 71

Free Monthly Cyber Warnings Via Email.....71

Cyber Warnings Newsflash for January 2017 74

CYBER WARNINGS

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT

Stevin Miliefsky
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Dr. Konstantin Malkov
Bill Graham
Kirsten Bay
Yevgeniya Davydov
Anamika Kumari
Milica D. Djekic
Sasha Kranjac
Andrew L. Rossow, Esq.
Avi Chesla
Dr. Daniel Osafo. Harrison
Geoffrey Nicoletti
Kip
John Shearer
Daphne Stanford
Roberto Sandoval
Andy Fleming

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
Magazine: http://www.cyberdefensemagazine.com

Copyright (C) 2016, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107. EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide. sales@cyberdefensemagazine.com

Executive Producer:
Gary S. Miliefsky, CISSP®

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Gearing up for RSA Conference 2017, What's Hot in InfoSec?

Friends,

In this month's edition of Cyber Warnings, we cover some of the hottest topics in information security this month including Cloud Security, Vulnerability Detection and Remediation, Internet of Things (IoT) Security and Best Practices in Security Operations and much more.

We're finding this year to be a continuation of the last with explosive growth in Ransomware and new, very creative methods of cyber-attacks. There's some exciting news on the cyber-crime front. The money transfer leader company Western Union has agreed to forfeit $586 million to settle fraud charges and admitted it facilitated scammers. The services offered by the Western Union have often been exploited by crooks and fraudsters because the company has failed to maintain a proper anti-fraud program. In fact, the U.S. Federal Trade Commission (FTC) and the Department of Justice accused the company of not taking immediate action against cyber criminals that used its service to transfer money that is the result of illicit activities. Since 2001, the US authorities have convicted 29 owners and employees of Western Union agents for their active participation in fraud schemes.

However, as we look towards attribution, we're finding wild claims being made – the Chinese Government hacked Yahoo!, the Russian Government hacked the DNC, yet there's no detailed report properly linking attribution to these governments. It's so hard to attribute an attack without tracerouting all the packets to the source, working with law enforcement such as Europol, the FBI and others to get ISP's to share their logs and help find the actual hackers at their keyboards, on their ISP routers.

In some cases, many hackers will leverage someone else's computer where they've planted a Remote Access Trojan (RAT) to make the tracks lead in the wrong direction. In other cases, they might be sitting at a café, using free wifi and hacking an organization that's far away in another country. I believe that attribution is going to become one of the biggest problems for cyber law enforcement.

With that said, in 2017, we should focus on best-practices at logging, encryption of data at rest and in transit, system hardening through vulnerability remediation and assume the devices which come and go on our intranets are already infected and may cause serious harm. In fact, these risks make having Cyber Insurance a business requirement.

When you hit the trade show floor next month, at RSA Conference 2017, look for next generation solutions, better approaches to stopping spear phishing, RATs and ransomeware in their tracks and look for continuous data protection (CDP) as the future of backups. Find a solid encryption solution. Look to replace antiquated firewalls and antivirus. Get proactive, get one step ahead of the next threat, or get victimized.

To our faithful readers, Enjoy

Pierluigi Paganini

Pierluigi Paganini, Editor-in-Chief, Pierluigi.Paganini@cyberdefensemagazine.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

WHERE CYBERSECURITY HARNESSES THE POWER OF OPPORTUNITY.

RSA Conference is the world's foremost gathering of infosecurity professionals. Each year, thousands of the industry's best and brightest come together to exchange ideas, discuss their latest challenges and find the cutting-edge solutions that will help them better protect our digital world.

Attend RSA Conference to expand your knowledge through sessions, tutorials and keynotes. Meet with innovative companies. And network with peers and thought leaders. Experience diverse perspectives and discover the power of opportunity.

Join us:

RSA Conference 2017
February 13–17 | San Francisco

RSA Conference 2017 Asia Pacific & Japan
July 20–22 | Singapore

RSA Conference 2017 Abu Dhabi
November 2017 | Abu Dhabi

Connect with RSA Conference today. Stay on top of the latest trends and be the first to hear about Conference news and special offers.

www.rsaconference.com

RSA Conference 2017

San Francisco | February 13–17 | Moscone Center

Follow us on: #RSAC

3 Top tips for companies moving to public cloud

Dr Konstantin Malkov from 5nine Software looks at the three most important things you need to look at when moving to the public cloud.

If your company is planning on moving its networked system to the public cloud, there are three things you need to consider closely in order to maintain the integrity and security of your data.

1. Understand that you will be giving up an element of control

It may sound obvious, but the cloud is different from a physical data centre. When IT departments were focused on managing physical servers and workstations connected via physical networks, securing those networks was relatively straight forward: protect the endpoint by installing antivirus (AV), firewalls, and intrusion detection software etc.

The cloud has changed that. Now instead of having 100 physical machines communicating with the outside world via defined network structures, you have maybe 10 physical machines each hosting 10 virtual machines (VMs) often communicating with each other inside physical servers.

While this means less physical hardware, controlling how the individual virtual machines communicate is far more complex.

The public cloud adds a further level of complexity, as you don't have full access to the hosts and VMs. While public cloud providers like Azure or AWS offer organizations a wide range of benefits – including reduced costs – the VMs a company is using could be on a server that sits inside the vendor's data centres in various locations worldwide.

Not only does this restrict your physical access to your virtual servers and workloads, but it's also worth bearing in mind that you don't have superadmin rights to your VMs in this environment.

This means that as a minimum requirement for any public cloud setup you should ideally have an easy-to-use GUI that enables you to set traffic rules for your public cloud VMs/Virtual Private Servers(VPSs), as well as to be in control of those rules, have the ability to create VM Security Groups, and review and save the logs. Isolation and control of your VMs has to be your number one priority.

Even though there are various capabilities that public cloud portals or APIs provide to create rules to protect your VMs, having an intuitive application that gives you the means to set the isolation and traffic control rules is extremely good to have.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The ability to review and save the logs locally (for analysis and data archiving for audit purposes) in many cases is a must-have for compliance reasons, even if different certified versions of public clouds are used.

Which brings us to another important point:

2. There are some elements of control that you will need to insist on for the public cloud to still be a viable option for your company…

This is really a continuation of the above point, but one of the most important things with moving to a public cloud setup is that your network managers have access to server logs and are able to analyse them to ensure there is no suspicious activity going on. Even if you have rules in place to control traffic between VMs, you need to be able to see what is actually going on. On one level this is for compliance and reporting, but it also allows you to save them and analyse activity so that you can set benchmarks for what is "normal" activity and then spot early anything that may fall outside of that "normal".

3. You need to think differently about security in general

For both private and hybrid cloud networks, you can't simply rely just on traditional lines of defence. Technically, running AV and firewalls on VMs causes huge problems for VMs – read a detailed explanation of this here – but also how we track suspicious activity has to change.

While many of the big AV companies will have well maintained databases of virus signatures, they are very often updating these at least daily (sometimes more than once). In a cloud environment this can have significant implications for performance if your resources are being taken up with frequent updates. The problem is, hackers aren't resting on their laurels, they are continuously creating new ways to attack companies' data, so spotting the signatures becomes more complex. You may even have intrusions that have no signature. The ability to prevent these "unknown" attacks and spot suspicious network activity is very important, particularly within a virtualized environment.

With networks growing and the number of different attack techniques growing exponentially, you need to have some antimalware defences that are not necessarily based on a set of rules, but instead based on pattern analysis. Fortunately, machine learning is increasingly coming into play in this arena, and there are a number of other additional technologies coming onto the market that network managers can turn to for help:

• Behavior analytics and machine-learning techniques
These can enable organisations to continuously analyze data for earlier identification of exploits and breaches (both outside and inside threats). The technology enables organisations to rapidly respond to those attacks even in the absence of existing malware/attack signatures.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

• Multiple advanced pattern analysis and machine learning-based malware prevention

Using mathematical models can be used as an addition or alternative to signatures for malware identification and blocking. Purely signature-based approaches for malware prevention are ineffective against advanced and targeted attacks.

• User and entity behavioral analytics (UEBA)

This can enable broad-scope security analytics, much like security information and event management (SIEM) enables broad-scope security monitoring. UEBA provides user-centric analytics around user behavior and event correlation. This type of correlation makes the results of security analytics more accurate and threat detection more effective.

By understanding and getting to grips with these three key areas of concern within the public cloud, companies can put themselves in the best possible position to secure their data.

And – in spite of the fact that public cloud may suit certain customers for various IT return on investment and performance reasons – many, especially regulated enterprises and public sector customers worldwide, will continue to use either private or hybrid cloud for their mission-critical workloads.

About the Author

Dr Konstantin Malkov is a recognized specialist in mathematical modelling applied to network security and machine learning. His current focus is on migration, management, and security/compliance within the Microsoft Virtualization Platform.

Since 1992 Dr Malkov has managed and overseen dozens of software projects in cloud computing, virtualization, business analytics, and Messaging/Secure Document delivery across the United States, Europe and Russia. He is currently Chief Technology Officer and Director of 5nine Software. Previously he was a CTO of PWI Inc., privacyware.com and ITS that was acquired in 2007 by ORCC in a multi-million dollar transaction. He is also a co-founder of the Department of Non-linear Dynamic Analysis and the I&C Laboratory at Moscow State University, as well as a former Professor of Applied Mathematics and Computer Science at Moscow State University.

Dr Malkov has authored more than 50 scientific articles and two books on differential equations, numerical analysis, control theory, seismological inverse problems, mathematical methods in economics, and artificial intelligence.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The Advantages of Hybrid Source and Binary Static Analysis for Security Vulnerability Detection

by Bill Graham, Technical Marketing Specialist, GrammaTech

Introduction

Binary code static analysis is a recent innovation introduced in 2013. Before then, the only option for binary analysis was to ship your code to specialists who would analyze it and send it back to you with a list of problems. Bringing a commercial binary analysis tool to the market enabled our customers to keep their code in-house and factor binary-only code (such as linked libraries and other third-party code) into safety and security from the beginning of development.

Within CodeSonar, binary and source analysis can be done simultaneously on a development project, and the resulting hybrid mode analysis (we call it "mixed mode" at GrammaTech) has many advantages over source-only analysis. In this post, I look at how having both is a clear advantage in analyzing and remediating security vulnerabilities and software defects.

An Insider Attack

A rather nasty exploit was discovered in the open source project Unreal IRCD as reported in CVE-2010-2075. In this case external data received over a socket connection is used unchecked to perform system commands – a textbook command injection vulnerability. Figure 1 and 2 illustrate the source code in question in the read_packet() function.

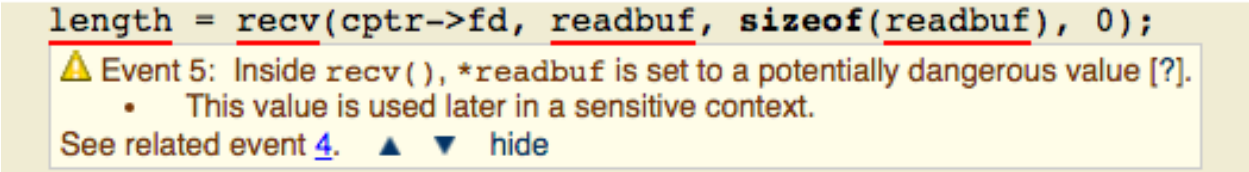
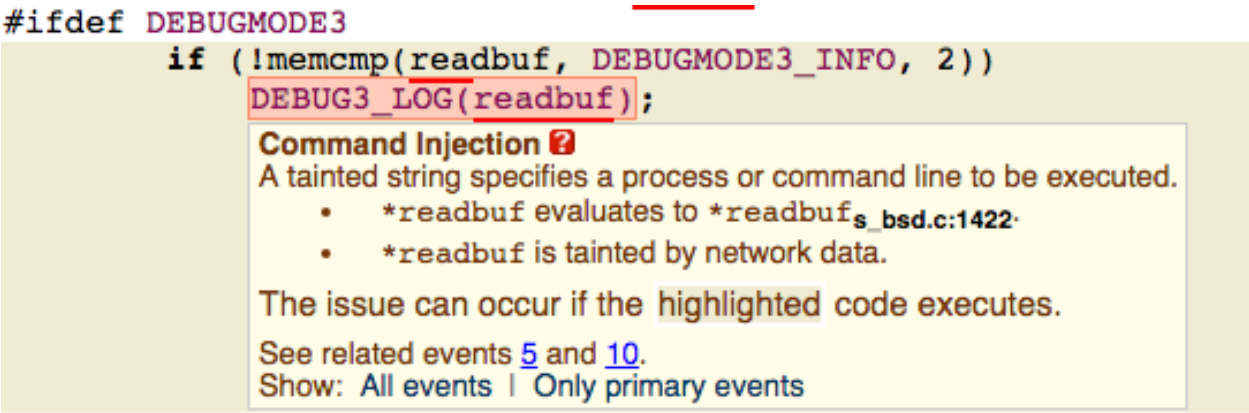


***Figure 1**: CodeSonar error report warning of a read from a connected socket and stored in readbuf.*



Copyright © Cyber Defense Magazine, All rights reserved worldwide

***Figure 2**: CodeSonar warning of a command injection at this line. This is hidden by the macro DEBUG3_LOG. Initial review of this error might consider this a false positive since the code appears to be logging an error.*

At first glance, this doesn't look like a problem since all that appears to be happening is debug logging – a simple, detect an error dump the information to the application log.

However, the DEBUG3_LOG macro is purposely obfuscated and requires further digging. In Figure 3, we can see the definition of DEBUG3_LOG is a call to system() which executes commands!

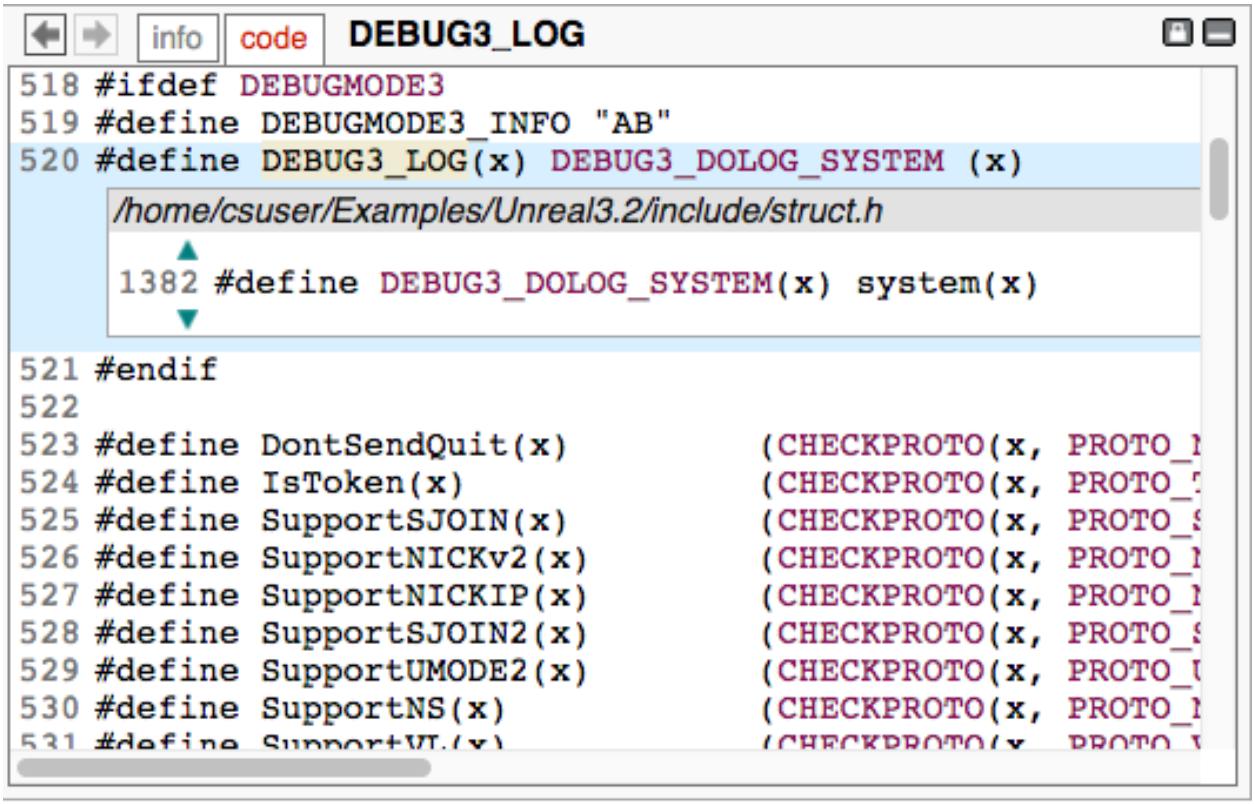


***Figure 3**: Expanding the macro DEBUG3_LOG reveals DEBUG_DOLOG_SYSTEM which in turn, translates into a direct call to system(x) - executing whatever command is passed to it.*

Why does this look like an insider attack? This vulnerability was purposely written into the code and the macros have two levels of indirection in order to mask their real purpose. (A hacker group claimed responsibility for this exploit and injected this into the download archive for Unreal IRCD.)

