CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

CDM TOP 20 CYBERSECURITY CDM LEADERS 2016

Winners listed inside!

IN THIS EDITION:

- IoT Security
- Machine Learning & Cyber Defense
- Big Data Security

October 2016

MORE INSIDE!

CONTENTS

Cybercriminals Never Surprise Me: New Attack Vectors 3

5 mistakes hindering effectiveness of SIEM solutions: Learning from real-life cases 8

Cloud Computing Security Issues: What Can Be Done? 12

OPEN ACCESS APIs 17

Not Listening to Your CIO Can Cost You Millions 21

Privacy and Security Issues in Autonomous Cars 25

Understanding Bluetooth and its role in the Internet of Things 31

Lock, stock and two smoking … access controls 35

Comparing the Options: An MBA or a Master of Science in Cyber Security 38

Cybersecurity: Why Your Cell Phone is Your Weakest Link 42

Developing an immunity to cyber-crime 45

Database Honeypots: Sweet and Simple Breach Detection 49

Top 10 Best Practices for Cyberbreach Post-Crisis Communication 52

Companies in Middle East Using DNS for Data Transport will become Cybercrime Targets 55

The Evolving Role of Today's CFO to Chief Protection Officer 59

How Can You Tell If Your WordPress Site Has Been Hacked? 63

Layered Security 66

The packet analysis as a helpful way of network monitoring 69

Adding Efficiency to Security 72

IMPROVING QUALITY AND SECURITY WITH BINARY ANALYSIS 74

Privacy Babel: Making Sense of Global Privacy Regulations 77

No One Likes Passwords, So Why Are We Still Using Them? 80

Top 10 Data Security Issues in Large Enterprises 83

Three Key Business Lessons From The Founder of a Big Data Security Company 87

NSA Spying Concerns? Learn Counterveillance 91

Top Twenty INFOSEC Open Sources 94

National Information Security Group Offers FREE Techtips 95

Job Opportunities 96

Free Monthly Cyber Warnings Via Email 96

Cyber Warnings Newsflash for October 2016 99

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

Serguei Tchesnokov
Dr. Daniel Osafo
David Midgley
Jean Turgeon
David Navetta
Boris Segalis
Kris Kleiner
Dimitri Vlachos
Milica D. Djekic
Megan Ray Nichols
Dave Palmer
Dave Rosenberg
Rishi Bhargava
Rod Rasmussen
Drew Del Matto
Graeme Caldwell
David Share
Dave Thompson
Bill Graham
Dimitri Sirota
Charles Durkin
Alex Hooper
MacLane Wilkison

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

Executive Producer:
Gary S. Miliefsky, CISSP®

Cybercriminals Never Surprise Me: New Attack Vectors

Friends,

Imagine you receive this email (see below) while you are being bombarded with 700mb to 1Gb of DDoS attack? Ransomware was supposed to be an 'inside' job where a trusted employee clicks a link, gets infected (accidentally) and then you need to pay the cybercriminal their fees to provide the unlock code. Cryptolocker became the norm, then Locky took it up a notch by searching for Structured Message Block (SMB) file shares, worming its way across your organization so that the ransom requested could be even more – remember Locky has crippled hospitals who had to pay as much as $200,000 USD just to get the unlock key:

"If you will not pay in time, DDoS attack will start, your web-services will go down permanently. After that, price to stop will be increased to 5 BTC [bitcoin] with further increment of 5 BTC for every day of attack. NOTE, i?m not joking.

My attack are extremely powerful now – now average 700-800Gbps, sometimes over 1 Tbps per second. It will pass any remote protections; no current protection systems can help."

At first, no one was sure if this was the group or person that hit Dyn, which provides DNS services to major providers like Spotify and Twitter. In any case, during National Cyber Security Awareness month, this DDoS attack of this magnitude, affecting all of the US East Coast internet shows how simply weak our networks are to the latest onslaught of cyber attackers.

This month, we have decided to publish the most articles we possibly can on the subject matters of breach prevention, handling the post-crisis situation when you have been breached, developing an immunity to cyber-crime, how to better use your SIEM and so much more.

In addition, this month we're very exciting to name the top twenty Cyber Security Leaders of 2016 for their innovations in the field of information security with the full list to follow in this edition of Cyber Warnings and on our website, here: http://www.cyberdefensemagazine.com/cyber-security-leaders-2016/

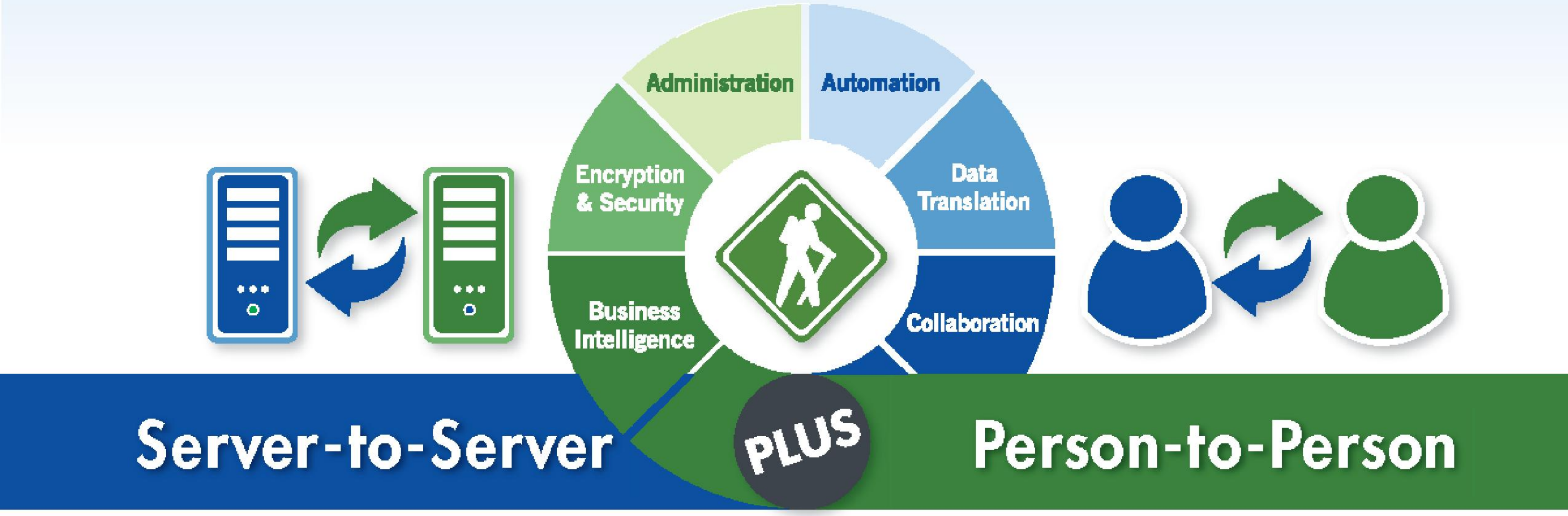
Please join us in congratulating these innovators who are helping us all stay one step ahead of the next threat. Fall and winter are coming so stay tuned as we gear up for RSA Conference 2017 and our annual print edition – right around the corner. Cheers!

To our faithful readers, Enjoy

Pierluigi Paganini

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

Secure File Transfer



VENDOR LANDSCAPE AWARD
BEST OVERALL VALUE
INFO~TECH RESEARCH GROUP

VENDOR LANDSCAPE AWARD
LEADER
INFO~TECH RESEARCH GROUP

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

CDM

CYBERSECURITY CDM LEADERS 2016 | TOP 20

clearswift	**Clearswift**	clearswift.com
wirex	**WireX Systems**	wirexsystems.com
RiskVision	**RiskVision**	riskvisioninc.com
LINOMA SOFTWARE REVOLUTIONARY SOLUTIONS FOR YOUR WORLD	**Linoma**	linomasoftware.com
Karamba Security	**Karamba Security**	karambasecurity.com
AMGINE SECURUS	**Amgine Securus Inc.**	amgine.co.kr
COVERTIX All your files secured. Anywhere.	**Covertix**	covertix.com

CDM

CYBERSECURITY CDM LEADERS 2016 TOP 20

Towerwall Protecting Data Integrity	Towerwall	towerwall.com
Cynet PRECISE THREAT DETECTION	Cynet	cynet.com
CATO NETWORKS	Cato Networks	catonetworks.com
Code Dx	Code Dx	codedx.com
inspired eLearning education for your enterprise	Inspired eLearning	inspiredelearning.com
NNT™ WORKPLACE SOLUTIONS	New Net Technologies	newnettechnologies.com
GuardiCore	GuardiCore	guardicore.com

CDM

CYBERSECURITY CDM LEADERS 2016 | TOP 20

MeasuredRisk	MeasuredRisk	measuredrisk.com
VERINT®	Verint	verint.com
AVG®	AVG Technologies	avg.com
VOTIRO SECURED.	Votiro	votiro.com
exabeam	Exabeam	exabeam.com

Congratulations to all our winners!