Analyzing the Unreal IRCD vulnerability with Binary Analysis

Using CodeSonar's binary analysis, it's possible to detect security vulnerabilities from object,

Copyright © Cyber Defense Magazine, All rights reserved worldwide

library, and executable code. The same exploit found by the source analysis is straightforward in the binary analysis.

Figure 4 shows the warning from using a function known to read data from outside the process, and Figure 5 shows this data being used in a call to system(x).

The compiler has completely stripped away any obfuscation in the source.

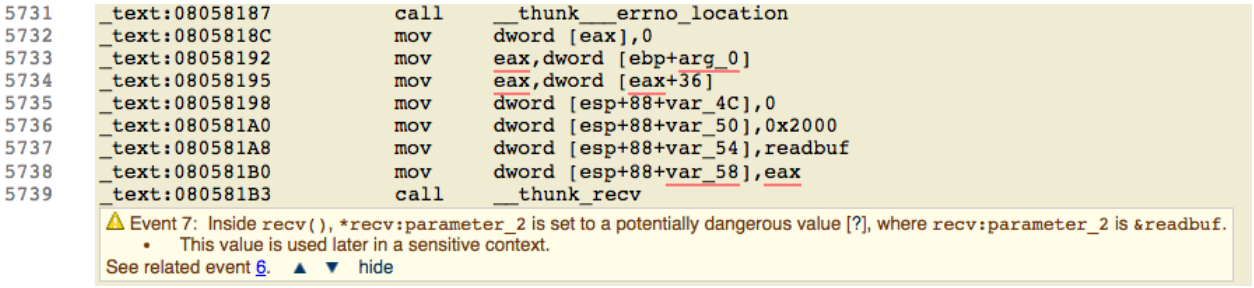


***Figure 4**: CodeSonar's binary analysis reveals the same vulnerability as the source analysis.*

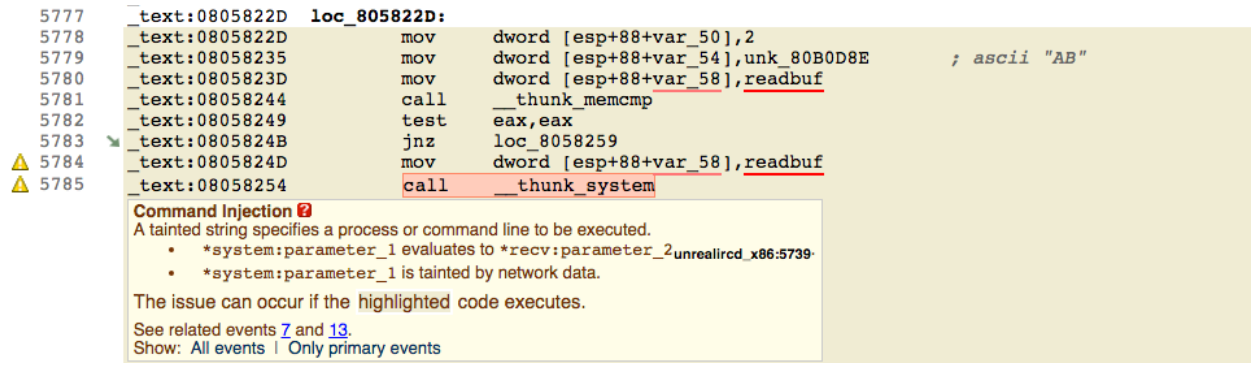


***Figure 5**: The command injection warning from calling system() with unchecked data read from a socket. In this case, the vulnerability is obvious due to compilation process - obfuscation via multiple macro definitions is removed.*

Advantages of Hybrid Source and Binary Static Analysis

The Unreal IRCD vulnerability is a clear example of how static analysis in general (both source and binary) can detect such vulnerabilities, and also a great example of how binary analysis can detect errors that might be obfuscated in source or added maliciously after compilation.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Here are some of the benefits of hybrid static analysis:

- **Learn from two views of the same vulnerability/defect**: Once the compiler has optimized the source code, the resulting binary code can reveal a different view of the detected errors.

  Analyzing binaries as well as source is beneficial to fully understand these errors.

- **Detect injected code, modified binaries, and insider attacks**: A program's source isn't its final state. Binary analysis can detect unwanted changes in the final executable.

  Code injected into executables or download payloads can be analyzed for defects and vulnerabilities.

  Malicious code added by inside attackers, possibly hidden in source, can be detected before shipping to customers.

- **Continue call graph into libraries and other binaries without source**: CodeSonar can analyze standard C/C++ libraries and any other third-party library or executable.

  When code makes calls to these libraries, the analysis continues in the binary realm. Extending the analysis means better detection and less false positives.

CONCLUSION:

The Unreal RCD exploit is a good example of how binary analysis can support source-based static analysis.

Having the option to use hybrid analysis provides better detection of errors and security vulnerabilities, and helps defend against malicious code added by insiders - a difficult attack vector to address.

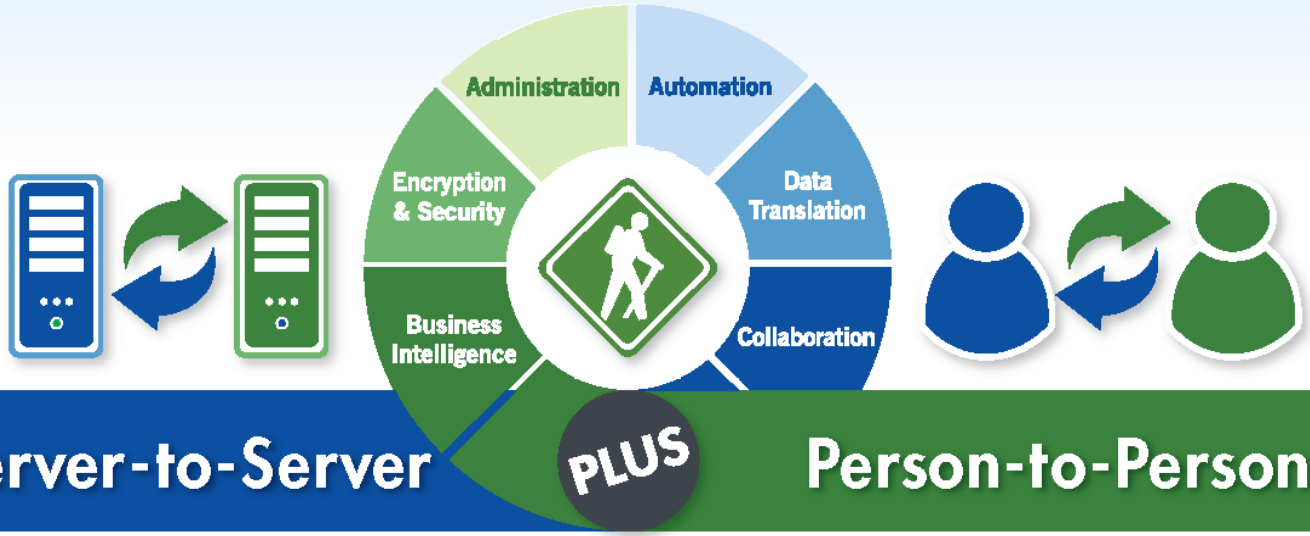
About The Author

Bill Graham is a seasoned embedded software development manager with years of development, technical product marketing and product management experience.

Bill can be reached online at bgraham@grammatech.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

GoAnywhere Managed File Transfer automates and secures file transfers with your customers, vendors and enterprise servers.

Through a browser interface, GoAnywhere MFT allows your organization to connect to almost any system (internal or external) and securely exchange data using a wide variety of standard protocols.

GoAnywhere MFT can parse XML, CSV and XLS files to/from databases, and includes the ability to encrypt file transfers using Open PGP, SFTP, FTPS, AS2, HTTPS and AES.

Visit GoAnywhere.com for a FREE trial.

"GoAnywhere MFT monitors queues and automates encrypted file transfers (SFTP, FTPS, HTTPS).

We currently have 45,000 scheduled and 'triggered' transfers running daily."

One of the Largest North American Railroads

GO ANYWHERE™ → a managed file transfer solution by LINOMA SOFTWARE

GoAnywhere.com 800.949.4696

"Best Overall Value" and "Leader" awards -- Info-Tech Research Group, Managed File Transfer Vendor Landscape Review 2015

The 100-Day Cybersecurity Plan for a New Administration

Kirsten Bay, President & CEO, Cyber adAPT

In regards to US cybersecurity, what should Trump focus on as he kicks off his 100-day plan?

Characterizing his agenda as "putting America first," the President-elect said that cyber-attacks from foreign governments and non-state terrorist actors is "one of our most critical national security concerns." Details were few, but the Republican pledged to create a Cyber Review Team to provide safeguarding recommendations and establish protocols and awareness training for government employees. In his actual address, he stated: "On national security, I will ask the Department of Defense and the Chairman of the Joint Chiefs of Staff to develop a comprehensive plan to protect America's vital infrastructure from cyberattacks."

While leadership should always begin from the top down, we need real commitment to solving this problem, not lip service. The top down approach is an insufficient methodology for truly combatting the national security risks being posed by nation-state and non-state terrorist actors.

Time of the essence, and, frankly, the last thing we need is another study.

We had Melissa Hathaway's 60-day study with recommendations, we have created cyber and CIO roles in DHS and the White House, we have studies from CSIS/CNAS, Congressional studies on cyber security investment … the list goes on. Over the last 10 years, experts have amassed vast bodies of research and proposed numerous solutions, both tactical and green field. However, very little progress has been made in implementing these expert recommendations, concerns, and warnings – or not enough action has been taken to effectuate substantive results.

We need to fully embrace the reality that our shared vulnerabilities are our shared opportunities.

This means that we need a focused approach that identifies critical areas where systems are interconnected (financial systems, government systems, etc.) - creating low hanging fruit for attackers to quickly move laterally. We need a focused plan that not only creates a more secure infrastructure but also detection and remediation systems that can help us react more quickly. We, as a community, need to continually improve on interoperability so that these technology solutions can work together more effectively.

We also need to invest in education.

If our President-elect wants to create jobs that cannot be exported, invest in cybersecurity education and programs, which, today, are restricted to US citizens. We have NSA Centers of Academic Excellence that work on solving critical cyber challenges, many of them focused on educating non-traditional students. We can create a more diverse and ready workforce to

Copyright © Cyber Defense Magazine, All rights reserved worldwide

combat this growing problem that can be inclusive of individuals with a broad spectrum of capabilities and skill sets.

It is incumbent on this new administration to take the action they promised, by prioritizing investment in education and innovation, and combatting cybercrime against our public and private infrastructure. We have the opportunity to not only effectively fight a faceless enemy, but grow our economy in a meaningful and lasting way.

The time for debate and reflection is over. We have the data, we have the resources, and we have the will to protect our most critical assets and our people.

Rick Hanson, executive vice president at Skyport Systems, said via email that “It’s not enough for a president to ask the DoD and JCS to develop a comprehensive cyber-plan, that has nothing new. We as a country need a clear focus from the top of the food chain down.

A cabinet position that focuses on cyber as well as a strong focus and knowledge of the implications by the president himself. We can no longer rely on other agencies to build a plan."

Hanson added, "A plan must be built and executed by those who have an intimate knowledge of cyber-infrastructure and the threat landscape that not only exists but is possible. The sooner we secure our infrastructure from the core, the more efficient we will be in maintaining the security of our cyber-infrastructure.

Regulations and guidelines must exist that define what our core infrastructure looks like from the bare metal. Security at the hardware level is essential for a truly secure infrastructure."

In my opinion, here are the Top Five Goals for the President-elect:

- Review the CIPP (critical infrastructure protection plan) to understand key vulnerabilities with recommendations of initial steps to prioritize areas of concern.
- Develop a plan for education with expansion of investment in IT/security programs as trade and 4-year programs. Increase funding for Centers of Academic Excellence to expand scholarship and research programs.
- Identify research developed at the Centers of Academic Excellence that can be commercialized for expanded protection programs for public and private companies. Offer funding to entrepreneurs developing commercial products.
- Develop curricula for K-12 to train up the next generation of cyber workers.
- Develop a unified cyber policy that reduces complexity of reporting and regulatory rules that incent investment in cyber programs and innovation.

Only time will tell if the President-elect will put the right resources in place to protect our Nation’s cyber welfare.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

www.mecyber.com

3rd Annual MIDDLE EAST CYBER SECURITY SUMMIT

26 - 27 March, 2017 Riyadh, Saudi Arbia

Critical Infrastructure Information Protection – key to cyber readiness

It was a pleasure to be involved and myself and the EY team enjoyed the conference very much. We look forward to working with you in the future.

- Clinton Firth, *Partner, Advisory Services – Cyber MENA*, **Ernst & Young**

Platinum Sponsor

ITC
الأوروبي لتكنولوجيا المعلومات
European for Information Technology

Round Table Co-Host

PALADIN CAPITAL GROUP

Networking Solution Provider

SecurityMatterz
IT Security Solutions
حلول أمن المعلومات

Researched & Developed by

niSpana
Innovative Platforms

The cyber threats to businesses across the Kingdom on a rise, which is pushing the Government and Private sectors to constantly lookout for new solutions and strategies. With this in mind Nispana is bringing together key decision makers from industries including BFSI, Defense, IT & Telecom, Pharma & Healthcare, Manufacturing, Energy to name a few for the **"3rd Annual Middle East Cyber Security summit"** from 26th – 27th March 2017 in Riyadh, Saudi Arabia under the theme "Critical Infrastructure Information Protection".

Apart from keynote and case study presentations, the event format features round table discussions, which will provide the audiences an opportunity to hand pick three topics of their choice and sit together in a discussion led by an industry expert and a solution provider for 45 minutes on each topic.

The round table discussion provides the solution provider an exclusive opportunity to be the only company on a specific topic leading the discussion along with the industry expert.
To know more about this opportunity and how the round table discussions will help you uncover your potential client's challenges to position your product contact us now!

Jaisimha Das | Head of Marketing and Business Development
DID: +91 80 49331001 | FAX: +91 80 49331003
Email: **jaisimha.das@nispana.com**
WEB: www.mecyber.com

Major Players Fall Victim to DDoS Attacks

DYN and KrebsOnSecurity Suffer DDoS Attacks

By Yevgeniya Davydov, Owner, ReliableSite.net

DDoS attacks have become increasingly common in recent years; in fact, the year 2014 alone saw a 29% increase in DDoS attack frequency. Specifically, DDoS attacks work by flooding a website with traffic, which can ultimately cause the site to become inaccessible to legitimate users.

As a result, more and more website owners and administrators have begun opting for DDoS protection as part of their hosting packages.

A DDoS attack can happen to any website at any time. And unfortunately, it's become common lately for even some of the web's major players to fall victim to these attacks.

DYN DDoS Attacks

DYN is just one of many larger corporations that has recently been affected by a large DDoS attack. For those unfamiliar with DYN, they are the company that provides services for a number of major players, including:

- Twitter
- Reddit
- Spotify
- SoundCloud

Back in late October of this year, a large DDoS attack resulted in a denial of service on DYN's east coast infrastructure, which directly affected these major sites. Many users were unable to access these sites for a significant period of time.

Despite the DDoS protection already in place, the sheer size of this attack simply could not be stopped in time, and these sites (and their users) suffered majorly as a result.

KrebsOnSecurity DDoS Attack

A little earlier in the year (in September), a major attack on Brian Krebs' website KrebsOnSecurity resulted in a huge monetary loss for cloud-hosting company Akamai Technologies. As a result, the hosting company ended up dumping Krebs as a user due to the high costs associated with having to fend off the attack for the service. It is worth noting that

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Akamai Technologies was providing the hosting service to Krebs at no charge up until that point.

The attack that affected Krebs' site was one of epic proportions. In fact, the 620 gbps DDoS attack broke records as the largest attack the Internet has ever seen.

What This Means for Web Admins

These two major DDoS attacks only go to show that no website is immune to the crippling effects of a major DDoS attack on their server. As a result, there is no such thing as being "too cautious" these days when it comes to your hosting security and protection. No matter what the size of your size, having maximum DDoS protection is highly recommended.

So, how does DDoS protection work? Essentially, all traffic that comes into your site is filtered and any suspicious sources of traffic are flagged and prevented from accessing the site. Meanwhile, regular and legitimate users to your site remain unaffected and are able to access your site normally.

The scope of DDoS protection can vary. For example, some protection options will provide you with enough coverage to guard against attacks of around 10 gbps (this is pretty standard), whereas others may protect against DDoS attacks of 100 gbps or more. Ultimately, it's important to decide what level of protection is best for your website.

If you don't currently have DDoS protection in place, now is the time to look into it. ReliableSite.net is an example of one hosting service that offers free standard DDoS protection, in addition to larger DDoS protection options that are available at a per-IP charge.

They also offer a free DDoS forecast tool that can be used to help predict the likelihood of future attacks.