5 mistakes hindering effectiveness of SIEM solutions: Learning from real-life cases

5 MISTAKES HINDERING EFFECTIVENESS OF SIEM SOLUTIONS: LEARNING FROM REAL-LIFE CASES

With a SIEM solution installed, the security department can think it's time to grab some popcorn and watch the system perfectly dealing with all possible threats impending their networks. Ah, if only it all would be so easy.

According to the survey conducted by 451 Research, only 31.9% of respondents get more than 80% of the value they expected from their SIEM system, while another 42.8% claim to benefit from only 16-60% of their SIEM system's capabilities. It means that the majority of implemented SIEM solutions don't prove even a half of their real potential, thus letting intruders stay unseen within corporate networks. But why?

Are SIEM systems to blame?

SIEM software is always the first to blame when a company fails to improve their information security environment. When the system is prone to performance issues or overlooks security events, it's easy to conclude that this solution doesn't meet a company's requirements and thus cannot handle its mission. However, in the real life, issues often result from human negligence towards vital details ensuring a SIEM solution's viability.

Here are 5 common mistakes companies make while planning, deploying and customizing a SIEM solution, supported with real-life cases from our SIEM consulting practice proving that merely installing SIEM software isn't enough to ensure full-fledged threat management.

Mistake 1: Leaving non-customized correlation rules

One of the solution's main functions is to correlate security events and detect offenses that threaten a corporate network. Though modern SIEM systems offer out-of-the-box correlation rules (e.g. in IBM QRadar, over 500 correlation rules are available), they usually cover only the most typical use cases. Customized correlation rules are indispensable to make the system work according to a company's network topology and security policy.

Case 1: A financial organization implemented a SIEM solution as a part of their security strategy and activated a range of out-of-the box correlation rules. However, there wasn't a single custom correlation rule adapted to the company's domain controller security policy. It meant that the implemented system didn't qualify cases of multiple user login failures into offenses, failing to detect any attempts of brute forcing across the network. SIEM consultants built up a relevant correlation rule aligned with the existing domain controller policy, which allowed to see the first results 24 hours later when the SIEM system generated 30+ offenses triggered with authentication mistakes. Having investigated the detected offenses and their source IPs, security administrators found out that one of them belonged to a malicious external user persistently trying random passwords to access one of the employees' workstations.

Case 2: A SIEM system installed at a bank had no customized correlation rules on the traffic baseline analysis, therefore it couldn't detect abnormal network activities and prohibited communication with important network devices. To fill this gap, the bank turned to SIEM consultants who fine-tuned a set of flow rules, including a custom correlation rule applied to the database production server. With new rules in place, just 3 weeks later a SIEM system identified an abnormal increase in the server traffic by more than 25%, as well as detected a suspicious IP that wasn't authorized to communicate with the server. Security administrators were then able to start investigating the offense.

Mistake 2: Allowing false-positives to flood out the system

With non-customized correlation rules, organizations are not only unable to capture a whole array of security events, they also risk to overlook real incidents in the mounting pile of false-positives. This creates unnecessary workload for security administrators and analysts along with making investigation of security offences cumbersome.

Case 1: A healthcare organization turned to SIEM consultants to fine-tune their SIEM solution. They discovered that the SIEM solution functioned with out-of-the-box rules activated all at once without any customization. As a result, the system generated 7,000+ offenses daily. It's obvious that such a volume of security incidents was impossible to analyze manually. By updating the network hierarchy and forming log source groups, the SIEM team fine-tuned the out-of-the box correlation rules, as well as developed custom rules aligned with the company's infrastructure. This allowed to cut down the number of false-positives along with reducing the number of daily generated offenses to only 150.

Mistake 3: Overloading a SIEM solution

The estimated system load (the number of events per second (EPS) and flows per interval (FPI)) is one of the most important factors to consider while designing a SIEM solution architecture. If the solution's actual load mismatches the real number of security events, a huge amount of data will just pass by without being sieved through a SIEM system, putting the organization's security at stake.

Case 1: An oil company deployed a SIEM solution with the total load of 4,000 EPS. However, once SIEM consultants came on-site to fine-tune the system, it turned out that the real number of log sources exceeded the default license, generating 8,000+ EPS all together. Without fixing, the system would ignore more than a half of security events. To ensure the correct functioning of the solution, the company had to purchase additional licenses extending the load threshold. Furthermore, the SIEM consultants filtered thoroughly both events and flows coming from all the log sources to improve the system's general performance.

Mistake 4: Overlooking deployment gaps

Even a well-designed architecture cannot guarantee a SIEM system will be properly deployed. Though the deployment process isn't rocket science, security administrators should check that the system components and licenses are activated appropriately to ensure the solution functions correctly.

Case 1: A bank deployed a SIEM module to monitor network device configurations but it didn't operate for an unknown reason. Analyzing the solution, a SIEM consultant discovered that a security administrator activated the license incorrectly, which disabled the entire module. To fix the issue, a SIEM consultant had to redeploy the module in a virtual environment, reactivate the license, then to reconfigure it according to the bank's requirements.

Mistake 5: Neglecting system configuration requirements

SIEM solution configuration is another important aspect to consider during the implementation phase. Misconfigured SIEM systems cause performance issues that impede security event processing and analysis. There can be the following misconfigurations:

No auto-updates

When auto-updates are misconfigured or disabled, a SIEM solution doesn't receive updated lists of vulnerabilities and bad IPs, while protocols and modules are not renewed. In essence, such a system doesn't identify a whole range of recently introduced offense types.

Case 1: A SIEM system didn't scan vulnerabilities even with appropriate licenses activated. The investigation showed that the company was using an outdated version of the vulnerability scanning module that wasn't updated for the last 3 months due to misconfigured auto-updates. Once auto-updates were reconfigured, the system started detecting new security threats.

Inconsistency of backups and available storage volume

If not controlled, SIEM system backups can take all available storage slowing down the system and even causing its complete inoperability.

Case 2: While planning out a SIEM solution, a financial services company decided to have the online data access for 1 month and the offline data access for 1 year. After implementing the system, the company increased the term of the online data storage up to 6 months, and the offline data access was prolonged up to 3 years without taking into consideration the system's initial capabilities, which led to a storage bottleneck. The company had to turn to SIEM consultants to solve the problem. After analyzing the issue, the SIEM team offered to set up an external storage that could take the load off the SIEM solution.

Conclusion

Installing SIEM software is not enough to ensure effective threat management. Once deployed, a SIEM solution requires proper fine-tuning to fit an organization's unique IT landscape and threat profile. To see real returns on their investments into SIEM, companies have to ensure not only a system's basic configuration, but also go through correlation rule customization that allow a SIEM system to show its real capabilities as an advanced analytical security tool, not just to be a mere warehouse of uncontrollable security events.

About the Author

Serguei Tchesnokov

Senior SIEM Consultant at ScienceSoft, Serguei is an IBM certified Security Professional with a 9-year background in Security Information and Event Management and a 16-year work experience in Information Technology. Serguei's portfolio includes projects on architecture design, integration, and deployment of security solutions based on IBM Security QRadar SIEM, IBM TSIEM/TCIM, IBM Security Identity Manager (SIM) for healthcare, banking, financial and governmental organizations.

Cloud Computing Security Issues: What Can Be Done?

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

The goal of cloud computing is to bring all of an organization's features like databases, mail, software applications and more into one easily accessible place. Organizations that use cloud computing do not have to pay for hosting the information because the service provider hosts the information. Data storage and applications for the organization are kept in the cloud. This also means that the service provider will have more control of the security infrastructure, will have control over compliance and regulation, and will do the monitoring of the organization for compliance. Although the cloud was supposed to be a better way to store data, the use of the cloud brought with it new security risks. This paper will explore some of those risks. .

Introduction

The advent of cloud computing has made subscribing to services like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), easier for organizations easier for organizations to operate. These subscriptions were created to cut costs and maximize profit for the organization, by allowing employees to work at any time in any place (Orman, 2016). Organizations are not only providing a way for all employees to access the system, hackers can also find ways into the system more easily.

Generally, when an organization has the infrastructure in house, both internal and external audits can be easily done to monitor the system at any time. However, when all resources are move to and stored in the cloud, there can be challenges to confidentiality and integrity of the system (Ryoo, Rizvi, Aiken, & Kissoll, 2014). Another challenge for cloud users is that instead of a closed system that is controlled by the organization, a three-way system exists between the organization, the cloud service provider and the end users. The more systems involved, the more vulnerable the organization is to attack. In addition, auditors are not always familiar with the cloud's terminology and may not understand how the cloud works (Ryoo et al.).

Viega (2012) stated that the cloud is more secure than people think. Viega attempted to assuage people's fears by showing how the cloud has similar controls as traditional IT models. Viega suggested that organizations have the same control over the cloud as they have in traditional systems, and at the same time, these two systems are very different so comparison is difficult. Although it is true that the cloud has many good qualities, there are still issues of security that must be addressed.

Analysis of Cloud Articles on Security Issues

A random literature review using the key words cloud security and cloud computing compliance issues, was conducted analyzing challenges with cloud security and compliance issue. I analyzed the challenges to cloud computing in 25 peer reviewed articles about between 2011 and 2013 and then compared them to problems between 2015-2016.The results were that the problems within these years, problems were the same and solutions were similar. The articles were generally written by people working in IT fields and computer security. This information made it clear that people using the cloud must understand the ramifications of it and how to circumvent security problems.

Identification of Security and Compliance Issues

There are many issues encountered in past years that continue in current articles. One major issue is the fact that several organizations come together to use a public cloud for hosting. With more than one organization on the same host, if one is hacked, it can leave all other organizations at risk (Ogigau, 2012). Another challenge in security is that vulnerabilities happen during transition from an older system to the cloud. Primarily, when organizations make the transition, a failure to think out the entire process before the move is made creates common vulnerabilities. Organizations may have to spend time dealing with glitches in the process that can also leave them vulnerable. In addition, if the organization does not understand the big picture of security concerns, they may not understand the changes that need to be made. When this happens, the problem is shared between the service provider who may not understand the bigger picture of security concerns (Doney & Leite, 2011).

Khan (2016) pointed out that cloud outages are common and they are more targeted security attacks. A Symantec (2016) report showed that an increase of attacks by 91% came from targeted attacks due to spear-phishing attacks that began in 2013. Ryan (2013) stated that the major problem for cloud security is the fact that information is shared with the service provider. The sharing of data makes the organization vulnerable to attacks from both inside and outside the organization. Also, data can be lost by the host through accidental deletion or information that is modified incorrectly. These are just a few of the challenges that organizations face as they continue to operate within the cloud.

Compliance Issues

Yimam and Fernandez (2016) stated that when organizations move to the cloud, they do so without understanding that there are compliance issues that are pertinent to each of the software packages. In the United States, FISMA, HIPAA, SOX and PCI are all compliance entities that have to be taken into account depending on the type of business.

Buckman and Gold (2012) researched education and noted that when educational institutions moved to the cloud, the issue of security and confidentiality still had to be in place. Education must be able to comply with FERPA laws and other programs that govern how educational institutions deal with students, financial needs, and Internet security needs within their institutions. This means that moving to the cloud will make the institution more dependent on a third party to offer security. In each of these situations, organizations can see that when they move to the cloud, no matter what industry, the organization must understand how transition to the cloud and understand compliance issues prior to making the transition.

Solutions

Although cloud security has challenges, there are solutions that can impact the way in which security is done that can decrease risk. Solutions begin with the enactment of the agreement. For example, creating international agreements with subscribers in their country of origin that promote and enforce compliance and regulation of the laws, is one way to start working on solutions. Employees who work with IT security must also understand what is needed to transition to the cloud before the transition begins. For example, treating the transition to cloud as a project would assist the entire organization to understand the roles for the transition and the planning that is necessary. For example, project management principles could be used from start to finish so that roles could be identified, innovation could occur, and the process of transition would be more smoothly completed.

Conclusion

Weakness in the public cloud environment presents hackers an opportunity to exploit the host network to create loss of information or data across the network. To circumvent critical systems of organizations residing on the same host, organizations using the cloud must understand what this means and how to develop the process over time. Lack of intercontinental regulations, compliance and laws for cloud computing violates HIPPA, GLBA and PII rules. To solve this problem, governments and industry leaders must agree on technological standards, establish universal compliance, implement a provision of cloud computing services to guarantee data security and privacy, and understand that the organization is still vulnerable.

References

Buckman, J., & Gold, S. (2012). Privacy and data security under cloud computing. *College and University, 88*(2), 10-22.

Dlodlo, N. (2011). Legal, privacy, security, access and regulatory issues in cloud computing. *International Conference on Information Management and Evaluation*: 161-168. Reading: Academic Conferences International Limited. Retrieved from ProQuest database. Document ID: 1010335812

Dorey, P. G., & Leite, A. (2011). Commentary : Cloud computing – A security problem or solution? *Information Security Technical Report,16*(3-4), 89-96. DOI: 10.1016/j.istr.2011.08.004

Khan, M. A.(2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications, 71*, 11-29. DOI: 10.1016/j.jnca.2016.05.010

Ogigau-Neamtiu, F. (2012). Cloud computing security issues. *Journal of Defense Resources Management, 3*(2), 141-148.

Orman, H. (2016). Both sides now: Thinking about cloud security, *IEEE Internet Computing*, 20(1), 83-87. DOI:10.1109/MIC.2016.17

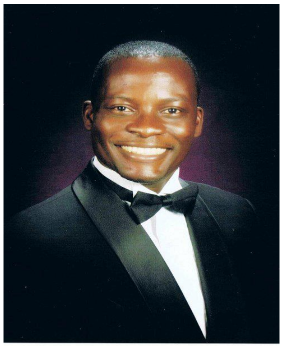
Ryan, M. D. (2013), Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software,86*(9), 2263–2268. DOI:10.1016/j.jss.2012.12.025

Ryoo, J., Rizvi, S., Aiken, W., and Kissell, J.(2014). Cloud security auditing: Challenges and emerging approaches. *IEEE Security & Privacy, 12*(6), 68-74. DOI:10.1109/MSP.2013.132

Symentec. (2016). 2016 Internet security threat report. Retrieved from https://www.symantec.com/security-center/threat-report

Viegan, J., Cloud security: Not a problem. (2012). *IEEE Security & Privacy, 10*(4), DOI:10.1109/MSP.2012.93

About The Author



Dr. Daniel Osafo. Harrison, D.C.S, Security+
Daniel is a Doctor of Computer Science in Information Assurance, Senior Cybersecurity Administrator and Compliance Auditor for Industrial Control Systems at Bechtel Nuclear Security & Environment and a member of Cyber security Team at Pueblo Chemical Agent-Destruction Pilot Plant for Department of the Army. He functioned across the enterprise as a technical liaison between governance and administration, regulatory compliance and implemented and managed cyber-security solutions. Daniel can be reached online at odharrison4@yahoo.com and at our company website http://www.bechtel.com/

OPEN ACCESS APIs

WHAT NEEDS TO BE DONE TO MAKE THE PLATFORM MORE SECURE

By David Midgley, Head of Operations, *Total Processing*

I'm sure if you're reading this, you already have a reasonable idea of what an API is and how it works. For anyone who may have stumbled upon this article though, an API lets one website use elements of another. In its' simplest terms, an API is what allows third-party apps to run in Facebook.

For example, it is an API that allows you to share an article on a national newspaper's website via your social media accounts and then show on the national newspaper's website how many people have shared that article.

APIs also have their use in the payments sector too. For example, in the case of Total Processing and other payment gateway providers, we give our clients access to data so they can connect their website to the payment gateway we provide them and then also allow them to access data when payments are made via the gateway, and I'm sure this is also the case for other payment gateway providers.

Therefore, given that an individual's personal and financial details are being provided on the website and via these gateways, it is important this access is properly secured and cannot be easily worked out or hacked into by malicious parties.

For example, in January 2015, the self-titled 'internet security enthusiast' Paul Price flagged up that the API of British greeting card manufacturer Moonpig used a hard-coded username and password to connect to their server that was easily retrievable.

This meant that, according to Price's analysis, it would have been very easy to build up a database of the addresses and card details of over three million people who used Moonpig's service in a matter of hours.