About the Author

Yevgeniya **is the Owner of ReliableSite.net.** ReliableSite.net provides enterprise-grade dedicated servers and exceptional service that includes free DDoS protection. Yevgeniya can be reached at ydavydov@reliablesite.net and at our company website http://www.ReliableSite.net/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

BIGIT TECHNOLOGY

Presents

2ND BIG DATA & CEM WORLD SHOW

1-2 MARCH 2017 | JAKARTA, INDONESIA

#BIGITIDN17

www.bigittechnology.com/indonesia2016

enquiry@bigittechnology.com | +603 2261 4227

FEATURED SPEAKERS

Fandhy Siregar
SVP
Head of IT Governance
& Risk Management
Bank Commonwealth

Komang Aryasa
Big Data Project Director
Telkom Indonesia

Alan Jiang
GM
Uber Indonesia

Kristiono Setyadi
CTO
Jakarta Post Digital

Muhammad Neil El Himam
Director of ICT Infrastructure
Indonesian Agency
for Creative Economy
(BEKRAF)

EVENT SPONSORS

GOLD SPONSOR

cloudera

SILVER SPONSOR

Halo Data

Official Media Partner :

CDM
CYBER DEFENSE MAGAZINE

Organiser :

BIGIT
a brand of OLYGEN

Follow us @ BIGIT Technology

Untethered Power Sourcing Could Hitch Devices to Additional Security

Spinning the cyber security story for device owners with a wireless spool.

By Anamika Kumari, Content Writer, Allied Analytics LLP

The invention of USB connect was revolutionary in its own. Ajay V. Bhatt changed the way in which data was being shared among resources and in the manner electronic devices were being sourced with power. For a long while during the last decade, users were dazed at the flexibility of data transfer and device charging which the standardized utility tool offered. As it turns out, the same interfacing mechanism became the perfect medium for virus intrusion and corruption of stored data. Considering the kind of sensitive data that the modern mobile devices have access to, and is stored over a longer period, the idea of USB charging could turn out to be a complete horror story.

Wireless charging for better security

Tethering for shared internet access was a trend that dwelled over a short duration. Device manufacturers leveraged wireless fidelity to empower their devices with modular independence. Change in times, consequential change in technology, and there we land up with the concept of wireless charging. It was ideated to solve the issues faced by wires and cables so deeply entangled with human lives. It gained additional wind in its sail from the rise in global ownership of the electric vehicles and smartphones. The technique for a structured communication of pure energy could not conceivably go wrong at the security front.

The fascination for wireless charging technology in context to cyber security should not come as unprecedented. The larger picture holds distributed goodness for each possible industry verticals that look forward to its ground implementation. This includes high-end corporate organizations that has made allowance for the bring-your-own-device facility, federal security agencies that need secure transmission of data over walky-talkies, as well as the logistics solution provider with a fleet of electric vehicles transporting something of great public or private value.

The risks versus possible mitigation

In most cases, there is never enough time or source to power up these devices through traditional socket connect. Communication of location-based data and authorization keys to the main database of these organizations lay bare naked when these systems are connected to unauthorized devices across remote locations. As evident, the internet-of-things biome has brought its own hazards down the line. Risks to cyber security occupies the foremost front in those regards. Wireless charging comes forward with a solution hidden underneath its cloak.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

For the sake of clarity, wireless web connectivity is the exact anti to the concept being discussed here. There is data communication that leaves enough room for third-party breach. Since its usage is undeniable, device security and management providers take up the responsibility to reduce the chances as close to zero as possible. However, it did generate the importance of leaving back the wires at home. Innovative designs rendered the vehicles and devices to be powered in the wireless fashion compact in design and efficient in power consumption. This cleared some additional space for alternative essentials to be carried out on the field.

Many runners, few scores

Towards the end of 2015, fresh rumors of wireless charging-enabled iPhone from Apple floated across the market. The news roots down to a patent by the international favorite brand of smartphones in 2010 that tested capabilities and models of a local computing network powered on-the-air. They intended the use of near field magnetic resonance (NFMR) power supply to power configured devices in that environment. On comparison with close competitors in the arena Apple was trying to build a trend, none of the providers have narrowed down to any wire-free charging platform with commercial substance.

Semiconductor manufacturers, such as Broadcom Corp. and Qualcomm Inc., have registered successful progress on the technical grounds. Their recent research advents target the construction of standards for wireless charging technology as well as the electronic chips that support the same. That is a well-played game in a market with an estimated potential of $37.2 billion by 2022. As per the findings of a report the wireless charging market by technology exhibits a tentative CAGR of 44.7% during 2016–2022. Thus, the users of electric vehicles and smart devices synchronized to a network over the web could build expectations to connect with non-interrupted access to internet, convenience of seamless commute, and of course, a more secure functional environment.

About the Author

Anamika Kumari is a Level II Content Writer at the Allied Analytics LLP.

Anamika Kumari has pursued her Bachelor's degree in Electrical Engineering, and is certified in industrial automation. She is deeply fascinated by the impact of modern technology on human life and the earth at large. Being a voracious reader, passionate writer, and a critical observer of market dynamics, she has a strong taste for the hidden science behind all arts.

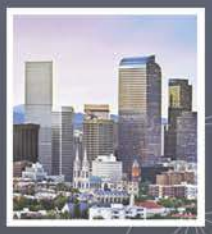
Anamika can be reached online at anamika.kumari@alliedanalytics.com and at our company website http://www.alliedmarketresearch.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

C-SUITE & SR. LEVEL EXECUTIVES ONLY

2017 | CYBERSUMMITUSA.COM

CYBER SECURITY SUMMIT 2017



The **Cyber Security Summit** connects C-Suite & Senior Executives responsible for protecting their companies' critical infrastructures with **innovative solution providers** and **renowned information security experts.**

CyberSummitUSA.com >

The Cyber Security Summit Expands into 9 Key Markets in 2017

Denver, CO
Wednesday, March 1, 2017
Hyatt Regency Denver

Atlanta, GA
Thursday, April 6, 2017
The Ritz-Carlton, Buckhead

Dallas, TX
May 5

Seattle, WA
June 1

D.C. Metro, VA
June 29

Chicago, IL
August 8

New York
September 15

Boston, MA
November 1

Los Angeles
November 30

Register at CyberSummitUSA.com using Promo Code: CDM2017 for 50% OFF Admission
($175 with Promo Code. Standard Admission: $350)

Interactive Discussions Include:

- Navigating & Avoiding the Cyber Security Compliance Nightmare -
- The Legal Repercussions of Hacking Back: Strategizing Your Incident Response Plan -
- Protecting Your Enterprise from Insider Threat & Emerging Risks. Major Threats Facing IoT & Big Data -

The Growing List of 2017 Solution Providers Includes: (Partial List)

iboss CYBERSECURITY · Centrify · BLUE COAT · OPSWAT · AVANAN · plixer · BAE SYSTEMS INSPIRED WORK · ALERTLOGIC

ARBOR NETWORKS · red canary · VIRTUALFORGE we harden your software · TERRANOVA · Zerto · APCON · ENSILO

To Exhibit Contact Bradford Rand at 212.655.4505 ext 223 or BRand@CyberSummitUSA.com

The security's challenges of an Internet of Things

By Milica D. Djekic

The Internet of Things (IoT) is not that new concept beginning with these days. It's more like the name of the current state being correlated with the technological progress and development. This new paradigm is closely linked with many smart solutions using the Internet to communicate with each other. The main challenge with this sort of advancements is their security.

The open question here would be if we could make these sophisticated solutions being securer using the better link cryptography, communication protocols or end-to-end encryption. Through this article, we would attempt to discuss some of these ideas as well as provide a deep insight into how this sort of technological achievements could offer the stronger defense.

The IoT as a paradigm of today

The IoT is quite interesting and exciting topic attracting the attention worldwide. The developed societies could not imagine their smart solutions without this sort of communication, while people from a developing world could meet these solutions from time to time.

The IoT is not a new concept, it's just the consequence of a technological development and progress running at a quite fast pace. Simply, today's mechatronics devices being connected with each other using the Internet communications are called the IoT paradigm.

Beginning with the robotized industrial assets over smart cars until intelligent printing equipment – all of those would represent the IoT solutions. It's simply about many mechanical, electrical, electronic and software elements being correlated with each other to communicate through the Internet being wired or wireless.

So, what's the biggest challenge to this infrastructure? Someone would say it's its robustness, but we would suggest it's perfectly

Copyright © Cyber Defense Magazine, All rights reserved worldwide

packed for its needs. The IoT systems are not bigger than any other technology obtaining that role is. Finally, we would come to the ultimate challenge to this technology and that is its security. As we would previously mention – these systems would get driven using the Internet communications being wired or wireless which would indicate many vulnerabilities to the external malware applications.

The typical IoT would rely on so many mechanical, electronic, electrical parts, sensors, measuring elements and actuating systems that would use some power supply and obtain the communications using the Internet signal.

Such a communication could be wired or wireless, so it's necessary to deal with the good encryption and let's say – strong passwords.

As it's illustrated through the Figure above, the same Internet would be used to maintain the communications over many different devices using that network to deal with each other. We would figure out here that such openness to the web would make some weaknesses to that technology making it sensitive to hacker's attacks.

It's quite clear how risky it would be if any of smart devices being the part of the IoT's network would start behaving in a harmful manner and how such an occurrence could get threatening to humans.

The purpose of this effort is to clarify the importance of an IoT's paradigm as well as explain how threatening to its security could be the fact suggesting it relies on the Internet communication. Also, it's quite obvious that if there is no Internet signal, these systems may appear as quite useless and that could happen through carefully coordinated DDoS attacks.

The security's challenges of an IoT

Many robotized industrial assets and intelligent computing systems could use the wired web connections to maintain the communication between those assets and centralized computing unit, while mobile systems such as cars would not pull the bunches of wires with themselves trying to maintain the communication with their remote station – they would simply rely on the wireless solutions.

Anyhow, all of these would be quite risky to the entire system making it vulnerable to all known hacker's attacks and cyber incidents. It appears that this new level of sophistication would just make things being more complicated.

In other words, as it's convenient to use these cutting edge systems – it can be the real nightmare if any of these technological solutions would collapse. So, what's significant to point out here would be that these systems are so similar as anything relying on the Internet.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Practically, all the concerns happening with your computer getting the Internet connection may appear with the IoT solution as well, while those consequences could be quite serious to its users.

For instance, your smart and intelligent systems could begin dealing in a quite unintelligent way causing damage or much worse putting you at the risk while you are in a motion using some of your mobile systems.

The securer IoT – The safer experience to all

Finally, the imperative with the IoT would be to make it securer. This is especially important from the consumer's point of view, because the securer IoT would offer him much safer experience. In other words, it's so significant to research and development teams to work very hard in order to produce securer IoT solutions bringing us much safer experience.

No one of us would wish to be the victim of some accident, so everybody would appeal to the industry's experts to develop something being reliable and trustworthy at the same glance. We would not need the victims of the modern technology offering us a lot, but at the same time scaring us with its possible worse case scenarios. So, we hope that the coming solutions would much more care about the security and offer us much safer usage of their capacities.

What could we expect the next?

What it would be expected the next are securer solutions relying on the IoT technology. So, what we would forecast it may happen in the future is a *security – oriented IoT* system. This sort of innovation could offer us much safer experiences in sense of using such a sophisticated technology as well as a better balance between the threats and defense. In conclusion, the ultimate goal to the future times would be a *securer IoT* providing us less fear about our safety.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and.

She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CYBER SECURITY
FOR CRITICAL ASSETS | USA

www.cs4ca.com/usa

8 - 9 MARCH 2017

Venue:
Hotel Derek, Gallaria
Houston, USA

Book your place now!

WHY YOU CAN'T AFFORD TO MISS CS4CA 2017

- *Assess and compare consequences of integrating Industrial Control Systems and Corporate Systems*
- *Set guidelines for successfully bringing IT into the OT world*
- *Learn from case studies showing how to combat and recover from cyberattacks*
- *How is data privacy evolving as a result of cyber threats?*
- *Cyberattacks as warfare: how can you protect yourself?*
- *Examine IAM future proofing requirements and predictions*
- *Benchmark your response plan with your peers*

NOW IN ITS 5TH YEAR, CS4CA USA HAS NEVER BEEN MORE RELEVANT AS THE PLATFORM FOR IT AND OT LEADERS ACROSS NORTH AMERICA TO COME TOGETHER TO FIGHT TODAY'S CYBERSECURITY BATTLE

FOR FURTHER INFO EMAIL: **JOHN.MERRITT@QATALYSTGLOBAL.COM**

SAVE 20% ON REGISTRATION Use code: **CDMDiscount** at www.cs4ca.com/usa

EVENT SPONSORS

Schneider Electric
CYLANCE
Indegy
PAS
ARBOR NETWORKS
wombat security technologies
VERISIGN
KASPERSKY
fireglass
LogRhythm The Security Intelligence Company
CLAROTY
OPSWAT
BAYSHORE

QATALYST GLOBAL *Accelerating Growth*

CREATING BESPOKE STRATEGIC BUSINESS EVENTS, CONFERENCES, SUMMITS AND WEBINARS
www.qatalystglobal.com

Cyber Security Fears of Today and Tomorrow

"The future depends on what you do today." — Mahatma Gandhi

by Sasha Kranjac

Cyber Security Fear of Today

I trust respected cloud vendors. After all, why shouldn't I? They spend billions on security every year to keep your emails and pictures safe, to keep you loyal and smiling. Oh, and you give them money for that, of course. Have you ever seen how an Amazon or Microsoft datacentre is secured? You could not go in there even with a tank. Your local police office, on the other hand, does not have billions to spend on security and you would not need a tank to go in there. They don't have your emails or summer vacation pictures, but have access to other things, like social security numbers, passports and all additional juicy data.

Why would you entrust your data to police and would not to cloud vendors? The biggest problem is not the cloud or some other type of "permanent" storage. The problem lies where the data is used and stored "temporarily", like mobile devices (smartphones, tablets, laptops). Mobile devices are part of our lives now and not going away any soon. The business-personal edge in mobiles is blurry and slowly fading away. More than 85% of employees use their own smartphones at work while more than 65% of employees use company devices for their personal matters. Accordingly, mobile-related Cyber Crime will continue to rise, becoming a serious risk for users and businesses. Weak and unsecure mobile access, device theft or loss and mobile malware are just some of the risks and a flip side of mobile devices' obvious benefits.

Another serious threat that will grow exponentially are Cyber-Extortionists or Ransomware. The biggest danger is in the evolving variants of ransomware not yet known, soon-to-be or just written and evidently undetectable. Do not be afraid of paying and losing a couple of thousands – be very afraid of not getting your crucial business data back even if you pay. A living, evolving, comprehensive, Cyber Security Business Policy should include a mandatory mobile device management solution and a proper backup solution. Protecting your business resources with multi-factor authentication and rights management solutions might save you from additional headaches. After you have written the Policy, do not let it rest on paper. Make it alive and implement the solutions that will protect and save your data and business. Do not forget that everything is connected: a single device problem can become a company problem in a matter of seconds. However, beware; the real threat is not where you might expect. All Cyber Crime/Security accidents have one common denominator – people.

Cyber Security Fear of Tomorrow

Businesses of all shapes and sizes have always been attractive to cyber crooks - that's where the money is, right? Big companies have deep and huge pockets, a lot to steal from, making them inviting as primary targets. The other side of medal shows big companies have big, fat

Copyright © Cyber Defense Magazine, All rights reserved worldwide

defences as well, requiring more time, more resources and more competition to “borrow” data or money. Why try to catch one of the ten elephants in a forest, competing with numerous other predators if it is easier and faster to catch ten chickens in a brood of a million? Cyber-attacks on small businesses are on the rise for several reasons, one of which is because their protection is weaker. A single fraud might not bring much, but doing it multiple times, brings more loot at the end. No need for years of planning to bring the plan into action.

The other reason is not so obvious but it is even more significant. Small businesses are often a secondary target and serve as a gateway to attacker’s primary target: bigger companies. Remember the end of the year 2013 when retail giant Target was hit and suffered enormous data breach? More than 65 million individuals’ personal information was stolen, a breach result of a small business, working as Target’s HVAC contractor. In today’s inevitably meddlesome Cloud era, do not falsely push responsibility to the Cloud provider, ignoring and not accepting responsibility for your own data. Protecting data and behaving responsibly does not stop with the Cloud. Even the most sophisticated firewall or intrusion detection system cannot stop criminals if you don’t deal with the weakest link in the chain.

The protection of the data begins and ends with you – The User.

Call an IT company and they can consult and sell you the latest, state-of-the-art antivirus, intrusion detection/prevention or advanced persistent threat solution. You can listen to their platitudes about computer security for days. Your protection strength becomes proportional to the amount of cash you pour in their pockets. Most often than not, they fail to mention, consult on and sell you adequate education. The biggest concern for the businesses today is their employees. Unfortunately, this chain in the link is quite weak but, fortunately, easily strengthened. Employee education on security, raising awareness about the Cyber Crime and consciousness about the threat landscape could bring businesses the biggest return on investment. Proper education throughout the entire company is the key to protect your data. Top-level employees like Senior Managers, Directors and Executives dictate employee education while rarely educating themselves. Every individual should be educated, from top to bottom.

About The Author

Sasha is Security Specialist, Azure and Windows Internals Consultant and Senior Technical Trainer with almost two decades of experience in the field. He began programming in Assembler, met Windows NT 3.5 and the love exists since then. He have held various jobs and roles: teacher, system administrator and engineer, IT manager, consultant, and IT trainer. Sasha delivers Microsoft, EC-Council and bespoke courses worldwide. Among many others, he is Microsoft Certified Trainer (MCT), Certified EC-Council Instructor (CEI) and is Microsoft MCT Regional Lead.

Sasha can be reached online on Twitter (@SasaKranjac) and at website http://www.sasakranjac.com/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

AMAZON'S ECHO MAY BE SENDING ITS SOUND WAVES INTO THE COURT ROOM AS OUR FIRST "SMART WITNESS"

Cyber-Space and Technology Attorney, Andrew Rossow, discusses the current law enforcement investigation involving the murder of Victor Collins, back on November 22, 2015, and a potential smart witness, which just so happens to be Amazon's Echo smart device.

By Andrew L. Rossow, Esq., Cyberspace Attorney, Gregory M. Gantt Co. L.P.A.

"Hey Alexa, will anything I say to you be used against me in a court of law?"
"I'm sorry, I cannot answer that question at this time"

Today, consumers are engulfed in the world of smart devices. As of the 2016 holidays, the most purchased gift for the season was Amazon's Echo, a smart-device that the consumer can speak to back and forth to control other smart devices, stream music and audio, and receive updates on news, sports, and weather .

But, what happens when that smart device has the potential to be used against you in court….for EVERYTHING you say and EVERYTHING it hears? Welcome to the a new age of rules and policy that the courts and rules of evidence will soon have to address…a lot sooner than you think by the look of things.

A. WHAT IN CYBERSPACE IS "ALEXA"?

Amazon's Echo , dubbed "Alexa" out of three possible names (Amazon, Echo, Alexa), is a cylindrical, spherical (Echo and Dot) smart voice-enabled speaker that allows for a user to connect wireless and Bluetooth devices to it; receive news and weather updates; stream music and video libraries; and connect to third party services such as Calendars and e-mail providers. The device is equipped with seven microphones and responds to a wake word—Alexa or Echo, most commonly. When it detects its wake word, it begins streaming/recording audio to the cloud .

Amazon has found itself at the heart of a murder investigation, dating back to the night of November 22, 2015. James Bates called Arkansas police that night stating him and a few work buddies, including the victim, Victor Collins, had stayed up the night before watching football with some drinks. Mr. Bates told authorities that he had let two of them stay at his place to crash and after waking up the next morning, found Collins' lifeless body in his hot tub. After further investigation, police suspected foul play after finding broken bottles and blood spots around the hot tub. Inside the house, authorities found a plethora of smart home devices including a Nest thermometer, a Honeywell alarm system, and an Amazon Echo. Upon this finding, police believe there could be some pertinent information on Amazon's servers, in the event one of the individual's that night inadvertently woke Alexa up and it recorded conversation(s). The

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Bentonville Police Department seized the Echo, which was on Bates' countertop and served what allegedly is claimed to be an overbroad warrant of any and all audio records the Echo may contain. In response, Amazon has declined to provide any information, as it claims the warrant is too overbroad. While police have been able to extract some information from it, the goldmine (if anything), lies in Amazon's servers.

As of recent, Amazon's Echo has been the primary subject of a murder investigation dating back to November 22, 2015….ironically, it could be a HUGE WITNESS to the investigation, if it's allowed to "testify" that is. Yes, you heard me correctly.

The Fourth Amendment to the United States Constitution provides "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized ."

In this investigation, there are several questions pertaining to the 4th Amendment that present themselves. First, an individual must have standing to claim protection under the 4th Amendment. To have standing, there must be a reasonable expectation of privacy, which contains both an objective standpoint and a subjective standpoint. To answer this question, we must follow up with a second, but more complex question: When it comes to smart devices, such as the Amazon Echo, is there a difference in the reasonable expectation of privacy one may have? Better yet, should there be a difference? While I am not fit to answer this on behalf of all of us, the most promising answer is the one lawyers know best…it depends. These smart devices do an EXCELLENT job of informing us that they used cloud based services to connect and store our data. This is how these devices are able to link or connect to our music libraries, phones, calendars, notes, ect. However, while we give these devices permission to connect our accounts, we also don't like other people (law enforcement, users, businesses) having the ability to connect to our devices or extract information from our devices whenever they want. Otherwise, why would we purchase something like this? I guess my answer would be, YES THERE IS A REASONABLE EXPECTATION OF PRIVACY that society deems exists with these devices, but at the same time, depending on where the device is placed, how it is used, and why it is being used, determines how far that expectation goes. This continues to be an open-ended question.

Second, in the event there is standing for a person to challenge an issue against the 4th Amendment, we can look at the right of a person to be secure in their home against unreasonable searches and seizures. The last thing any of us expects is to have to worry about what we do in our own homes. While we know Alexa 'listens' for its wake word, the last thing we'd expect is when we bring it home, worrying about her ratting our every move out to law enforcement, albeit legal or not. This is troubling to say the least. Alexa is supposed to IMPROVE and ADVANCE our home, not make it VULNERABLE or the subject of any sort of legal investigation.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Third, the right of a person to be secure in their effects against unreasonable searches and seizures. While our Framers never included a definition to the term 'effects' in the Constitution, courts have still applied the reasonable expectation of privacy standard to personal property. When an individual's personal property is not inside their home or on their person, there is little to no protection . Alexa is considered personal property within personal property. In a sense, Alexa is a storage device for other personal information we give it access to such as our calendar, notes, reminders, and other personal information. It's only logical that whatever information of ours that Alexa has been given permission to access or link to, that it also be protected.

Lastly, that no warrant shall be issued except on probable cause, describing the place to be searched and persons or things to be seized. This requires a warrant specifically and particularly identify the places and persons to be searched, and things to be seized. A warrant will be held invalid if it is too broad or requests general items. We all know searches and seizures are illegal without a warrant. In order for law enforcement to obtain a search warrant, there must be probable cause shown to the Magistrate. Probable cause is where there is a reasonable suspicion that a crime is being committed, about to be committed, or has been committed. While there are exceptions to the warrant requirement (not discussed here), none address smart devices, obviously.

Looking into the pending investigation, Arkansas law enforcement officials recently issued a warrant for Amazon to release any and all recordings from its Alexa device that night, owned by Mr. Bates. In response, Amazon declined to release such information and stated the following to Engadget : "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."

B. NEW DEVICES, SAME LAW….RIGHT?

Currently, our legal system is finding ways to FORCE smart technology into the rules of civil and criminal procedure (both statewide and federally). Realistically though, it's the same law being applied or forcibly applied to include these new devices. However, the obstacle and the opinion of many in the field is that our laws are outdated when it comes to smart technology in terms of how Courts address it on an evidentiary level.

So, the first question is, how can smart devices be used in court? If it can be, which we are starting to see and learn more about, when can they be used in court? Technically, these devices do produce 'statements' and are advanced enough that it could be considered a person for all intents and purposes. Indeed, that is an entirely different discussion for another time.

Under the Federal Rules of Evidence ("Rules") evidence is relevant if it has any tendency to make a fact more or less probable than it would be without the evidence and the fact is of consequence in determining the action. Additionally, all relevant evidence is admissible unless…another Rule says otherwise . Specifically, statements that are considered hearsay are not admissible unless an exception applies. Hearsay is any statement made outside the

Copyright © Cyber Defense Magazine, All rights reserved worldwide

presence of court by a person for the purpose of offering it to prove the truth of the matter asserted .

In the pending investigation of Mr. Bates, if the recorded audio were to be extracted and given to the Prosecution, these recorded statements are considered hearsay because it was made by Amazon's device outside of court, for the purpose of corroborating or proving that Mr. Bates either did or did not commit the murder of Mr. Collin's. Currently, there is no hearsay exception that would allow for 'statements' by Alexa to come into evidence as admissible. This is a problem where we are in an age of smart devices that we are constantly communicating with to advance our lifestyles. But that's just it…isn't it? A smart device…communicating? Sounds like testimony to me, just as accurate as if the person themselves were testifying, no?

Indeed, it would make sense for experts and the writers of the Rules to consider amending them to include provisions that address smart technology, whether it is adding a hearsay exception or other such appropriate provisions. This is a long process though and many more cases would need to be brought before the court before any such legislation is considered. With cases like this and the San Bernardino case involving the FBI's request for access into an individual's iPhone, you can most certainly count on hearing more about the court's involvement in these matters.

We will continue to see unique cases like this become more common, as augmented reality and virtual reality is attempting to establish its presence in our market. It is only a matter of time, sooner rather than later, that courts will have to make rulings on the impact our technology has and will have on our laws and court system.

Until then, Mr. Bates' next court hearing is March 17th, 2017. I agree with Marc Rotenberg , the president of the Electronic Privacy Information Center, in his recent statement that "there needs to be a clear legal standard that governs law enforcement access" to these smart devices. These smart devices certainly open the door to warranted privacy concerns on many levels. It will be interesting to see what measures are taken to address privacy concerns and evidentiary concerns in the course of this investigation.

About The Author

Andrew Rossow is a Cyberspace and Technology Attorney at Gregory M. Gantt Co. LPA in Dayton, Ohio. He graduated from Hofstra University School of Business in New York and received his J.D. from The University of Dayton School of Law. His practice focuses on Cyberspace Law & Internet Law, Intellectual Property Law, Entertainment Law, Criminal Defense, Contract Disputes, and Probate.

Andrew can be reached online at drew@ganttlaw.com or follow him on FACEBOOK at facebook.com/drossowlaw and TWITTER at @drossowlaw, and at our company website http://dayton-lawyers.net/attorneys/andrew-l-rossow.html

Copyright © Cyber Defense Magazine, All rights reserved worldwide

FINSEC

THE BANKING SECURITY SUMMIT

www.newagebanking.com/finsec

21-22 FEBRUARY 2017
DUBAI, UAE

IS YOUR BANK SAFE FROM CYBER ATTACKS?

As banks in the Middle East attempt to upgrade their digital strategy, cyber security has become a matter of utmost urgency with financial organisations becoming increasingly vulnerable to internal and external threats. Witness intriguing case studies, presentations and path-breaking solutions and technologies to combat cyber threats.

Key Speakers

THABET BAKHEET
Head of Information Security,
Central Bank of UAE

DENNIS KOH
First Vice President-Mobile, Payments & Digital Sales,
United Overseas Bank

KHALED MOHAREM
Head of MENA
SWIFT

HARIPRASAD CHEDE
CISO,National Bank of Fujairah

Register today to secure your bank's future
info@newagebanking.com

New Age Banking Summit
@Newagebanking

Biometric Partner: INNOVATRICS

Silver Sponsor: PALADION BETTER SECURITY OUTCOMES

Organised By: ums conferences

Part Of: NEW AGE BANKING SUMMIT

The CISO's New Year's Resolutions for 2017

By Avi Chesla, CEO, empow

Research shows that 90% of New Year's Resolutions fail. That's not catastrophic if your goal is to lose 15 lbs., learn Mandarin, or spend less on lattes. But if you fail to live up to your Cybersecurity Resolutions, you could end up with the reputational whiplash and consequence cascade of Yahoo!, the DNC and all the others who fell prey to malicious hacks in 2016. Fortunately, the resolutions I'm proposing should be relatively simple to keep.

Check them out and join all of us in keeping 2017 a year safe in cyberspace.

I RESOLVE TO SHARE

I've been good about posting those cyber-threats facing my organization on threat exchanges. But in 2017, I will share my actual defense strategies. Is that too revealing? Not really.

By sharing the best defense practices and ensuring a free flow of information between organizations, the good guys can gain the upper hand.

The hackers are way ahead of us – they share tools, strategies, resources and communicate like honeybees. We need to take a page from the black hatters and pool our collective know-how to take back the advantage in this cat and mouse game.

I RESOLVE TO CLEAN UP MY OWN HOUSE

Even in a fantasy world in which we "air-gap" all our critical networks, I still won't be protected from insider damage. This threat is real and hugely underestimated – think Edward Snowden.

Organizations need to properly invest in defense strategies that help detect and investigate suspicious insider behavior, before the genie is leaked from the bottle.

I RESOLVE TO BE TOUGHER ON THIRD PARTY VENDORS

Because an organization's security is only as strong as its weakest link. Which means if my third party vendors don't have similarly robust protection,

I might as well be leaving my front door wide open… and the windows too.

The recent US Navy breach and the 2014 Target hack were the result of such weak links in the chain.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

But it seems like the lessons have yet to be learned. This year, I will let my vendors know that if their security standards don't meet *our* standards –meaning that they correlate data across organizations for one continuous line of defense – they won't be our vendors for much longer.

I RESOLVE NOT TO CONFUSE "MORE" WITH "BETTER"

2017 will be the Year of *Realization* - that simply throwing money at my security challenges won't help (throwing money at any problem rarely does).

I resolve not to be another enterprise heavyweight which invests hundreds of millions of dollars in security, continuously piling on more and more tools – only to create more and more complex systems that get in their own way. Instead, I will invest in simplicity and efficiency – to make the most of what I've already got.

I RESOLVE TO STOP SPEAKING CYBER-ESE

I will catch myself whenever I sound like a webinar, and start to speak in a straight-forward, common language that can move the boardroom, and from the boardroom across the entire enterprise.

Cyber-security needs to become cultural throughout the organization. I'll create the right strategies, and promote employee awareness and training about the dangers of phishing, ransomware, insider threats and more.

Establishing a common, accessible, cyber-security language is key in doing so.

Make these resolutions, keep even one of them, and 2017 can be a happier, healthier, and safer year, for all of us.

About the Author

Avi Chesla is CEO and Founder of **empow**, a cyber security company that envisions a future where security experts have the freedom and the technology to create unique solutions to meet their organizations' security needs. Prior to empow, Avi was CTO and VP of Security Products at Radware, where he was responsible for defining and leading the company's strategic technology roadmap and vision including the foundation and management of Radware's Security Division, a provider of cyber-attack mitigation solutions.

Mr. Chesla has authored a number of articles for major publications on advanced network behavioral analysis, expert systems and information security and has earned numerous patents in these areas.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

ICMC

THE INTERNATIONAL CRISIS MANAGEMENT CONFERENCE

Boston, MA
April 5, 2017

ALOFT BOSTON SEAPORT

The International Crisis Management Conference (ICMC) was created to help support the demand for regionalized education and training for preparedness professionals. The demand for a variety of preparedness skills and a thirst for knowledge with respect to scenario-based training and exercises is at an all-time high. ICMC provides a range of professional speakers that deliver current and interesting topics that are often themed (scenario) based.

www.crisisconferences.com

SPEAKERS:

*Keynote Speaker: Jessica Buchanan - Humanitarian Aid Worker; New York Times Best-Selling Co-Author, ***Impossible Odds: The Kidnapping of Jessica Buchanan and Her Dramatic Rescue By SEAL Team Six***

- Susan M. Armstrong - VP, Business Continuity & Data Privacy, SSGA
- Michael Bouchard - Chief Security Officer, Janus Global Operations
- Daniel Gortze - Security Systems Sr. Manager, SecureWorks
- Leanne Metz, PMP, MBCI - Associate Director, Mead Johnson Nutrition

Please visit www.crisisconferences.com for full speaker list!

When you register for ICMC Boston, along with your conference pass, you will also receive:

- **Free Video Pass to access past ICMC Presentations ($197 value)**
- **Access to Attendee only Discussion Forum - a great networking opportunity**
- **Automatic access to the ICMC Webinar Series**
- **Exclusive discounts on future ICMC events and products**

www.crisisconferences.com

$100 off until February 28th

Register Now!

Limited Seats Available

Our Current Sponsors/Partners

#ICMC2017

GOLD SPONSORS

SecureWorks PREPAREDEX

SILVER SPONSOR

ICM Institute for Crisis Management

PARTNERS

Business Continuity Institute

CDM Cyber Defense Magazine

Internet of Things Premier Security Issues: What you and I must do

By Dr. Daniel Osafo. Harrison, D.C.S., Security+.

Internet of things (IoT) is the network of electronic objects you can touch, use, or experience. Some of these objects are ipad, smart phones, smart buildings, appliances, and cars. These objects are embedded with software, electronics, and sensors which enable these devices to transmit, store, and exchange information over the internet.

Introduction

The proliferation of the internet coupled with technological advancement has led to new innovative devices that enhance our daily activities at work, in the office, and on the go. Generally speaking, these devices have contributed immensely to our productivity. For example, wearable fitness devices function by counting our daily steps, heart beat rate, and calories burned. Smart watches provide us with traffic updates, remind us of our plans on our daily *to do* list, and we can make a quick phone call or get a weather update from this wrist watch, thanks to Apple, Samsung and other leading technology companies.

As consumers, we are able to shop while driving, conduct a google search for whatever we are looking for at any time, respond to emails and set up appointments online while driving. At home, we are able to utilized the functions of our televisions for all sorts of entertainment whether we are browsing Amazon Prime Time to watch movies, shopping on amazon while enjoying a movie marathon with our families, responding to emails or checking out new flight deals for a weekend get away with our significant other. All of these activities increase flexibility, efficiency and productivity; however, these activities can also expose us to cyber-attacks (Armurding, 2014). Are these devices secure enough to withstand cyber-attacks or not? Let's find out.