Thus, it is evident that vulnerabilities that can be exploited exist in APIs. This means patches and other updates still need to be developed in order to firm up the integrity of the firewalls put in place to prevent undesirables from being able to access what is very sensitive financial and personal information that can be used to access a person's bank account or steal their identity.

It's not difficult to sure up the security of an API either, and no one should feel unconfident or overwhelmed at the prospect of doing this.

As a start, a company should keep all security software used internally and externally up-to-date and make sure their privacy and spam settings are rigid to help prevent a hacker from gaining access via a company's own systems.

Furthermore, organisations should implement two-stage authentication like 2FA (2-Factor Authentication; Password and SMS) at the very least.

In addition, limiting the data request rate for consumer applications would also help to prevent, or at least limit, a malicious party's ability to bring your site down by overloading it with high-frequency traffic via the API.

The API developers using Representational State Transfer (REST) principles when designing the interface should also help with security too. REST uses a set of at least five different commands to access data.

Therefore, if an API is implemented in a RESTful way, it will have predictable outcomes, thereby simplifying the security for the person implementing it, but making it difficult for an outside party who doesn't have access to break the security walls down.

All of this is particularly pertinent for us in the UK as our present government has said it wants banks to open up access to customer data using APIs in order to help drive innovation and boost the level of competition in the sector. The government has even said they will legislate to make this a reality if they have to as well.

There is an argument to be made for why this would be a good thing too, as more competition in banking means these institutions will have to work harder to innovate.

Hopefully, this in turn will drive the product and service levels up for the consumers. Furthermore, a more open publication of data should assist alternative providers by giving them a new source of information that will help them to make more efficient and effective lending decisions.

Therefore, the implementation of open APIs giving access to banking data is going to happen. However, this doesn't have to be as worrying as it may seem. Banking APIs being open should hopefully force them to prioritise making their API tools as secure as possible.

I say this as banks opening up access to customer data should also lead to new stricter regulations coming in that would require these institutions to make sure adequate security measures are in place.

Furthermore, the government has tasked an Open Banking Working Group (OBWG) led by the industry to develop the framework that would underpin the open banking standard needed to facilitate the plans.

As part of this, the OBWG has published a report has said that an independent authority would be responsible for handling complaints and establishing "how data is secured once shared, as well as the security, reliability and scalability of the APIs provided".

This independent authority would also be able to "vet third parties, accredit solutions and publish its outcome through a white list of approved third parties".

Access would only be granted where the bank account holder has given informed consent, so if you're still worried about your banking data being accessible via an open platform, it is possible to opt out.

Therefore, it is safe to say that safe that the use of APIs will continue to grow, particularly given that the UK government wants our financial institutions to use them and even uses open access APIs themselves to give anyone who is interested access to their own departments' data sets via the launch of data.gov.uk.

The increased use of APIs is in many ways a good thing too. Software or websites being able to use the data and functionality of other software and websites helps to create a quicker and more fluid browsing experience for users.

Furthermore, the government is now pushing for banks to use open API, which is very good, as if nothing else, the implementation of an open API should make the security of the platform your data is held on even better, and these better security measures should also spread to other industries.

Finally, open access APIs will also help to make the level of competition among banks even higher for you as a consumer, and the government then looks for other industries to also do the same, your choices as a consumer should improve in other areas too.

About The Author

David is Head of Operations at the payment gateway and merchant services provider Total Processing. Prior to joining Total Processing in February 2016, David spent over two and a half years at the merchant services provider Axcess Merchant Services having previously sent over nine years in a variety of roles at the banking group HSBC.

He lives in the city of Leeds, West Yorkshire in Great Britain. David can be reached online on Twitter @davidmidgley4 and at our company website https://www.totalprocessing.com/.

New Venue
New Opportunities

Not Listening to Your CIO Can Cost You Millions

Why companies need to rethink traditional, perimeter network protection

By Jean Turgeon, Vice President & Chief Technologist, Avaya

When you leave your house for the day, do you lock the front door but leave the back door unlocked and the windows open? No, because you wouldn't leave other access points open and exposed.

In a recent study commissioned by Avaya, businesses cited complexity (35%), lack of resources (29%), didn't know it was possible (22%) and too risky to the rest of the network (22%) as reasons for not implementing end-to-end network segmentation, an essential security measure.

Using the same analogy, if a locking mechanism for your home seemed complex or was going to cost more initially than anticipated, would you simply just leave your home exposed? Neither would I.

So, why relax standards when it comes to securing confidential company and customer data?

End-to-end network segmentation is essential to ensuring the various entry points to business data are kept secure.

The dilemma most companies face is that while a majority of security spending is directed towards a rigid network perimeter, this traditional perimeter has morphed into an "everywhere perimeter" due to cloud computing, outsourcing,

IoT and BYOD technology. All respondents to the aforementioned study agreed that end-to-end segmentation is an essential security measure (75% "strongly agree") – yet only about one-in-four (23%) say their organization actually implements end-to-end segmentation.

Without proper controls, a breach of one of these entry points – such as an employee's email or device, or a wireless connection – could provide a hacker with the virtual keys to the castle.

A proper end-to-end network segmentation deployment is a foundational measure to address the fluid characteristics of an everywhere perimeter.

Unlike traditional technologies that may not extend network wide and are onerous to deploy, end-to-end segmentation natively extends from the data center to the desktop or smart devices while reducing complexity and operational burden.

Today’s network segmentation provides businesses the ability to create stealth segments that span the entire network. Network security is initiated at the core and extends wherever it’s needed; between the company’s hub and server, and across all access points, including email and individual devices, whether they are in country or 6,500 miles away.

All applications can be isolated and secured individually, yet still run over the same physical infrastructure. Running business critical applications independently of one another creates a safety zone that hackers cannot see and therefore cannot access.

Managing application security individually also enables businesses to add or remove segments securely, without exposing or leaving gaps in the network.

The cautionary tales are all around and should serve as perpetual wakeup calls for businesses to implement effective strategies to reduce their exposure.

Most recently the World Anti-Doping Agency data breach springs to mind in which 30 top athletes’ private medical records were exposed.

If we look at Health Care in the U.S. alone, data breaches cost American hospitals roughly $6 billion per year. In fact, Federal health regulators recently announced a record-breaking $5.55 million settlement with one of the nation's biggest health-care systems for breaches that compromised about 4 million electronic patient records.

Setting aside the actual cost of a data breach – there’s also the intangible costs of damage to brand, reputation and consumer trust.

The average business may well be able to sustain a one-time breach cost financially, but the loss of trust and loyalty from consumers and partners can be crippling.

In a world where more employees are insisting on flexible work environments and the ability to use their own devices, and where customers have an expectation that businesses be “on” and accessible at all times, the need to ensure security over extended networks and distances will only increase. It’s not enough to just lock the front door.

About The Author

Jean Turgeon (well known in the industry as ‘JT’) is vice president and Chief Technologist of Software Defined Architecture within the Worldwide Sales organization at Avaya.

Turgeon is responsible for driving and delivering the strategy for Software Defined Architecture, and accelerating adoption of Fabric Networking solutions in the Enterprise and Midmarket.

He also leads the strategic solutions initiative for Public Safety.

In his current role at Avaya, Turgeon leads a global team of Networking Sales specialists, and is the lead Networking evangelist.

His team works closely with customers to advocate and drive strategic sales investments and initiatives promoting an end-to-end Fabric-based architecture solution that delivers business value.

Turgeon was instrumental in launching the Avaya Collaboration Pod, a turnkey solution to quickly deploy unified communications and contact center solutions in a public, private or hybrid cloud environment, through partnerships with VMWare and EMC.

Turgeon joined Avaya in 2009 through its acquisition of Nortel's Enterprise assets, and played a pivotal role in integrating the Nortel Networking business, team and products into the Avaya portfolio.

At Nortel, Turgeon was most recently General Manager for the Networking Business Unit leading its Product and Strategy groups.

Prior to that, Turgeon held numerous leadership roles at Nortel and Bay Networks within the Research & Development, CTO Office, Support and Professional Services, Training and Technical Marketing organizations. He is a prolific speaker at international industry events and conferences.

A native of Ottawa, Canada, Turgeon holds a degree in Electronics from the Institut Teccart, and an Executive MBA from University of Ottawa.

Outside of work, Turgeon is a self-confessed 'speed-freak', and enjoys motor racing, snowmobiling, boating, biking and hockey. He and his wife, Lorraine, are proud parents to four children.

Jean can be reached on Twitter, and on the company website, http://www.avaya.com/en/.

Privacy and Security Issues in Autonomous Cars

by David Navetta, Boris Segalis and Kris Kleiner, Norton Rose Fulbright US LLP

As the development of self-driving car technology progresses, the prospect of privately-owned autonomous vehicles operating on public roads is nearing. Industry experts predict that autonomous vehicles will be commercially available within the next five-to-ten years. However, the use of this technology presents significant privacy and security issues that should be explored and addressed before these vehicles are fully commercialized.

I. Privacy issues

Because autonomous vehicles are largely experimental at this time, it remains unclear what type of personal information may be collected by these vehicles. Nonetheless, at a minimum, location data associated with a particular vehicle will be tracked and logged. Location tracking has already proven to be a lightning rod with respect to mobile phones. Some of the privacy considerations related to the use of autonomous cars are discussed further below.

a. Owner and Passenger Information

Perhaps the most important information that could be collected, particularly when combined with other information discussed below, is identifying information about the owner or passenger of the autonomous vehicle. It is likely that the autonomous vehicle would need to maintain information about the owner and passengers for a variety of different purposes. For example, the vehicle would likely need to maintain information about passengers to authenticate authorized use. Furthermore, information about the passengers would also lend itself to a variety of conveniences that are common in many cars available today, including customizable comfort, safety, and entertainment settings. It is likely that cars, based on setting preferences and other information collected while in use, will be able to identify drivers, passengers and their activities with a high degree of certainty.

The Drivers' Privacy Protection Act and other federal statutes, including the Electronic Communications Privacy Act and Federal Communications Act, could apply to certain aspects of autonomous vehicle data and communications. Additionally, 47 states and the District of Columbia have enacted laws applicable to personal information. While these laws are generally applicable to data breaches, many also include requirements for safeguarding personal information. Although these laws provide for some protections of various personal information, because of the type of data involved, the manner of collection, or the entity collecting the data, some or all of these protections may not be applicable to autonomous vehicles.

b. Location tracking

Location data is something that is necessarily implicated in the use of autonomous vehicles. In fact, it has been happening for some time now, but additional location information would allow the ability to provide additional features and benefits to the user. For example, navigation features available in many modern cars include the option to save specific locations in memory;

use current location and planned route to identify additional information relevant to the trip, including real-time traffic data, points-of-interest on or near the planned route; and to set routing preferences, such as avoiding highways or toll roads.

Correlating location, destination, speed, and route data with additional information about the passenger, and date and time of the trip would allow someone to get a picture of when, where and how an individual travels, particularly if this information is stored or logged over some period of time. This information may prove very beneficial for purposes of traffic planning, reducing congestion and improving safety, but it also could be used for secondary marketing purposes. However, viewing travel data and patterns over time may also enable one to deduce other information about the owner or passengers, such as where they live and work as well as locations like stores, restaurants and other establishments that they frequently visit.

The privacy risks associated with the collection of and access to location information raise both individual personal and larger policy and societal concerns. On an individual basis, the availability of location information "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." For example, accessing an individual's historical location and destination information would permit visibility to "trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." Even where location information does not reveal this type of private information, the ability to identify the present location or historical travel patterns of a particular person make them more susceptible to physical harm or stalking if the information is accessible to the wrong person.

From a commercial perspective, location and destination information could provide valuable marketing information to advertisers. Knowing where a person lives, works, and shops would allow a business to infer information about income level and spending habits. One could envision the tracking and storage of autonomous vehicle data to lead to lawsuits similar to those filed against various internet advertising companies engaged in behavioral tracking using cookies. There are various other implications of this data, ranging from providing customized advertising using interfaces connected to the Internet in the a vehicle (on a dedicated screen, through the car's speakers or to mobile devices in the car) to specifically routing a vehicle to expose a captive audience of passengers to certain businesses or destinations based on personalized interests inferred from their individual data.

Perhaps the most fundamental question that needs to be considered is how the collection and sharing of location data impacts the concept of an individual's "reasonable expectation of privacy," which impacts both protections afforded by Fourth Amendment and the applicability of privacy interests in tort law. Another factor that complicates the reasonable expectation of privacy issue is the potential that location data from autonomous cars would be shared with third parties, including the manufacturer or other service providers.

c. Sensor data

Autonomous cars in use today (and again many existing human-driven vehicles) contain various sensors that collect data relating to the operation of the autonomous vehicle as well as its surroundings. By constantly collecting data about its surroundings, however, the vehicle is continuously capturing information about the people and things it encounters, creating a potential privacy concern in the same way that a different Google project, Google Street View, drew the interest of the Federal Communications Commission (FCC).

There, the FCC imposed sanctions on Google for its conduct in gathering Wi-Fi network and “payload” data during the Street View project. One can imagine that autonomous vehicles could collect driving habits, destinations and other revealing information about other drivers without their knowledge or consent. Additional concerns could arise based on the use of imagery captured by the vehicle, including ownership disputes and potential invasion of privacy claims, depending upon the circumstances in which the images are captured.

One specific type of “sensor” that deserves particular attention is the voice-recognition and control system of the autonomous car. Many consumer devices currently on the market integrate voice control functionality, including smart phones and televisions. The addition of these features to consumer products has led to public concern and complaints about the collection and transmission of private communications.

In October 2015, California enacted legislation regulating voice-recognition technology in smart televisions. These laws require manufacturers of smart televisions to inform customers about the voice-recognition features during initial setup or installation and bar the sale or use of any speech captured by voice-recognition technology for advertising purposes andprohibits the manufacturer or entity providing these features from being compelled to build specific features for allowing an investigative or law enforcement officer to monitor communications through that feature.

II. Security issues

In addition to individual privacy concerns, autonomous vehicles also present issues relating to personal safety and security. The potential security risks come from a variety of sources, both internal and external to the automated vehicle itself, which are discussed in further detail below.

a. Hacking

In a 2014 Harris Interactive survey about the use of autonomous cars, more than 50 percent of respondents raised concerns about the prospect of having a hacker gain control of the vehicle. In 2015, researchers Charlie Miller and Chris Valasek were able to exploit a vulnerability in certain Chrysler vehicles to gain control of the vehicle’s internal computer network. Miller and Valasek discovered the vulnerability in the entertainment system, which allowed remote access through an open port in the system. With access to the entertainment system and the CAN bus, Miller and Valasek were able to remotely manipulate various systems, including the air conditioning controls, stereo, windshield wipers, transmission, steering, and were able to both kill the engine and engage or disable the brakes. Although these vulnerabilities occurred in normal vehicles, they illustrate some of the potential risks that could arise with autonomous vehicles, as one would expect many of the features and systems available in normal cars to be available and included in autonomous vehicles. Furthermore, to the extent that autonomous cars lack the ability for a passenger to take control of the vehicle to respond, the safety threat posed by these vulnerabilities could be even more acute.

b. Bugs

The next source of risk related to personal safety with autonomous cars comes from the technology itself. Karl Lagnemma, director of a start-up focused on the development of software for self-driving cars explained the risk posed by software bugs, stating: “[e]veryone knows security is an issue and will at some point become an important issue. But the biggest threat to an occupant of a self-driving car today isn’t any hack, it’s the bug in someone’s software because we don’t have systems that we’re 100-percent sure are safe.”

Steven Shladover, a researcher at the University of California, Berkeley, stated that having “safety-critical, fail-safe software for completely driverless cars would require reimagining how software is designed.” Although bugs in the software in other devices, like computers, smart phones or other devices, are relatively common, the implications of software failure in an autonomous car could have much more serious implications. This is a risk widely recognized by American consumers, as 79 percent of consumers have cited fears that “equipment needed by driverless vehicles—such as sensors or braking software—would fail at some point.”

c. Algorithms

The algorithms used in the autonomous vehicle’s decision-making process also present potential risks to the safety of passengers and those in the vicinity of the vehicle:

- How should the car be programmed to act in the event of an unavoidable accident?
- Should it minimize the loss of life, even if it means sacrificing the occupants, or should it protect the occupants at all costs?
- Should it choose between these extremes at random?

Unlike human drivers who make real-time decisions while driving, an automated vehicle’s decision, although based on various inputs available from sensor data, is a result of logic developed and coded by a programmer ahead of time.

The difficulty in making and coding the decision process is illustrated in the following hypothetical:

An automated vehicle is traveling on a two-lane bridge when a bus that is traveling in the opposite direction suddenly veers into its lane. The automated vehicle must decide how to react with the use of whatever logic has been programmed in advance. The three alternatives are as follows:

A. Veer left and off the bridge, which guarantees a severe, one-vehicle crash;

B. Crash head-on into the bus, which will result in a moderate, two-vehicle crash; and
C. Attempt to squeeze past the bus on the right. If the bus suddenly corrects back toward its own lane (a low-probability event given how far the bus has drifted) a crash is avoided. If the bus does not correct itself, a high-probability event, then a severe, two-vehicle crash results. This crash would be a small, offset crash, which carries a greater risk of injury than the full, frontal collision in Alternative B.