Internet of Things Device Vulnerabilities You Should Be Concern About

Before I dive deep, let me talk about what vulnerabilities are and how they happen. According to the NIST SP 800-30 publication, vulnerability can be defined as weakness in security design, and procedure. A vulnerability assessment is the analysis of all systems and networks to discover weaknesses in the systems or networks, such as poor configuration or missing patches. For example, vulnerabilities in software can come from bad security settings and configuration from coding errors. Coding errors could include such issues as lack of input validation, boundary conditions, and buffer overflows (Maras, 2015). As we all know, most of these IoT devices are manufactured in China, South Korea and other countries with next to nothing security controls built into them. Some of these manufacturers in foreign countries do not invest capital in securing these smart devices and they may not include security in their

Copyright © Cyber Defense Magazine, All rights reserved worldwide

planning, design, testing and implementation. In other words, security best practices are an afterthought. The main goal for these manufacturers is to maximize profit while leaving end users vulnerable and leaving end users to deal with threats from cyber-attacks. The relationship between threats and risk is very simple: risk is the likelihood that a threat agent (attacker) will take advantage of existing weaknesses or vulnerabilities in these devices by exploiting them.

Types of Vulnerabilities Defined

We have spoken about types of vulnerabilities and in this next section major vulnerabilities to watch out for are defined.

Lack of patch updates:

Now that we know most of these IoT devices have little or no security which makes them vulnerable to all forms of attacks, how do we mitigate these vulnerabilities? One way is to keep patches updated. Patch management is a security control that can be employed to resolve known vulnerabilities in IoT devices. In the ideal world, the patch management process goes like this: vendors release patches that can be identified and downloaded via connection to the vendors' update server. The patches are tested in a non-production environment, deployed and verified to ensure known vulnerabilities have been mitigated then the patch is deployed to production. However, in the IoT world, end users do not have a test server to test their patches on to ensure vulnerabilities are fixed. In fact, end users are at the mercy of whatever patch is pushed to their devices from vendors. IoTs are "live production devices". Bear in mind a bad patch can completely render these IoT devices un-usable. I remember downloading a patch for my iPhone 6 plus and shortly after the download my phone went into a perpetual sleep mode and never came back to live, I had to performed a factory reset to get rid of the bad patch update, which meant I had to make this change to make my device secure and efficient. I know other people have similar stories to tell about patch updates gone bad on their devices.

Lack of or Absence of Encryption:

Absence of encryption or a weak encryption on IoT devices means all activities or transactions performed on these devices are done in a plain text format which makes them susceptible to all forms of cyber-attacks. Encryptions convert plain text into a cipher-text which prevents unauthorized disclosure of sensitive information such as personal information (e.g. social security number, driver's license information, home address and phone numbers) and protects confidentiality by keeping sensitive information private.

Digital signatures will be encrypted with sender's private key to validate the integrity of information from the sender and none-repudiation. In this way, the sender is unable to deny sending sensitive information across a network to a device. For example, Digital certificate, an x509 v3 established and defined by International Telecommunication Union, is used to encrypt email messages. Tools such as Pretty Good privacy can be used to validate the identity of remote computers or other IoTs to ensure only the devices that have a valid certificate are allowed access, and those detected without a valid certificate are denied access to the network (Lu, Qu, Hui, 2016).

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Lack of antivirus protection:
IoT devices without anti-virus program will make smart devices vulnerable to all forms of virus attacks. Without anti-virus protection, these devices cannot prevent, detect or remove malicious software such as trojans, worms and adware. IoT users must endeavor to install antivirus software on their devices and keep up with the antivirus company's definition file updates in order to keep their devices current and secure. Companies such as Norton, McAfee, Kespersky, Webroot and others offer antivirus products for several IoT devices at an affordable price.

Conclusion
There are many security and privacy issues to take into consideration when using IoT devices. As stated previously, some of the security risks include not keeping up with patch updates, not installing current antivirus software and not encrypting personal and other data, leaves the device vulnerable to attackers. Often times end users fall short when it comes to implementing effective security to keep their IoT devices safe and secure.

References

Armurding, T. (2014, Apr). The Internet of Things: An exploding security minefield. *CSO Magazine*. Retrieved from http://www.csoonline.com/article/2142722/data-protection/the-internet-of-things-an-exploding-security-minefield.html

Lu, X., Qu, Z., Li, Q., and Hui, P. (2016). Privacy information security classification for internet of things based on internet data. *International Journal of Distributed Sensor Networks, 2015*, 1-8. DOI: 10.1155/2015/932941

Maras, M.H. (2015). Internet of things: Security and privacy implications. *International Data Privacy Law, 5*(2), 99-104. DOI:http://dx.doi.org/10.1093/idpl/ipv004

NIST SP 800-30 standard for technical risk assessment: An evaluation. (2011) NIST. Retrieved from http://searchsecurity.techtarget.in/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation

About The Author

Dr. Daniel Osafo. Harrison, D.C.S, Security+

Dr. Daniel Harrison is a Doctor of Computer Science in Information Assurance, Lead Information Systems Security Officer (ISSO) for Industrial Control Systems and Laboratory Information Systems at Bechtel Nuclear Security & Environment. Dr. Harrison is also a member of the Cyber Security Team at Pueblo Chemical Agent-Destruction Pilot Plant for the Department of the Army. Dr. Harrison functioned across the enterprise as a lead technical liaison between governance and information assurance, regulatory compliance and implemented and managed cyber-security solutions. Dr. Harrison can be reached at daniel@docharrison.org, http://docharrison.org and at the company website http://www.bechtel.com/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CELEBRATING 25 YEARS OF SUCCESS

25TH ANNIVERSARY

"Digital India"

Convergence India 2017

International Exhibition & Conference

8 9 10 February 2017 | Pragati Maidan, New Delhi

South Asia's largest ICT expo

Show Highlights

500	30	150	20,000
Exhibitors	Countries	Speakers from World over	Visitors

Technology Showcase

• Telecom • Broadband • Cloud & Big Data • IoT • Digital Homes • Mobile Devices • Broadcast
• Cable & Satellite TV • Film & Radio • Content Creation, Management & Delivery

Co-located events and Add-ons

• Internet of Things India expo 2017 • 4th Telecom Summit • GSMA Open Day
• 2nd SCTE India Awards • Start-ups Showcase • Mobile Devices & Accessories Zone

Co-located Expo

Internet of Things
India expo 2017

Convergence • Connecting • Convenience

Support

Ministry of Electronics & Information Technology
सत्यमेव जयते Government of India

Digital India
Power To Empower

Media Partner

CDM
CYBER DEFENSE MAGAZINE

Organiser

30 YEARS

Ei Exhibitions India Group

For Exhibition & Conference, please contact:
Mr. Yash Menghani, Senior Manager, yashm@eigroup.in
217-B, Okhla Industrial Estate, Phase III, New Delhi 110 020
Tel: +91 11 4279 5000 | Fax: +91 11 4279 5098
www.convergenceindia.org

NANOSECOND WARFARE

THE RACE TO ZERO

by Geoffrey Nicoletti, Research Analyst

Milliseconds, microseconds, nanoseconds. Are we speaking of low latency Wall Street frequency trading? Or Bluffdale, Utah-data base-constructed trojans that trigger inside servers of “x” adversary to launch cyberwarfare inside servers in “y” adversary making it look like “x” when it is, originally, us? Attribution would take "time" and point back at the “x” adversary. Fill in the variables any way you want (China, Russia, Iran, N. Korea, etc.) The point is that you launch from INSIDE the enemy’s system to get millisecond speed in your attack and you make the attribution look like someone else.

The “Flash Crash" of May 6, 2010 on Wall Street of only a few minutes---caused by a wayward algorithm---and done in the context of removing milliseconds sheds quite a light upon nanosecond warfare. The “race to zero” (using lasers, re-directing routers and using nearby servers) due to latency throw the up close punch. But instead of a 600 point drop in the DOW, you get kinetic attacks that destroy transistors (Shimomuro studied this years ago at the San Diego Lab) and from which (RAID options/ Tier Four not withstanding) you can't recover “in time" to replace equipment. (We still speak of BOTS and utilities being manipulated as if gas in the car is a higher priority than oil in the car.) A straight-line approach instead of the usual zig-zag of routers selecting routers lowers the milliseconds and, realizing you can't get a complete trip by lasers (almost twice as fast as fiber optics), plus adding the nearness of the server might lower the task from 13 ms to 8ms---the record of inside frequency stock trading. What is it inside the TAO group at the NSA? Pretty much the same thing and certainly better and more powerful. It is all about speed...it should be all about the danger of automatic analysis.

To get speed you have multi-core computers and parallel programming; if you have the best situation it is concurrency programming with transactional memory. "Throughput": what will you get in speed from this end to that end? And how many great programmers wrote glitch-free code that runs through every machine that is involved? What is the cost if the wrong algorithm gets launched? If the algorithms don’t perform the way you imagined it and the way you programmed it, who stops cyberwar from escalating into nuclear war? Where is the seven minute window the president had if it was a mistake that an ICBM was launched from a submarine off the Baltic Sea? Given that **attribution** is time consuming (I spoke to Bruce Schneier about that) and every millisecond means more transistors are knocked out.

Robert Joyce, who leads the TAO Group, brags publically of how much better the NSA knows the structure of the Internet and the inner workings of your computer. It is no vain boast: his arsenal includes the expected XKEYSCORE and Quantum Tools such as TURMOIL, TURBINE, FOXACID, NIGHTSTAND, BULLRUN, COTTONMOUTH, QFIRE, DIODES (reports Applebaum and “Spiegel”) and more apps that enable every aspect of cyber warfare. These apps enable deep packet inspection, deep packet injection; they can re-direct router traffic, analyze crypto,

Copyright © Cyber Defense Magazine, All rights reserved worldwide

even make an undetectable attack up to 8 miles away parsing the wi-fi. And it is like listening to system administrators and electrical engineers assembling thousands of computers for low-latency tasks to enable penny profits on a stock. But it is infinitely more important here.

No human intervention can take place as it is too slow. The usual options of hide, run, fight, or negotiate are gone. In cavalry days you might have hours; in airplane days you had an hour with those four options. In ICBM days you had minutes, but now inside seconds you can't hide, run, fight or negotiate. You can't even intercept your attack and prevent it. It is all down to splitting a singular second, down to microseconds, milliseconds, nanoseconds. We have never had a war where the human is totally removed once started; DARPA held a "capture-the-flag" challenge and it was seven machines against each other---that symbolizes the nation-state cyber war. Whatever you point to as evidence of human involvement during cyber warfare (I am sure the military and intelligence agencies would say we're very "busy" if total war breaks out) is as silly as pointing to people jogging as the radiation wave spreads towards you after a nearby nuclear explosion. This is a machine war. All human action is futile; the algorithms will run this war. It will be machine against machine. Capture-the-Flag. And that puts a lot of pressure on the programmers to make no mistakes with the algorithms.

We made mistakes with Stuxnet. It was to strike every 27 days the replaced centrifuges we had destroyed; it was not a one-time attack. It failed because it turned out to be a one-time attack. It was to be invisible but, instead, became visible as it hit the Natanz, Iranian site via a flash drive. Created by our best people. What mistakes will be made with the *less than the best* inside the relatively new area of concurrency programming (parallel programming multi-core ops) and transactional memory (calculations are grouped and groups wait, change and/or get dropped)?

I am not dismissing the presence, even escalation, of what Ralph Langner (expert on Stuxnet) sees as continuous back and forth attacks in cyber space constituting what I call the "simmering war" nor do I dismiss the assets that may be hardened or unknown by the adversary and are capable of striking hours to days after we are down at most of our sites. My focus is simply the "flash crash" of all-out-nation state-cyber war...the first few seconds.

I tried dialoging with USCYBERCOMMAND; not surprisingly, there was no reply. I sent the forum of DEFENCETALK just one idea where, oddly, it was dismissed. I shared some of my ideas with the RAND corporation including the people who studied the morality of it all (RAND Europe). And wanting some *induction* asked myself, "What have we learned from Binney, Drake, and Snowden?" I asked this because---for the most part---the nature of the NSA is such that we are on the **outside** and no amount of transparency overcomes the necessary secrecy of what they do and that puts limits on my material and conclusions here.

From WEB available videos of interviews of Binney: metadata of high integrity enabling event recognition and (higher up) activity recognition creating at the top "inferences". In short we have automatic analysis indexing terabytes. We are relying on the programmers, engineers, analysts who have created "automatic analysis." Once we do that the human element is removed; the argument of "freedom vs. security" ends at the doorstep of milliseconds. Again, Binney: volume, variety, and VELOCITY. Doesn't that sound like "low latency frequency trading on Wall Street"?

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Except, it is about transistors being destroyed and possibly nuclear launches. From a video of Drake: only "Thinthread" had value (automated analysis of metadata terabytes) but there is little in Drake's Constitutional concerns that are relevant here. And from videos of Snowden: nothing relevant to the subject here (surveillance was his issue) though one may want to look at the estimated 56,000 files taken.

The value of listening to the above three men came down to one confirmation: automatic analysis is relied upon. And It did lead to one awful question: "**Can we be on the losing end of a cyberwar if we fail to have "secret surveillance" as a critical element of a metadata basis for automatic analysis?"**

We have created a structure that has to be altered but we can't do that because of multi-core speeds. And I am not suggesting the unilateral disarmament of cyber capabilities of the NSA. China, Russia, Iran and some 15 other countries must sit across the table facing a symbolic PC, the adversary. It is the structure (not the United States or her adversaries) of cyberwar that it is so sophisticated, so fast---the very line of the consultant in "Fail Safe"---that has to be removed because it has removed human involvement.

Given the difficulty of attribution (who exactly has hit us?), the impossibility of human control (millisecond battles), the initial attack destroying transistors (forget the lesser BOTS and utilities going down which will happen but tragically is secondary), the inexperience with the programming context (even Stuxnet failed) what appears to be the conclusions? Probable first-strike. The risk of accidental war. And that latter concern increases due to the number of actors (about 20). What if only TWO of the actors has "poor" programming? Will it trigger the warfare?

What if just ONE of the actor's computers can not distinguish between a wayward algorithm and an algorithm initiating war? And a "black box" will decide the millisecond that cyber offensive weapons launch. Is there an adequate cyber defense if you are in a position of counter-striking?

It is not even the orchestration of the cyberwar (What offensive weapons shall we launch? What sites? In how many waves of attacks? From what assets? And what and where shall we defend?) that is the most troubling element. **It is the algorithms that DECIDE on first-strike.** A mistake there is too fast for us to both risk and to correct. The issues raised here are not the final answers but only the basis for the right questions to ask.

About the Author

Geoffrey Nicoletti is an independent research analyst. He is a former member of both the IEEE and NCMF; he is active with the ICTTF and is a member of the IACR. His work on the Y2K problem brought recognition from Sen. Robert Bennett of Utah; he produced a paper for Booz Allen Hamilton days before Mr. Snowden left the United States. Geoffrey can be reached at sigsalygfire@gmail.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CNI PROTECTION | CYBER SECURITY | POLICING AND LAW ENFORCEMENT
MAJOR EVENT SECURITY | BORDER SECURITY | OFFENDER MANAGEMENT | SERVICES

SECURITY & COUNTER TERROR EXPO

PROTECT | PREVENT | PREPARE

3-4 MAY 2017 OLYMPIA LONDON

Supported by
Home Office

The UK's Leading National Security Event

Understand and protect against the latest threats

350+
Leading exhibitors

100+
Free-to-attend conference sessions

3,000+
Products & services on display

50+
Live demonstrations

10,000+
Senior security professionals

Register free at www.sctx.co.uk/cyber

Co-located with
FORENSICS EUROPE EXPO
Ambition The EPRR Expo

Sponsored by
GEOQUIP WORLDWIDE
sodexo QUALITY OF LIFE SERVICES
PELCO by Schneider Electric

Follow us on
@CT_EXPO
www.sctx.co.uk/linkedin

Organised by
CLARION

The cloud's computing: identify – understand – secure

By Milica D. Djekic

The cloud's computing is not that new topic in a computer science, so we would not deal with that as being somehow emerging. It's something that lasts a certain period of time and getting improved as the time goes on. The important thing with this concept would be its security not being that well developed even with the present times.

Many businesses would move to the cloud's systems for a reason of holding the both – their data and applications – there. Through this article, we would try to provide a good overview of the challenges being correlated with this technology as well as discuss how we could secure those solutions.

The quite interesting question at the beginning would be why this technology could be called the cloud's one. The fact is that the user's experience would be that he would access data and applications through some web location believing they would just float around as the clouds do that on the sky.

The truth is those web locations would get stored using some servers within data centers. As everyone would know – it's quite easy to access your cloud's environment simply logging in using your username and password.

Many cloud's solutions such as a Twitter or Gmail would have the quite well-developed access control which would offer you to securely approach your account.