Conclusion

The technological advancement in autonomous vehicles will be staggering and has already generated significant excitement. However, the legal issues and risks associated with obtaining and using personal data, as well as the various cybersecurity threats, need to be thoroughly considered before commercialization.

About The Authors

David Navetta is a US co-chair of Norton Rose Fulbright's Data Protection, Privacy and Cybersecurity practice group. David focuses on technology, privacy, information security and intellectual property law.

His work ranges from compliance and transactional work to breach notification, regulatory response and litigation. David has helped hundreds of companies across multiple industries prepare for and respond to data security breaches.

Boris Segalis is a US co-chair of Norton Rose Fulbright's Data Protection, Privacy and Cybersecurity practice group and has practiced exclusively in this area since 2007.

Boris advises clients on data protection, privacy and cybersecurity issues arising in the context of compliance and business strategy, technology transactions, breach preparedness and response, disputes and regulatory investigations, and legislative and regulatory strategy. He represents clients across industries, from Fortune 100 global organizations to emerging technology and new media companies.

Kris Kleiner is an associate in Norton Rose Fulbright’s Data Protection, Privacy and Cybersecurity practice group. Kris regularly advises clients on best practices as well as compliance with state and federal privacy and cybersecurity regulations and have experience assisting various clients operating in multiple industries in identifying, remediating, and responding to data privacy incidents.

David, Boris and Kris can be reached at David.Navetta@nortonrosefulbright.com, Boris.Segalis@nortonrosefulbright.com, and Kris.Kleiner@nortonrosefulbright.com, or at our company website http://www.nortonrosefulbright.com.

CYBER SECURITY EXCHANGE

DECEMBER 4-6, 2016

PGA NATIONAL RESORT AND SPA - PALM BEACH GARDENS, FLORIDA

www.cyber-securityexchange.com

#CYBEREXCHANGE

MEET THE SPEAKERS:

The Cyber Security Exchange speaker faculty is an exclusive community of innovators, **influencers, and leaders.** Embrace the **opportunity to enhance the power and reach** of your professional network by sharing three **days with the most respected cyber security executives in the industry, including:**

BOBBY SINGH
CISO
Toronto Stock Exchange

JOSH JAFFE
Director: Information Security Risk and Governance
Emerson

HARRIS SCHWARTZ
Global Head of Security
Levi Strauss

ALEX KOEHLER
Executive Director/CISO
Amgen

KATHERINE FITHEN
Chief Privacy Officer
The Coca-Cola Company

DENNIS DICKSTEIN
COO, Americas
UBS

PATRICIA COLLINS WEEDON
SVP & Global CISO
Discovery Communications

EDWIN MARTINEZ
CISO
CEC Enterprises

Empowering the Human Element of Cyber Security Across the Organization while Addressing Security Gaps and Vulnerabilities in the Ever-Changing Threat Landscape

- Strengthening third party and vendor relationships while reducing the risk privacy, security and compliance
- Evolution of Security Incident Response for more holistic enterprise management
- Effective business communications across the C-Suite to better secure the enterprise
- Inventive and productive ways to engage employees on cyber security awareness

BROUGHT TO YOU BY: IQPC Exchange

REQUEST AN INVITATION AT:
www.cyber-securityexchange.com | spexchange@iqpc.com | 813-658-2553 | Mention code: CYBERAD

Understanding Bluetooth and its role in the Internet of Things

By Dimitri Vlachos, VP of Marketing, Pwnie Express

Bluetooth technology was originally designed for continuous, streaming data applications - essentially, it was intended to replace wires to create the possibility of a Wireless Personal Area Network.

The (then new) technology added a digital layer in many consumer and industrial applications, and has since become incredibly widespread.

Bluetooth is now a standard feature in most phones, cars and computers, and becoming increasingly included in a variety of other devices. With the introduction of Bluetooth Low Energy, devices that are considered a part of the Internet of Things - like smart door locks or soccer balls - are now using Bluetooth technology.

Though Bluetooth Classic and Bluetooth Low Energy share a name and a wavelength, they are fundamentally different technologies. While most consumers don't realize that their Bluetooth headphones and their Bluetooth light bulbs function differently, they do understand that products with the stylized B symbol can be controlled with their phones.

This has contributed, in part, to the widespread adoption of BLE as an IoT protocol. Instead of learning an entirely new system, consumers just need to use the Bluetooth functionality on their phone or computer to control the cornucopia of devices using Bluetooth technology.

These devices are being used across all industries - healthcare, athletics, energy, home, and more. The Bluetooth Special Interest Group has even defined several BLE/Bluetooth Smart "profiles" for compatibility within different applications.

These include everything from blood pressure and glucose monitoring to calculating a runner's speed and cadence profile. New devices have included BLE in everything from health monitoring services to the ability to assess environmental conditions.

This widespread adoption of Bluetooth technology has not only led to cheap hardware and consumer adoption, but also criminal adoption. Not only is Bluetooth being added to consumer devices such as shoes and water bottles, but it is also being added to criminal devices such as credit card skimmers.

The same ease of use offered by consumer Bluetooth devices is now very common in criminal devices.

Unfortunately, the widespread adoption of Bluetooth functionality also comes with the prevalence of Bluetooth security risks. Far too little has been done over the years to ensure the security of a Bluetooth connection.

Some examples of Bluetooth security risks are Man in the Middle attacks (intercepting and then changing commands), identity tracking, intercepting information, disruption of a device's operations, and passive eavesdropping.

While most people think your heart rate or music preferences aren't that important, best practices for Bluetooth security should always be engaged, as eavesdropping (or unauthorized filming) could happen during an important, or secure, phone call made through an older Bluetooth speaker.

In fact, though the Internet of Things is striving towards making our everyday life easier, there is an ever-growing presence of an Internet of Evil Things.

The Internet of Evil Things is a very real threat. In fact, the UK Government has banned Apple Watches from Cabinet meetings out of fear that they will record the room audio, track GPS coordinates, or even monitor heart rates and be used as a crude lie detector.

As more and more capable devices are woven into people's daily lives, there is more and more risk associated with the vulnerabilities of those devices.

Some of Bluetooth's vulnerabilities have already been demonstrated, and while not all may seem dangerous, each provides another example of extra connectivity that resulted in expanded vulnerabilities.

As many know, cars have been hacked into, proving that insecure Bluetooth functionality will provide hackers with another beachhead in the future. Bluetooth Smart locks, which are meant to keep homes and businesses secure, have also been revealed to be easily penetrable.

Securing Bluetooth connections should be like securing any kind of device or network – first and formost, the protocol should be secure. However, you can still open yourself up to vast risks if you aren't careful implementing your Bluetooth technology.

The best security against Bluetooth vulnerabilities is simple: keep your devices up-to-date. Bluetooth 4.2 is more protected than previous versions, however only further updates will be able to protect against vulnerabilities as they crop up.

Another piece of advice is to take connected devices out of discoverable mode, and to be wary of any unknown devices you pair with.

In addition, configuration and standard protections are extremely important when it comes to Bluetooth. Never leave your device in its default configuration - that is probably the easiest way to allow a hacker to break into your device.

Also, take advantage of the security features that exist on your device. Is encryption optional?

If so, be sure to turn it on. Enable PINs when connecting to your device, and make sure you choose a strong one that you have never used before.

Lastly - and perhaps the most obvious piece of advice - don't download any suspicious files.

Though Bluetooth and BLE are increasingly adopted across all verticals, the security industry has lagged behind.

Current network security tools focus almost exclusively on standard wired ethernet networks, often ignoring wireless networks and Bluetooth devices.

Following Bluetooth best practices certainly helps, but businesses need to be aware and have the visibility and control over the devices - all of the devices - that are in their environment.

About The Author

Dimitri Vlachos brings over 15 years of marketing leadership in both startups and established corporations to Pwnie Express.

Most recently he served as VP of Marketing at ObserveIT where he was responsible for scaling demand generation and establishing the company as a leader in Insider Threat management.

Before ObserveIT, he served as VP of Marketing and Products at Riverbed Technologies, where he was responsible for all marketing and products across the $250M performance management business unit.

He has also held roles at Mazu Networks (acquired by Riverbed), Cisco, and BBN (acquired by GTE).

Dimitri is a graduate of Bucknell University, and can be reached online at
dimitri@pwnieexpress.com, @DimitriVlachos, or http://www.pwnieexpress.com

Lock, stock and two smoking … access controls

By Milica D. Djekic

The point of this article would not be to deal with some London's gangs, but rather to present what the access control is and why it matters. We already know that the one who controls the access – controls the entire asset. Right here, we would deal with so fascinating, but still so simple topic such as Lampson's matrix and also try to provide a better insight how the systems being based on that matrix function in a physical way. So, get prepared – this would be a good drive through the world of lock, stock and two smoking – let's say – access controls.

The access control got crucially significant to protecting your resources from the unwanted approaching on. Many today's solutions would rely on the well-known Lampson's matrix system, while some novel designs would deal with the fingerprinting technology. Such a technology got so convenient to highly sophisticated systems and it's something that we would usually meet in the science-fiction movies, follow ups and shows. The Figure on our right would illustrate some of those highly sophisticated technologies – probably finding its role with some well-simulated and graphically designed video game or film. The secret with this sort of technology is that you would take someone's fingerprint's pattern and use it every single time – you intend to access that asset. Only if your fingerprint trace and such a sample match relying on pattern recognition technology – you would get the access on.

Right here, we would suggest that the standard access control systems would deal with the Lampson's matrix. The matrix is something similar to a table where every row and column got their meaning. In a Lampson's matrix, the rows got called the subjects, while the columns got called the objects. The subjects can perform an operation over the objects which are defined in a table or – more precisely – the matrix. The Table 1 illustrates how this works in a practice.

As it's demonstrated through the Figure 1 – the users 1 and 2 are the *subjects* which can perform the *operations* read and write over the *objects* being recognized as files 1, 2, 3 or 4.

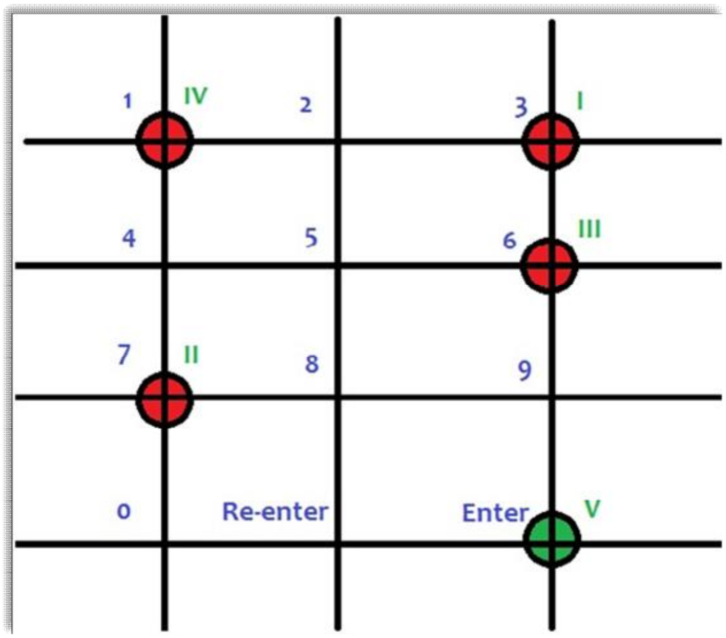


Table 1. The Lampson's matrix illustration

The Lampson's	File 1	File 2	File 3	File 4
User 1	-	read	read, write	-
User 2	read	-	write	read, write

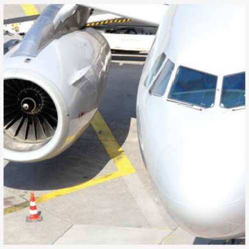
The experience would suggest that this could get created not only mathematically, but rather physically using the wires and buttons. Such a Figure has been given on our left and it demonstrates how pressing the button with your bank's card machine – you can get an access to your funds. In such an example, it's getting clear that entering the PIN code *3761* and pressing *Enter* – you can pass through that control's check. Simply, once you press the button – you will make a contact between two wires representing the rows and columns of the Lampson's matrix. It's all about the fields representing something and being used to offer an access. Finally, we would conclude this effort indicating that the access control found many practical applications and it's not used to secure your funds only – but rather your objects, assets and properties. Hope this brief insight gave a good overview on how everything function in a reality and what could be the advantages of this simple and still inexpensive technology.

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.

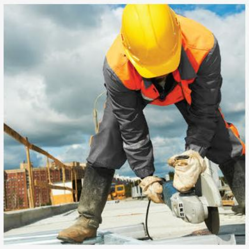
Indonesia Infrastructure Week 2016

9-11 NOVEMBER 2016 | JAKARTA CONVENTION CENTER

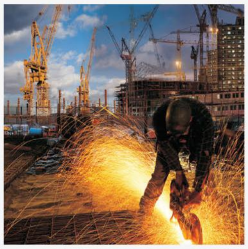


DISCOVER 1,000+ MULTIFORM PRODUCTS

OVER 20+ COUNTRIES



ACCESS TO THE GLOBAL MEETINGS PROGRAMME



200+ EXHIBITORS

EXPLORE 8,500 SQM EXHIBITION AREA

END TO END SOLUTIONS ACROSS CRITICAL NATIONAL INFRASTRUCTURE

ATTEND HIGH LEVEL CONFERENCES

JOIN THE FREE VISITOR CERTIFIED WORKSHOPS

INDONESIA'S LARGEST INFRASTRUCTURE GATHERING

AIRPORT SOLUTIONS INDONESIA 2016

IIICE 2016 INDONESIA INTERNATIONAL INFRASTRUCTURE CONFERENCE AND EXHIBITION

EXPO COMM™ INDONESIA 2016
BROADBAND – CYBER SECURITY – SMART CITY INFRASTRUCTURE

KONSTRUKSI INDONESIA 2016

THE BIG 5 CONSTRUCT INDONESIA
International Building & Construction Show

REGISTER NOW for **FREE FAST TRACK ENTRY!**
Visit at **WWW.INDONESIAINFRASTRUCTUREWEEK.COM/REGISTER**

EXHIBITION TIME : 9 NOV 2016, 13:00 - 19:00 | 10 NOV 2016, 10:00 - 19:00 | 11 NOV 2016, 10:00 - 17:00

Sponsored by
SMI PT SARANA MULTI INFRASTRUKTUR (PERSERO)
Vermeer EQUIPPED TO DO MORE.
alhua TECHNOLOGY
Telkom Indonesia the world in your hand
ARIM Technologies

Featured Event
ASEAN 628 INFRASTRUCTURE INVESTMENT FORUM 8th NOVEMBER 2016

Organized by
Infrastructure asia A Tarsus Group Company
Tarsus Tarsus Group plc

Co-Organized by
dmg::events
EJK E.J. KRAUSE & ASSOCIATES, INC.
F&E AEROSPACE A Tarsus Group Company

Comparing the Options: An MBA or a Master of Science in Cyber Security

What degree is right for you?

University of San Diego Center for Cyber Security Engineering and Technology

Moving into a leadership, managerial or C-level position within the cyber security field typically means obtaining an advanced degree. But which degree is the best degree? For most cyber security professionals, the choice comes down to a Master of Science in Cyber Security or an MBA.

A Master of Science in Cyber Security

There are many reasons to be excited about a Master of Science in Cyber Security. For one, the field is in desperate need of skilled, qualified and highly educated professionals.

According to reports, there are roughly 1 million unfilled cyber security jobs and that figure is expected to reach 1.5 million by 2019. Robert Herjavec – founder and CEO at Herjavec Group, a Managed Security Services Provider with offices globally – told CSO,

> "Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats."

Secondly, salary estimates for professionals with an advanced degree in cyber security are high. Entry-level positions, such as information security analyst, are commanding a median annual salary of $90,000 with figures reaching into the six figures in areas such as New York, California and Virginia. This means experienced and highly educated cyber security experts will be paid handsomely for their skills.

For example, one of the more senior jobs in the field, security software engineer, receives an average annual salary of $233,333 according to Dice and a chief security officer can expect an average annual salary of $225,000. Veronica Mollica, founder and executive information security recruiter at Indigo Partners, Inc. in Fairfield, Connecticut told Forbes,

> "Our candidates are facing competing offers from multiple companies with salary increases averaging over 30%. Current employers are scrambling to retain talent with counter offers including 10% and higher salary increases for information security team members to remain on board."