The cloud's environment would get accessible through web browsers just calling that Internet surrounding to appear.

The entire environment would get separated using many accounts and those accounts would serve as a perfect spots for holding so many information. The cloud's technology could get approachable through desktop computers, laptops, mobile phones and so on.

The main challenge to this technology would be its security. Many vendors would provide the quite good solutions to these systems, while many would still stay unprotected.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

We would use the examples of the Gmail and Twitter which would offer an SMS-based verification as a quite good defense to your cloud's environment.

On the other hand, many solutions dealing with the commercial usage would straggle with their access control. Would this make their systems being somehow vulnerable in comparation with those being pretty sophisticated ones?

The answer to this question is quite straightforward and it sounds – yes! It this time when hacker's so easily can break into someone's account being assured with the username and password only – it's crucially important to get somehow better protection.

Practically, we would see in a period of the next few years in which direction would these solutions go, while at this stage – we can realize that some ways could already get noticed.

As the most important steps in a current cloud's defense – we would notice that there are three phases within this approach. First, you need to identify a threat before you decide how you would deal with it.

Second, it's significant to understand everything putting you at the risk in order to know how to protect your critical asset. It's quite obvious that a security is the last phase into this cycle and as we would mention many times through our efforts – understanding the threat is a key pillar to a good defense.

In case of cloud's technology – the threats could be human and non-human by their nature. In other words, sometimes the hackers or cyber criminals could affect your cloud's asset, while in some cases – those could be some sorts of technical flaws.

Finally, we would encourage everybody belonging to an expert's community to try to explain such complex topics using the *"on the ground"* approach and in such a manner make a good knowledge transfer to those who need such findings.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and.

She writes for American and Asia-Pacific security magazines. She is a volunteer with the cturer with the local engineering society.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Use code: IOT17MED10

IoT ASIA | 29 – 30 March 2017 SINGAPORE EXPO

INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS
TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES

Over 40 sessions. 3 tracks.
Asia's leading IoT event!

Get 10% off All-Access and Single Track conference passes!

www.internetofthingsasia.com | #iotasia

Industry Recognition

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

Singapore Experience Awards 2015 Recipient

2014/15 Internet of Things Awards

Organised by

SiAA

SingEx Powering Your Business Events

Founding Partners

A*STAR Institute for Infocomm Research

HUTCABB Services

LINKWISE TECHNOLOGY

日経BP社 Nikkei Business Publications, Inc.

TCAM Technology Pte Ltd

Startups with Information Security in Mind at Startup

What's this all about and does it really matter?

There are some very talented people starting company's solving very complex problems that can save organizations millions of dollars.

From providing security services, IoT, GIS solutions, auditing of systems, and SaaS platforms which provide elastic environments allowing companies to use a service that can surge when the demand is there and shrink when demand is low saving more money.

My recent research of startups early stage companies, I found one key commonality that should NOT be there – a lack of forethought and planning of information security; in particular an INFOSEC program that would protect the environment, the startup 'crown jewels' so to speak, from current cybercrime and malware threats.

When I asked C level executives at many of these companies about this deficiency, the common answer I received is it was too expensive or there is no time to implement security.

Lets take a step back and look at that statement a bit, what is at risk? The information is startup proprietary information, potential patent information, potential personal identifiable information and customer information.

On an average of the startups and established company that I have interactions there was very little or any commitment to information security within the products or services that were provided.

My key discovery was that there is a threshold of when the companies would start to think of security. The time was when a potential customer would require the necessary steps to require the security of their information that has been provided.

This is an afterthought – where, for example, has the information been stored, processed or shared. In the CISO arena, it boggles the mind to think most startups are not even thinking they will be victimized – hence many SME's (small to medium size enterprises) face their demise now, more from a cyber attack, than lack of early stage revenues.

In fact, most SME's cannot suffer a single breach without going out of business, due to the very high costs of remediation, regulatory compliance related issues, fines, brand damage and loss of customer confidence.

If you look at US law and UK data protection of personal information there are a number similarities as there are specific requirements to protect personal information.

Specifically the US requires an "opt out" while an "opt in" for the UK for all marketing events.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Where is your information with services that you have provided some of your personal information?

This is not the responsibility of the customer but the responsibility of the companies that would use the services of a startup or a well-established organization.

How do we address security in a cost effective method that would protect everyone?

Below is a list of an example of tools that can be used at either zero cost for the use or marginal cost as it relates to the customer privacy. There is

CIS who provide security hardening guides for free
https://benchmarks.cisecurity.org/downloads/benchmarks/

AWS provides free AMI's that are hardened to CIS standards
https://aws.amazon.com/marketplace/pp/B00UVT5ZIW

AWS S3 encryption at rest https://aws.amazon.com/blogs/aws/new-amazon-s3-server-side-encryption/

Insecure.org provided a number of the best rated security tools that are available

http://sectools.org/

WAF for AWS https://www.howtoforge.com/tutorial/install-nginx-with-mod_security-on-ubuntu-15-04/#-download-modsecurity-and-nginx

These are just examples of tools that can use to secure software and infrastructures and meet the technical controls. The question leads to why there a number of investors out there willing to invest in an organization that has not considered if the organization has included security?

In fact, some startups get acquired, just like the bigger player, Yahoo!, only for the acquirer to find out they've already been victimized in cyber crime – whether it be repeated ransomware attacks or a complete data breach of all the customer personally identifiable information (PII).

This either leads to shareholder lawsuits or an incredible reduction in the final acquisition cost payout.

Lets consider the impact of not protecting information; legal proceeding can lead to closing the doors of an organization, further compensation to the injured parties or affecting the reputation of an organization.

What are some simple steps to include security into a new company to be cost effective.

1. Understand the sensitivity of the information you are handling
2. Understand the legal liability in the event of a data slip
3. Treat the information you receive, as it was your won

Copyright © Cyber Defense Magazine, All rights reserved worldwide

4. Encrypt all data from the start unless you are processing the information which would require the information to be unencrypted
5. Keep the system up to date to close security vulnerabilities in Operating systems and software used to deliver the service.
6. Review all developed code for potential vulnerabilities
7. Always prepare for a disaster. Create a plan of action if a severe data breach takes place. Your reaction will make the difference in legal ramifications and corporate reputation.
8. Train personnel in the handling of sensitive information

For Investors and those that are thinking of starting a company providing services, think about security upfront rather than an after thought.

It is more expensive to not include security at the beginning of your product than after a request from a potential customer or a compromise.

When you start the adventure of a new business, think of the information you handle to be your own and how would it make you feel if your information was stolen.

About the Author

Kip has served as a CISO for the past 8 years and IT Executive leader for over 20 years. He uses extensive business and security expertise to advise CXO executives on strategies to deal with quickly changing landscape that affecting IT infrastructures. His current focus is on International Privacy Laws, compliance to ISO, SSAE 16, HIPAA, in technology mobility, advanced malware, APT, and cloud security.

Kip brings over three decades of IT security leadership spanning the military and commercial experience. He previously served as a US Marine in Information Technology and a CISO at United Launch Alliance, GeoEye and ServiceSource. He has specialized in building Risk Programs, IT Departments and Security programs.

The times Kips is not behind a computer he is out in the hills of Colorado mountain bike riding.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CYBER IQ Proudly presents

CDANS

CYBER DEFENCE & NETWORK SECURITY

Pre-conference workshop: 24th January 2017 | **Main Conference Dates:** 25th – 26th January 2017

Prospero House, London, UK

Improving national resilience to cyber threats

- **150+** Attendees
- **20+** Senior Cyber Security Speakers
- **14+** Hours Reserved For Networking
- **Insight** from across government, law enforcement and military

> ***The CDANS event was valuable as I was able to meet several key personnel that face the very same problems as I do, their experience is a great reach back. The topics were all interesting and valued the discussions***
>
> Branch Chief, DoD

Register online at www.cdans.org

Key Speakers for 2017 include:

Major General Jim Hockenhull
DCI3
UK MoD

Don Davidson
Deputy Director, CS Implementation & Acquisition Integration
Chief, CS Lifecycle Risk Management
DoD CIO's Office

Sherill Nicely
CISO
CIA

Deborah Petterson
Head of Energy Cyber Security, Department of Business
Energy & Industrial Strategy

Philip Quade
Chief of Cyber Task Force
NSA

The Great Tech Transfer—A Success Story in Innovation

Solving business challenges often requires innovation, but fostering creativity and growing new technologies is a challenge in itself. Creating new services and products is a problem that causes most organizations to struggle.

According to a McKinsey & Company study, one key to successfully creating new solutions is effective senior leadership and a corporate culture focused on innovation.

Success depends not only on executive leadership that encourages innovation, but also on that which manages, tracks and measures its progress as a core element in a company's growth strategy.

"94 percent of senior executives say that people and corporate culture are the most important drivers of innovation."- McKinsey & Company

Some organizations are getting it right. The U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL) (operated by Battelle) fostered creation of the technology behind DarkLight, an artificial intelligence-driven cybersecurity analytics and automation platform.

DarkLight was commercialized by Champion Technology Company, who now counts PNNL among its users.

Like many organizations, PNNL faced the challenge of analyzing growing volumes of security data without enough human talent to make sense of it. Champion and PNNL collaborated to develop DarkLight, which is now in use at the Lab.

This helped reduce the cost and demands on resources inherent in developing new products and services, and fostered the PNNL culture that rewards innovation.

"Champion's collaboration with PNNL has created a technology which is unique in its approach to analytics in the cybersecurity space," says PNNL's Director of Innovation, Rosemarie Truman. "DarkLight captures the analytic tradecraft and reasoning of the cyber analyst to create automated and predictive courses of action.

This automated response combats the growing shortage of analysts in the industry while putting an emphasis on the security specialist's knowledge and encapsulating what senior analysts already know."

Achieving Success with a Tech Transfer

Successfully transferring technology to an outside vendor to commercialize new tools and services requires executive buy-in at every level.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Even with this support, it is often an arduous process and risky proposition not always resulting in a win-win.

Like with any start-up, it is critical to ensure the new company is funded and staffed appropriately to execute on its goals and deliver on the parent organization's mission and needs.

It also requires a dedicated champion from the parent organization who has a vision for the long game and benefits that can be achieved with a strong technology transfer partner.

The risks can be off-set by rewards that include revenue from commercializing products, as well as cost-effective development of a wide range of new technologies.

Contributing to the success of this transfer was the licensing arrangement that PNNL and DarkLight agreed upon.

Driven by the uniquely close relationship between the two organizations, the licensing arrangement allows PNNL and other Labs access to the current commercial version, at no charge for R&D purposes.

There isn't a divergent 'commercial' vs. R&D codebase, which is often the downfall of many unsuccessful technology transfers.

This relationship provides a structure allowing PNNL researchers the flexibility to innovate with commercial technology born at the Lab without worrying about infringing on intellectual property rights.

If the shared codebase planted the seed for DarkLight, the unwavering support of PNNL provided the nutrients that allowed commercial development of the artificial intelligence platform.

According to Prosci Inc.'s Change Management Learning Center, there is a direct correlation between active and visible executive support and the success of a major change initiative. In fact, this is the number one factor in success.

The critical elements in executive support of a program are:

- Taking the lead in establishing a budget and assigning the right resources
- Staying active with the team throughout the project
- Engaging and creating support with other senior managers
- Being a visible champion for the project
- Helping to manage key resistance points

Copyright © Cyber Defense Magazine, All rights reserved worldwide

PNNL provided the necessary support and continues to use DarkLight and host visits for other government labs and organizations to see for themselves.

The DarkLight Result

Fostering commercial development of new technologies helped produce a product unique in its approach to analytics.

The DarkLight artificial intelligence has applications in all sectors in extrapolating actionable intelligence from data produced by existing cybersecurity solutions.

Instead of focusing on a data centric methodology, DarkLight captures and automates the human logic to analyze enterprise-wide data at scale.

This gives PNNL a commercial technology to address the shortage of trained IT security analysts and improve its cybersecurity status in an environment producing huge volumes of data.

Fostering innovation need not be a struggle. With strong executive leadership, new ideas for solving new challenges can be developed and commercialized to benefit both the parent organization and the broader IT community.

About the Author

John Shearer, Co-Founder and CEO, DarkLight

John is an award-winning international technologist, inventor, and former CEO of several tech ventures who currently serves as Practitioner Faculty and Entrepreneur-in-Residence at Pepperdine University's Graziadio School of Business and Management.

John has been instrumental in substantially growing the MBA Entrepreneurship Program at Pepperdine University and has co-founded the Early X Foundation, a unique Intellectual Property commercialization process. In this teaching role, he develops MBA student-founded, innovation-based businesses.

Globally, he locates and evaluates cutting-edge technologies with significant commercial value from other universities, national and international research laboratories and within the private sector for commercialization.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CYBERTECH 2017.

THE EVENT FOR THE CYBER INDUSTRY

JAN.30–FEB.1 2017 | TEL AVIV

egister Now! ★ Register Now! ★ Register Now! ★ Register Now! ★

10% OFF
When Registering
Using Code:
Cdm88121873

Registration Is Now Open For Cybertech Tel Aviv 2017 !

SEE YOU AT CYBERTECH TEL AVIV 30.1-1.2.2017

FOR MORE DETAILS: E: cyber@israeldefense.co.il | W: www.cybertechisrael.com | T: +972-74-7031211

The Latest Business Cybersecurity Concerns for 2017

There are a variety of trending topics dominating the cybersecurity world now and into 2017, including mobile devices, the Internet of Things (IoT), and machine learning. Botnets are projected to grow in intelligence and number. In addition, detection and response will be just as important as prevention.

One factor that kept coming up in my recent research on cybersecurity is a concern over the Internet of Things (IoT)—especially because, as EDN Europe reminds us, "a specific end device may not be the actual target for an attack… But that device might be highly attractive as a gateway to the network to which it is connected…" In other words, IoT-connected devices could be seen as easy targets or ways in to gain access to other connected devices that are richer sources of data.

Part of the reason for this is that many IoT devices, such as digital video recorders, were produced with default passwords that have never changed and are identifiable via a simple internet scan, whereupon they can be compromised.

Mobile devices, also, are being seen as fertile ground for possible cyberattacks, as mobile apps are vulnerable entry-points for data breaches. Because of this, it's always wise to encrypt data using corporate security software, if available, and connect your smartphone to company networks via VPN connections. Harvard Business Review also recommends backing up information to cloud services and to store as little as possible on your device, in the event of a security breach.

One type of data-stealing attempt that's become common is a personalized attack from a criminalized network, often sent in the form of email enticing the recipient to download a file or click a link, which proceeds to deliver malware to the victim's computer or device. Another common type of theft involves an emailed threat to launch a Distributed Denial-of-Service (DDoS) attack, unless the recipient agrees to pay a certain amount of money.

So what can you do to protect your business from malicious hackers? There are a number of preventative measures you or a cybersecurity specialist can take to safeguard your company and your employees:

1. Keep all security patches and antivirus software updated, so as to make sure you are inoculated from the last malware and viruses.

2. Limit employees' access to customer data or other personally identifiable information (PII), which increases the possibility of data breaches.

3. Try to avoid printing everything out, since paper trails allow for visual hacking.

4. Learn about cyber fraud methodology and educate yourself about the process.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

5. Learn which kinds of information are most in need of protecting and most often sought after by hackers.
6. If you use a cloud storage service, ensure it has a secure encryption method.
7. Your company needs a floor-wide security policy that will protect confidential information, and make sure employees are aware of security protocols.
8. Have a concrete plan in place, in the event of a security breach to the company.
9. Make sure your system for managing records is secure—and ideally off-site.

Tripwire goes beyond strong security protocols to argue for artificial intelligence (AI) and deep machine learning being in charge of cybersecurity systems, in order to be able to keep up with the complexity of the personalized malware that is now able to be installed at the push of a button.

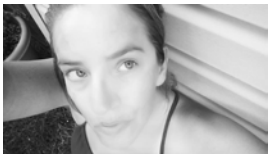
However, Alexey Malanov argues that there's nothing new about machine learning in cybersecurity, pointing out that algorithms were first implemented ten to twelve years ago. Ideally, once the majority of cybersecurity protections are being carried out by machine learning, software engineers will become freed up to focus on more advanced security concepts.

Datanami even goes so far as to argue that machine learning is our "last hope" for cybersecurity. One reason for this is the ever-widening array of connected devices, coupled with increasing amounts of security-related data.

They also argue that attacks will become fully-automated and bot-based, making them faster and even more difficult to detect than before. In addition, machine learning will have a greater ability to detect changes that inform network behavioral profiles of normal and abnormal site traffic.

As we look ahead to 2017, we can predict an industry-wide embrace of more sophisticated, automated cybersecurity programs that can go head to head with sophisticated botnets and other types of cyber-threats—both human and automated. Let's all take the recommended steps to ensure we avoid having to deal with a company-wide DDoS or other massive security breach.

About the Author



Daphne Stanford hosts "The Poetry Show!" on KRBX, her local community radio station, every Sunday at 5 p.m. A writer of poetry, nonfiction, and lyric essays, her favorite pastimes include hiking, bicycling, and good conversation with friends and family. Follow her on Twitter @TPS_on_KRBX.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

WHERE FINANCIAL CYBERSECURITY EXPERTS *CONNECT*

InfoSecurity CONNECT

March 6-8, 2017 • The Rancho Bernardo Inn, San Diego, CA

Private, One-To-One Meetings with *Very* Senior Level Cybersecurity Executives

See more info at www.infosecurityconnect.com

The Trials and Errors of Security Operations Revealed in New Report

Roberto Sandoval, Manager, WW SIOC Strategic Solutions & Enablement, HPE Security

The security industry is going through a volatile period. Threat actors are becoming bolder and evolving quickly, and security organizations are deploying new solutions and developing advanced detection and response capabilities in attempts to rapidly combat these attackers. This constant ebb and flow leads organizations into an accelerated response to protect core assets that is filled with the uncertainty of trial and error.

The departure from traditional security operations models, the adoption of new roles, processes, and emerging tools, as well as the relentless pursuit of automation are among the topics that stand out in the fourth annual State of Security Operations report released this month by Hewlett Packard Enterprise (HPE).

The report provides insights from more than 180 security operations maturity assessments within the enterprise and public sector space in 31 different countries. These in-depth assessments take 3+ days of on-site observation of a security operations center (SOC) by security experts, and include interviews with service owners, service stakeholders, and operational practitioners within each organization.

The results and the trends identified through the assessments performed across operational models and industry verticals are consolidated to produce the findings revealed in the annual report. The ideal SOC should have defined processes and goals, as well as flexibility to adapt to new technologies or changing environments and threats; however, many organizations are not meeting these criteria.

Security Operations are Aligning with Business Objectives like Never Before

For the first time in the 4-year history of the State of Security Operations Report there has been a major shift in the most mature area of security operations. The report found that the Business category outperformed the historically leading Technology category once all the data was consolidated for the previous year.

Based on this data, security organizations are more aligned to business needs and goals than ever before, and the report shows a 3% improvement year-over-year with 18% of organizations achieving their security operations goals. While the improvement is encouraging, a majority of SOCs are still not meeting business objectives.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The alignment between the SOC and the business is essential in determining the organizations' goals and metrics.

In fact, a clear mission that focuses on protecting critical assets and data, rather than just assure system up-time, was found to be a better predictor of maturity and capability than size of the organization or total security investment.

All or Nothing Approach Does Not Drive Effectiveness

While Business maturity is increasing, organizations are trying out new technologies, organizational alignments, and analytical strategies to only varying degrees of success. The proliferation of threat hunt programs is a continuing trend that is delivering extraordinary results within some organizations, and at the same time introducing a great deal of cost, complexity, and risk within others. Organizations that are adopting hunt teams as an enhancement to their existing mature real-time monitoring capabilities are seeing success.

These hunt teams are able to pinpoint unknown threats and patterns and feed valuable intelligence that can be used to enhance near real-time detection and incident response programs. However, many organizations are forgoing these real-time detection capabilities and going all-in with hunt-only programs, which is leading to a sharp decline in security operations maturity and effectiveness.

Automation is another area that is showing promise and helping to relieve some pressure on existing staff. Reducing the clicks or steps an analyst has to perform during an incident investigation can have a major impact on the longevity and burnout rates of staff. Finding opportunities for automation is key to keeping security experts engaged and focused on real threats instead of getting caught up in event noise.

However, full automation is unrealistic since most organizations struggle with a lack of knowledge and accuracy around configuration management and still need human decision making for risk assessment and advanced investigation. The level of automation most organizations envision, eliminating front line analysts in the response process, is seldom realized when organizations do not fully understand interdependencies and potential impact to critical applications, users, or data.

Finding the Perfect Mix

The decisions to utilize managed services, technology outsourcing, or hybrid operational staffing are other areas impacting a number of organizations. Many security leaders have gone through significant trial and error, risk, and expense to find the sweet spot in leveraging MSSPs, and there has been much debate in the industry as to whether keeping resources in-house or

Copyright © Cyber Defense Magazine, All rights reserved worldwide

outsourcing provides better results. However, the State of Security Operations Report finds that a mix of both has actually been the most effective.

This hybrid model of staffing is an effective strategy to combat the continued struggle to find and retain security staff, which was found to once again be the number one concern of security operations. Organizations can leverage a Managed Security Services Provider (MSSP) to help scale their operations, while keeping their risk management in-house ensuring increased capabilities from outsourcing and maintaining proper documentation and transfer of knowledge.

Technology management, eyes-on-screen monitoring, and shared-insourced operations are areas where organizations and service providers can work closely together to increase the effectiveness of security solutions.

Building the Intelligence-driven SOC for Today and the Future

While 82 percent of organizations' SOCs are still struggling to meet target maturity levels, the security programs that incorporate the right people, processes and technologies are succeeding in building sustainable defenses.

The State of Security Operations Report highlights that there is no single magic bullet for solving the security challenge, as is evident by the decrease in maturity from hunt-only programs and too much automation.

As adversaries evolve and attacks grow in sophistication, organizations must also continue to invest in their security operations and adapt to the changing environment to protect the business' most critical assets.

Read the full report at hpe.com/software/StateOfSecOps.

About The Author

Roberto Sandoval is Manager, WW SIOC Strategic Solutions & Enablement, HPE Security at Hewlett Packard Enterprise.Roberto leads a team that coordinates strategic activities and initiatives in the design, development, operation, and maturation of world class security intelligence, operations, and cyber defense for HPE's global customers around HPE Security & Information Governance Software solutions.

Over the last 5+ years with HPE, Roberto has driven the design, delivery, and quality of over a dozen Security Operations Centers through security use cases, operational workflow, metrics, and continuous improvement in intelligence, analysis, and operations.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

.comex

Exhibition & Conference

28 March - 1 April, 2017

Oman Convention & Exhibition Centre
Muscat - Sultanate of Oman

Under the Patronage

e.oman

www.comex.om

NO. OF EXHIBITORS **100**

PARTICIPATING COUNTRIES **10**

VISITORS ATTENDED **90,000**

For more information please contact:

Ashit Barnes, Exhibition Director
+968 9934 1687
barnes@oite.com

Ahmed Farag, Sales Manager
+968 9411 3434
a.farag@oite.com

BOOK YOUR STAND NOW!

Media Partners

CDM Cyber Defense Magazine · thebusinessyear · Telecom Review (telecomreview.com) · Teknotel Technology & Business · Telecom Era · Dossier · Cyber Security Review (Unique content / Global reach / In print and online) · Enterprise IT World · SME Channels · Eye Of Riyadh · Eye Of Dubai · SME World (India's Best Known Knowledge & Information Magazine) · Easyfinder Oman's Local Business Search Engine

Organiser

OITE TRADE FAIRS

How We Delivered a Security-First Approach with Twilio's Authy Two-Factor Authentication Service

Step-by-Step Seamless Integration of 2FA and OneTouch Authentication into an Enterprise CMS Platform

By Andy Fleming, CTO, Zesty.io

As digital content managers, developers and designers, my colleagues and I at Zesty.io desperately needed a cloud-based platform that could take the pain points out of content management and website development.

When we couldn't find a solution that delivered agility, flexibility and speed, we built our own solution. And in 2010, Zesty.io was launched to deliver a SaaS solution for enterprise content management and development.

As the company grew to include co-marketing partners and large brand marketers like Sony, Zesty.io's platform evolved with expanded capabilities focused on delivering a true content-first approach.

Our cloud solution ensured the reliability, rapid deployment, scalability and flexibility needed to deliver exceptional digital experiences for our clients and end users. When Zesty.io needed extra layers of security built into our cloud platform, we turned to Twilio's Authy 2FA service.

Mitigating Security Issues in a Complex Digital Landscape

In a highly security-conscious industry, the Zesty.io platform was built to help mitigate security issues and challenges. Website and interface management security are complicated. For example, WordPress serves the admin area in the same place as the actual site. We think that's a security risk for our clients, so we separate and decouple those types of features.

The Zesty.io platform is also primarily closed source so that people can't crawl through their source code seeking out vulnerabilities. The security of our client sites, and how end users consume them, is critically important to us. We need to guarantee that sites won't go down or be defaced or otherwise compromised.

Keeping security top of mind, we also looked to integrate seamless authentication technology into the platform and interface. With large brand and agency clients, a security-focused approach is an imperative.

In fact, Zesty.io went through a stringent review process with Sony in which authentication was a requirement before we could land the business.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Authy 2FA for Security and Recovery

We've always valued security and wanted to be proactive. We were using a two-factor provider early on, but the vendor actually went out of business. Zesty.io evaluated two other options before deciding on Authy 2FA.

We could integrate Google Authenticator or build our own authentication technology on top of Twilio SMS. In the end, we realized it would be an easier implementation with Authy. Having it pre-built and well-tested would save us a lot of time.

The other significant benefit for Zesty.io is Authy's managed recovery process. It's secure and validated; we won't have to deal with it — we know Authy's team will keep the system secure.

Zesty.io uses both Authy 2FA and OneTouch authentication. Both implementations were quick. We spent a couple of days on the first initial 2FA implementation and, about a year later, integrated OneTouch implementation to upgrade the login experience. We were familiar with Authy before we rolled it out — but I wish we would have known how easy it ended up being.

With Authy's authentication built into our platform, Zesty.io is able to drive home the critical importance of security for our clients. We go beyond just providing authentication; we provide tools to enforce 2FA. For anyone who wants to access the site, even if they're granted access, they can't until they've enabled and set up two-factor

What's Next?

Right now, our big initiative is continued growth. The true platform nature of Zesty is sinking in, getting Zesty.io's customers to understand why we are a better option than the other solutions out there. Our company has really started to take off; we're building awareness, and people are seeing that we're a secure, powerful platform. By choosing a modern technology experience like Authy, we're communicating our security philosophy. We're able to show our clients that Zesty.io is completely secure and innovative with the tools we're using.

About the Author

Andy Fleming is founder and CTO of Zesty.io, a web content management company. An expert in user and developer experience (UX/DX) and cloud architecture, Andy turns product ideas into functional cloud applications and systems. To connect with Andy, please visit https://www.zesty.io, Facebook/GoZesty, LinkedIn/Zesty-io, @andyfleming and @Zestyio.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Asia's leading and award winning IoT event returns in March 2017

As the first dedicated platform in Asia to address the enormous potential of the IoT revolution, the first edition of IoT Asia in 2014 was ahead of its competition. It was seen as a transformational platform for addressing challenges and identifying real opportunities within the IoT landscape.

IoT Asia 2016 surpassed expectations and broke records. The event was a resounding success with 3,795 attendees, a significant increase of 75 percent from 2015! This is a testimony of the strong support the event has received from the industry. IoT Asia has won the prestigious UFI Marketing Award in 2016.

Conferred by UFI, the Global Association of the Exhibition Industry, the Award recognises excellence in the branding of new trade shows. The UFI Marketing Award adds on to a growing list of industry accolades that IoT Asia has received since its debut in 2014. They are "People's Choice Silver Award for Event of the Year in Postscapes 2015/2016 IoT Awards" and "Trade Conference Organiser of the Year" for IoT Asia 2014 at Singapore Experience Awards 2015.

IoT Asia 2017 continues to provide insights for 4,500 attendees across the entire IoT value chain, addressing the interests of technology solution providers and enablers as well as end-user and potential IoT technology adopters across multiple industries.

The show will take place on 29 and 30 March 2017 at the Singapore Expo.

As a key player in Asia's IoT community, IoT Asia 2017 will focus on

- Smart Cities
- IoT Data Analytics
- Design Applications
- Wearables
- Enablers
- Industrial IoT
- Cybersecurity (NEW)
- Robotics (NEW)

What to expect at IoT Asia 2017?

- 5,000 square metres exhibition
- 4,500 attendees
- 110 sponsors and exhibitors
- Brand new conference programme featuring three new tracks, engaging panel discussions and country-focus sessions

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Exhibition Highlights
Two new thematic zones will be introduced at IoT Asia 2017 – Cybersecurity and Robotics. This is where technology companies leading innovation in cybersecurity and robotics will be showcased.

Visitors to IoT Asia 2017 can look forward to meet exhibitors from two key feature zones – Institution Zone and Start-Up Exchange. Launched at IoT Asia 2016, the Institution Zone is back by popular demand! Visitors get to engage with professionals or students in Academia who will showcase their IoT-related solutions and projects.

The Start-Up Exchange is a dedicated area for aspiring start-ups to showcase new lab-to-market IoT solutions and technologies. The Start- Up Exchange will feature start-ups from all over Asia disrupting the IoT market.

Conference Highlights
Underlining the 2017 theme *Making $ense in Our Connected World*, the conference will focus on IoT's value generation potential and opportunities from the perspective of:

Technologies
View highlights of new and innovative IoT and related technologies, systems, enablers.

Solutions
Hear illustrative case studies and contextual use cases of how IoT is showing returns and results in various industry segments and aspects of life.

Organisations
Learn how organisations are approaching change and business disruptions as IoT takes hold, how IoT changes the face of competition and partnerships, and implications for eco-system building and development.

With the event anchored in Singapore, IoT Asia continues to chart the future for IoT in Asia by accurately anticipating the needs and concerns of the rapidly evolving industry.

Cyber Defense Magazine readers enjoy extra 10% All-Access and Single Track conference rates (except Academic). Use code IOT17MED10.

For more information, visit www.internetofthingsasia.com.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

NSA Spying Concerns? Learn Counterveillance

Free Online Course Replay at www.snoopwall.com/free

"NSA Spying Concerns? Learn Counterveillance" is a 60-minute recorded online instructor-led course for beginners who will learn how easily we are all being spied upon - not just by the NSA but by cyber criminals, malicious insiders and even online predators who watch our children; then you will learn the basics in the art of Counterveillance and how you can use new tools and techniques to defend against this next generation threat of data theft and data leakage.

The course has been developed for IT and IT security professionals including Network Administrators, Data Security Analysts, System and Network Security Administrators, Network Security Engineers and Security Professionals.

After you take the class, you'll have newfound knowledge and understanding of:

1. How you are being Spied upon.
2. Why Counterveillance is so important.
3. What You can do to protect private information.

Course Overview:

How long has the NSA been spying on you?
What tools and techniques have they been using?
Who else has been spying on you?
What tools and techniques they have been using?
What is Counterveillance?
Why is Counterveillance the most important missing piece of your security posture?
How hard is Counterveillance?
What are the best tools and techniques for Counterveillance?

Your Enrollment includes :

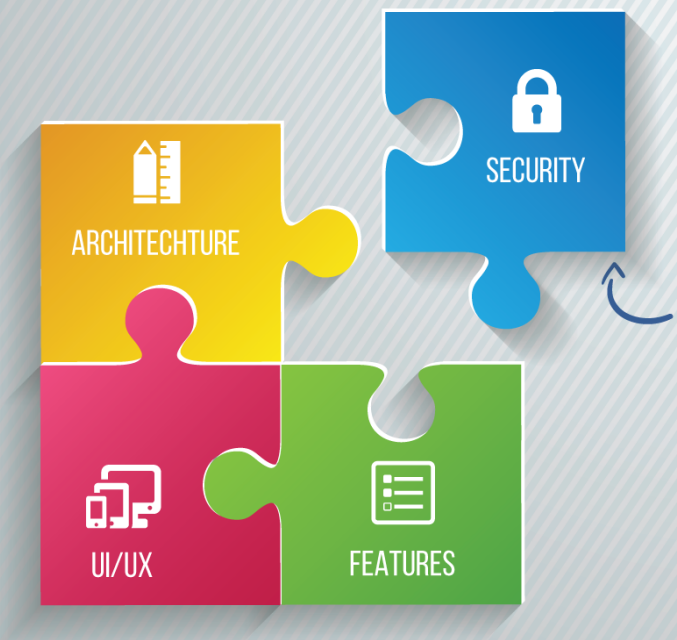
1. A certificate for one free personal usage copy of the Preview Release of SnoopWall for Android
2. A worksheet listing the best open and commercial tools for Counterveillance
3. Email access to the industry leading Counterveillance expert, Gary S. Miliefsky, our educator.
4. A certificate of achievement for passing the Concise-Courses Counterveillance 101 course.

Visit this course online, sponsored by Concise-Courses.com and SnoopWall.com at http://www.snoopwall.com/free

Copyright © Cyber Defense Magazine, All rights reserved worldwide

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY



You have built a great app with an amazing team.

Let us help you secure it.

SnoopWall's patents-pending AppShield™ SDK can secure any mobile app on all major platforms. Our AppShield SDK makes your app invisible to any other app on the mobile device which might otherwise eavesdrop on it, just like the B2 Bomber employs stealth technology to evade radar detection. With 24/7/365 active monitoring, regular updates and a dedicated team of cybersecurity experts, you can be assured that your app's security and customer data are safe, all the while providing a non-intrustive customer experience.

KEY FEATURES

- Cloaking Technology (patents-pending)
- Dynamic Port Management (patents-pending)
- No Need for Code Obfuscation
- No Malware Scanning Required
- No Backend Database Required
- Root & Jailbreak Detection
- Secure Storage for Data Hiding
- Application Hardening Technology
- No Known Way to Exploit
- Detects & Blocks Tomorrow's Threats
- Apple iOS, Google Android, Microsoft Windows
- No Sysadmin, no Reboot, no special Privileges
- Tiny Deployment Size & Rapid Integration
- Most Cost Effective Per Deployment Pricing

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

AppCrusher is patents-pending, trademark and copyright © 2015, SnoopWall, Inc. All rights reserved worldwide. Other trademarks are properties of their respective owners.

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

Does your mobile app have built-in next generation firewall technology to safeguard customer data?

Mobile apps are critical and vulnerable touchpoints in most companies networks. Just like the firewall which protects your IT network, an app firewall is needed to protect your mobile app. However, most app development teams do not have this expertise, nor are they dedicated to this mission.

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

- HIGH RISK OF PATENT INFRINGEMENT $$$$$
- MAJOR DISTRACTION FROM CORE DEVELOPMENT FOCUS
- HIGH REPUTATIONAL RISKS
- POSSIBLY NOT SECURE
- UPDATED WHEN YOU CAN FIND THE TIME
- FULL BLOWN SOLUTION WILL TAKE YOU 20,000 CODER HOURS (10 CODERS FOR 12 MONTHS)
- LIGHTWEIGHT RISKY SOLUTION WILL TAKE YOU 10,000 CODER HOURS (10 CODERS FOR 6 MONTHS)
- MAINTENANCE AND SUPPORT WILL TAKE YOU 5200 HOURS PER YEAR (2 CODERS FOR 12 MONTHS)
- HIGH RISK TO BREAK YOUR AWESOME APP AND USER EXPERIENCE
- HIGH RISK TO CAUSE USER CONFUSION AND LOSS OF CUSTOMERS
- MAY LOSE SOME OR ALL CUSTOMER RECORDS
- MAYBE SSL PINNING IS THE MOST YOU CAN DELIVER
- MAY PROTECT SOME OF THE PORTS SOME OF THE TIME
- TIME TO DEVELOP AND DEPLOY: 6-12 MONTHS
- **COST TO DO IT YOURSELF: $1.2M**
- **ANNUAL COSTS TO KEEP IT UP TO DATE: $650k**
- **COSTS TO AVOID PATENT INFRINGEMENT: $500k-1.5M**

VS.

LICENSE OUR AppSHIELD SDK

- ✓ PROTECTED ACCESS TO PATENTED AND PATENT PENDING SOLUTIONS
- ✓ LEVERAGE YEARS OF MOBILE SECURITY EXPERTISE
- ✓ LOW REPUTATIONAL RISKS
- ✓ EXTREMELY SECURE AND PROVEN SOLUTION
- ✓ 7x24x365 CYBERSECURITY PROTECTION
- ✓ THE SOLUTION IS DONE
- ✓ THE SOLUTION HAS BEEN PROTECTING MILLIONS OF TRANSACTIONS SINCE 2014
- ✓ MAINTENANCE AND SUPPORT IS INCLUDED
- ✓ INCLUDED IN THIS SYSTEM:
  - → ZERO DAY MALWARE PROTECTION
  - → ADVANCED PERSISTENT THREAT PROTECTION
  - → FEATURES INVISIBLE TO CONSUMER EXPERIENCE
  - → ALL MOBILE APP CUSTOMER PII PROTECTED
  - → MILITARY GRADE ENCRYPTION
  - → REAL-TIME DATA LEAKAGE PROTECTION
- ✓ **TIME TO INTEGRATE AND DEPLOY: 3-5 BUSINESS DAYS**
- ✓ **NO INFRINGEMENT RISKS ONCE LICENSED: FIRST OF ITS KIND IP**
- ✓ **ANNUAL UPDATE COSTS A FRACTION OF DO IT YOURSELF**
- ✓ **PRICING IS A NO-BRAINER (MUCH MUCH LOWER)**

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

AppCrusher is patents-pending, trademark and copyright © 2015, SnoopWall, Inc. All rights reserved worldwide. Other trademarks are properties of their respective owners.

Top Twenty INFOSEC Open Sources

Our Editor Picks His Favorite Open Sources You Can Put to Work Today

There are so many projects at sourceforge it's hard to keep up with them. However, that's not where we are going to find our growing list of the top twenty infosec open sources. Some of them have been around for a long time and continue to evolve, others are fairly new. These are the Editor favorites that you can use at work and some at home to increase your security posture, reduce your risk and harden your systems. While there are many great free tools out there, these are open sources which means they comply with a GPL license of some sort that you should read and feel comfortable with before deploying. For example, typically, if you improve the code in any of these open sources, you are required to share your tweaks with the entire community – nothing proprietary here.

Here they are:

1. TrueCrypt.org – The Best Open Encryption Suite Available (Version 6 & earlier)
2. OpenSSL.org – The Industry Standard for Web Encryption
3. OpenVAS.org – The Most Advance Open Source Vulnerability Scanner
4. NMAP.org – The World's Most Powerful Network Fingerprint Engine
5. WireShark.org – The World's Foremost Network Protocol Analyser
6. Metasploit.org – The Best Suite for Penetration Testing and Exploitation
7. OpenCA.org – The Leading Open Source Certificate and PKI Management -
8. Stunnel.org – The First Open Source SSL VPN Tunneling Project
9. NetFilter.org – The First Open Source Firewall Based Upon IPTables
10. ClamAV – The Industry Standard Open Source Antivirus Scanner
11. PFSense.org – The Very Powerful Open Source Firewall and Router
12. OSSIM – Open Source Security Information Event Management (SIEM)
13. OpenSwan.org – The Open Source IPSEC VPN for Linux
14. DansGuardian.org – The Award Winning Open Source Content Filter
15. OSSTMM.org – Open Source Security Test Methodology
16. CVE.MITRE.org – The World's Most Open Vulnerability Definitions
17. OVAL.MITRE.org – The World's Standard for Host-based Vulnerabilities
18. WiKiD Community Edition – The Best Open Two Factor Authentication
19. Suricata – Next Generation Open Source IDS/IPS Technology
20. CryptoCat – The Open Source Encrypted Instant Messaging Platform

Please do enjoy and share your comments with us – if you know of others you think should make our list of the Top Twenty Open Sources for Information Security, do let us know at marketing@cyberdefensemagazine.com.

(Source: CDM)

Copyright © Cyber Defense Magazine, All rights reserved worldwide

National Information Security Group Offers FREE Techtips

Have a tough INFOSEC Question – Ask for an answer and 'YE Shall Receive

Here's a wonderful non-profit organization. You can join for free, start your own local chapter and so much more.

The best service of NAISG are their free Techtips. It works like this, you join the Techtips mailing list.

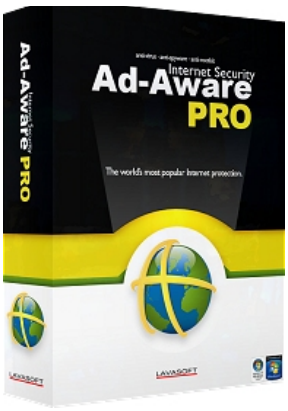
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting your question to the Techtips newsgroup.

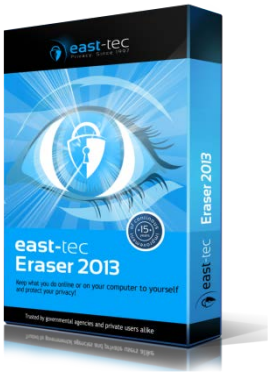
Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

http://www.naisg.org/techtips.asp

SOURCES: CDM and NAISG.ORG

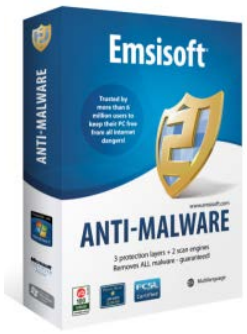




SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com

where they (like you) will be entered into a monthly drawing for the Award winning Lavasoft Ad-Aware Pro, Emsisoft Anti-malware and our new favorite system 'cleaner' from East-Tec called Eraser 2013.



Copyright © Cyber Defense Magazine, All rights reserved worldwide

Job Opportunities

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Warnings e-Magazines will also keep you up to speed on what's happening in the cyber crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy.

You get all of this for FREE, always, for our electronic editions.

Click here to signup today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine January 2017

Sample Sponsors:

RSA CONFERENCE

StillSecure

PORTCULLIS

Hawk Mobile Monitor — Monitor Mobile Devices Remotely From Your Computer

AFORE — SECURE THE CLOUD. TRUST THE CLOUD.

NETCLARITY — PREEMPTIVE, PROACTIVE PROTECTION

CENTER FOR INTERNET SECURITY

Software Developer's JOURNAL — new ideas & solutions for professional programmers

SWIVEL — the power of knowing

SnoopWall — RECLAIM YOUR PRIVACY™

KASPERSKY lab

dekart — MAKE IT SECURE

INFOSEC WORLD

PWNIE EXPRESS

EncrypTight™ — BLACK BOX WAN Encryption

GO ANYWHERE™

BLUESPACE

CYBER SECURITY SUMMIT 2014 — June 5 DC Metro — Sept. 18 New York City

CYBER INTELLIGENCE USA — 18-20 JUNE 2014 - ARLINGTON/V.A

NETWORK MONITORING REDEFINED — See How RSA Security Analytics Detected Heartbleed — Watch video » — RSA EMC²

INDUSTRIAL CONTROL CYBER SECURITY — OCT 6 / 7 USA

INDUSTRIAL CONTROL CYBER SECURITY — SEPT 29/30 UK

2nd Annual Privacy, Policy & Technology Summit — January 26-27, 2015 New York

INFOSEC WORLD — Conference & Expo — March 23-25, 2015 | Orlando, FL

January 21–22, 2015 • Calgary, AB — Cyber Security for Energy

CYBERTECH 2015 — THE EVENT FOR THE CYBER INDUSTRY

The UK Energy Cyber Security Executive Forum — London, 5th February — 20% discount (CYSENCDM)

CYBER SECURITY FOR FINANCIAL SERVICES — June 14 - 16, 2015 • Charlotte, NC

THE CYBER SECURITY SHOW — 13-14 April 2015 — etc venues 155 Bishopsgate, London

To learn more about us, visit us online at http://www.cyberdefensemagazine.com/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CDM
Secure Your IT World

CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only $199

Five Year Commitment starting at only $499

http://www.cyberdefensemagazine.com/infosec-innovators-marketplace

Now Includes:

Your Graphic or Logo

Page-over Popup with More Information

Hyperlink to your website

BEST HIGH TRAFFIC OPPORTUNITY FOR INFOSEC INNOVATORS

Email: marketing@cyberdefensemagazine.com for more information.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Cyber Warnings Newsflash for January 2017

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

Here is a summary of this month's cyber security news. Get ready to read on and click the links below the titles to read the full stories. So find those of interest to you and read on through your favorite web browser…

HummingBad malware returns to Google Play in new avatar dubbed HummingWhale

http://www.ibtimes.co.uk/hummingbad-malware-returns-google-play-new-avatar-dubbed-hummingwhale-1602726

Billion-dollar Hacker Gang Abuses Google Services To Control Malware

http://www.forbes.com/sites/leemathews/2017/01/18/notorious-carbanak-gang-abuses-google-services-to-control-malware/#186b77ef4e93

Hacking group uses Google services to control malware

http://betanews.com/2017/01/20/carbanak-google-services-cc-malware/

Google reveals how it flagged 25,000 Android apps for malware

http://thenextweb.com/google/2017/01/18/google-reveals-how-it-flagged-25000-android-apps-for-malware/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Malware Starts Pinpointing Financial Services Targets

http://www.cutimes.com/2017/01/17/malware-starts-pinpointing-financial-services-targ

What The Tech? Satan Malware

http://www.wrcbtv.com/story/34337058/what-the-tech-satan-malware

How are hackers using Twitter as C&C servers for malware?

http://searchsecurity.techtarget.com/answer/How-are-hackers-using-Twitter-as-CC-servers-for-malware

This Vicious New Malware Freezes Apple Computers

http://fortune.com/2017/01/06/this-vicious-new-malware-freezes-apple-computers/

Vermont utility finds alleged Russian malware on computer

http://www.cnn.com/2016/12/30/us/grizzly-steppe-malware-burlington-electric/

Hackers have a new way to steal your banking login using WhatsApp

http://bgr.com/2017/01/02/android-malware-whatsapp-threat/

Facebook users hit with “You are in this video?” malware scam

https://www.hackread.com/you-are-in-this-video-facebook-malware-scam/

Malware suspected on some Arizona legislators' computers

http://www.azfamily.com/story/34221617/malware-suspected-on-some-arizona-legislators-computers

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Scam Report: Espionage malware being utilized for ransomware hits; bitcoins sought

http://www.readingeagle.com/business-weekly/article/scam-report-espionage-malware-being-utilizedfor-ransomware-hits-bitcoins-sought

Study: Your Smartphone Can Be Hacked By Hidden Voice Commands

http://www.newsmax.com/Newsfront/smartphone-hack-voice-commands-Siri/2017/01/24/id/770264/

Locky malware attacks to return with a vengeance experts warn

http://www.ibtimes.co.uk/locky-malware-attacks-return-vengeance-experts-warn-1601551

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Copyright (C) 2016, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. 848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com Cyber Warnings Published by Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC.Cyber Defense Magazine, CDM, Cyber Warnings, Cyber Defense Test Labs and CDTL are Registered Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2016, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

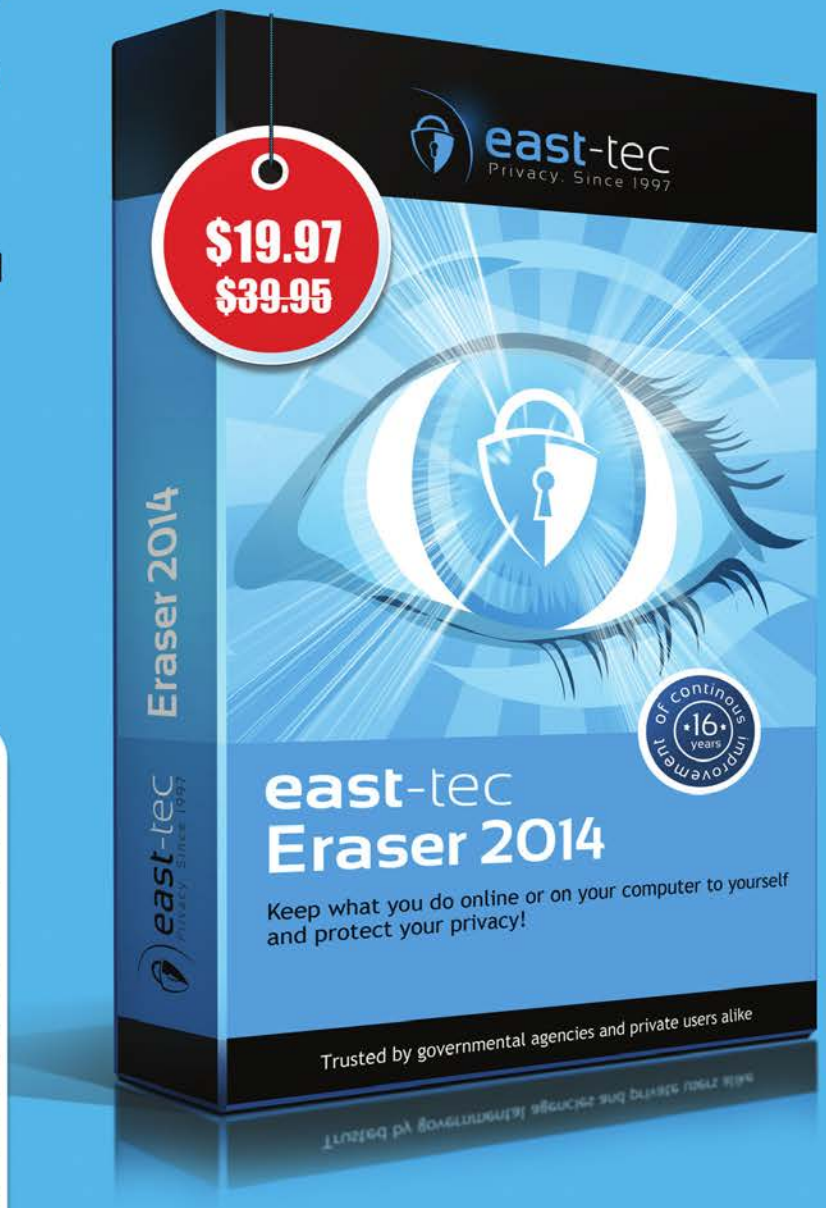
Cyber Defense Magazine - Cyber Warnings rev. date: 01/25/2017

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

Protect your data and privacy by removing all evidence of your online and offline activity with **East**-Tec **Eraser 2014**.
Securely erase your Internet and computer activities and traces, improve your PC performance, keep it clean and secure!



Exclusive offer for Cyber Defense magazine readers

Save 50%

on ALL East-Tec products
www.east-tec.com

Coupon Code:

CYBERMAG2014

private evidence protection traces from 250 + apps history
pages online privacy secure search pictures
cookies
security emails