A master’s degree in cyber security engineering will give students the specific skills and tools that are required by employers. Students will be able to explore cyber security mitigation strategies and tactics in depth and gain a level of expertise that is desperately needed to combat the rampant cyber security attacks affecting businesses, governments and individual citizens.

As opposed to a more generalized degree, a master’s in cyber security will offer extremely specialized and focused training. This can be especially helpful for students interested in cyber security engineering or a top-level leadership position.

Finally, because the demand for cyber security professionals is so strong, there are many scholarship programs available to those looking to further their education in the discipline. For example, the Information Assurance Scholarship Program and the Yellow Ribbon Program are two such scholarships.

Master of Business Administration (MBA)

An MBA with a technical specialization is another option that those interested in cyber security advancement often consider. The MBA is a well-known, highly respected degree that offers students a variety of options upon graduation.

However, because the MBA is such a popular degree choice, it is less likely that an MBA will help you stand out amongst the competition when you are vying for that top role.

If you are looking to differentiate yourself from the competition and know that you want to work in cyber security, an MBA might not give you a huge boost over fellow applicants.

Plus, in order for an MBA to get you a high-level position in cyber security, you will likely need to supplement a relevant bachelor’s degree and years of experience in the field with certain cyber security certifications.

However, many employers today are looking for cyber security professionals who possess certain skills such as accounting or management, in addition to their cyber security knowledge. An MBA would be the perfect degree through which to gain these skills. According to a 2015 report from Burning Glass Technologies,

> “The hardest-to-fill cybersecurity jobs call for financial skills, such as accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of the ‘hybrid jobs.’”

If you are looking for a degree with more flexibility that could lead to a broader set of career options outside of cyber security, or want to explore topics such as finance and operations, an MBA could be the right choice.

What If You Could Get the Best of Both Worlds?

There is a third option. Rather than simply choosing between a master's degree in cyber security or an MBA, consider a degree that combines the two.

If you are looking to benefit from both the leadership and management aspects of an MBA as well as the technical, theoretical and tactical components of a cyber security degree, your best option may be a degree in cyber security operations and leadership.

This degree gives you the best of both worlds by building on your bachelor's degree and your field experience to give you a deeper understating of tools and tactics for defeating adversaries, plus leadership and management skills specific to the cyber security field.

The University of San Diego, a leader in cyber security education, offers this degree 100% online, so that you can keep working while obtaining your masters.

Deciding what degree is right for you depends largely on your objectives and goals. By looking closely at what each program offers and aligning the objectives of each with your own career and educational goals, you will be able to find the best degree path for you.

About University of San Diego's Online Master of Science in Cyber Security Operations and Leadership

The University of San Diego's **100% online Master of Science in Cyber Security Operations and Leadership**(MS-CSOL) is designed for bachelor-prepared students who desire to effect positive change in mitigating cyber security threats and become leaders in their organizations. This degree program is designed to serve the needs of a diverse set of individuals who are currently in cyber security roles as well as those interested pursuing a career in cyber security.

University of San Diego Center for Cyber Security Engineering and Technology

The University of San Diego's Master of Science in Cyber Security Engineering program emphasizes critical skills for cyber practitioners who protect the prosperity and safety of citizens. Students of this program learn both applied and theoretical technical knowledge and skills which enables graduates to thrive in their chosen career. Learn how you can position yourself for the future and contribute to the mitigation of modern threats today.

Cybersecurity: Why Your Cell Phone is Your Weakest Link

The internet of things. It’s a wonderful product of society’s love of technology and needs to make daily tasks more efficient. Think about it. How many devices do you own? Most people today have at the very least a smartphone, computer, and tablet.

These devices all share data, so you don’t have to worry about which device you downloaded “Monster Mash” on for the kids to listen to in the car. All devices can play the song.

This idea of convenience has transferred not just through electronic devices but to other common household items. Today, homeowners can buy anything from a smart car to a smart fridge.

While smart home automation isn’t by itself insecure, any one of these everyday household objects is hackable. Why? They’re all controlled by your smartphone.

Small Devices, Big Security Risk

While most people know to install antivirus on their computers, not as many people think to add this protection to their smartphone, and even less think that they should protect their smart fridge or thermostat.

Any IoT device can be compromised if someone hacks your cell phone. What makes matters worse is that these hackers can then pivot from device to device and gain access to other devices like your tablet and computer.

This scenario involves just one home. Imagine every smartphone in the country getting hacked due to this security fall.

Homeowners are the only ones vulnerable, though. A 2015 study by Check Point Software “found that organizations with more than 2,000 devices on the network have a 50% chance that at least six of them are infected.”

With many companies opting for “Bring Your Own Device” programs, proper cybersecurity and has become critical for company success. Since personal cell phones can’t be monitored, it makes it harder to monitor.

If one of your employees decides to go out to Starbucks, for example, and connects to their wifi while there, they could actually be connecting to a dummy wifi-signal masquerading as Starbucks. Hackers can use Pineapple Wifi to view and collect any information transmitted over this signal goes directly back to the hacker.

As a business owner, you should do more than just hope they don’t open any company emails while on their coffee break.

Between rogue wifi, malware, and innocuous apps, there are multiple ways to infect phones and then other devices.

Attack Preparation Tips

The number of risks to both consumers and businesses will only increase in the coming years with new technology.

However, by increasing awareness of these problems more people can better protect themselves.

Here are some security measures you can take to protect your personal information:

- Download antivirus for your phone and update it regularly.
- Always use a password. Make sure it's not a commonly known fact or phrase. Never use this password for other applications.
- Disable Bluetooth when you aren't using it. This is one of the easiest access points for a hacker to connect.
- Encrypt your information with a VPN. Using a VPN allows you to easily secure your information and doesn't require much technical knowledge.
- If you have children and let them use y0ur cell phone or other connected devices, teach them online best practices.

Protecting your phone from unwanted cyber attacks will keep your personal and financial information safe. Hacking into phones is incredibly easy because anyone can Google articles online and teach themselves how to hack.

By increasing awareness about cybersecurity and informing people about which steps to take to stay safe, hackers will have a harder time trying to steal your information.

New devices come onto the market daily. It's important to make sure that with you purchase, you also invest in the proper security measures to keep it, and your current electronic family safe.

About the Author

Megan Ray Nichols is a freelance science and writer and the editor of Schooled By Science. She writes weekly on scientific news stories. Megan is a regular contributor to Datafloq, Big Data Made Simple and The Energy Collective. You can subscribe to her blog here and follow her on Twitter.

Developing an immunity to cyber-crime

How new machine learning and mathematics are automating advanced cyber defense

By Dave Palmer, Director of Technology, Darktrace

Overview and background

Do you know that more than 200 days can pass before a company realizes its firewalls have been breached and critical systems compromised? Conventional security breaches such as information being stolen or websites defaced are a thing of the past.

Instead, the real danger today are the quiet and unseen attacks – or insider threat – where attacks are perpetrated from within the organization, either inadvertently or with ill intent, and systems are altered at will or kill switches installed and ready to be activated.

Many high-profile headlining breaches, from the leak of the Democratic National Committee's (DNC) network to the recent Dropbox cyber-theft of 68 million passwords, display familiar characteristics of insider attacks. Instead of an immediate impact, the malware operates subtly, gathers information and waits for the correct moment to strike.

In the case of the DNC breach, the hacker capitalized on Windows vulnerabilities and remained in the network for close to a year, outwitting all detection attempts by allegedly relocating a Trojan from one machine to another.

With the Dropbox password hacks, the attack stemmed from a previously discovered theft of email addresses in 2012 – where the hackers managed to surreptitiously siphon passwords for years through a compromised vector that was thought to have already been patched and secured.

It is especially concerning that cyber-criminals succeeded in the above instances despite the deployment of advanced cyber-security software and policies. Clearly, a new era in cyber warfare has begun where machines are fighting other machines across the digital battlefield, and sophisticated criminals and attackers are ready to pounce at any opportunity.

Legacy approaches are not working

Existing tools are failing to deal with this new threatening reality because traditional approaches rely on being able to pre-define the threat in advance by writing rules or producing signatures.

However, today’s hackers are using unrecognized, un-signatured custom codes that constantly evolve past the latest security patches to fool and bypass legacy defenses.

Such black hat machines only need enter the organization once and from that point of entry, they observe how to appear as authentic as real devices, servers and users.

By modelling thousands of authentic users and devices, and hiding their actions quietly among everyday tasks instead of brute force port-scanning or head-on attacks, these automated attackers will blend into the enterprise system, conducting lateral reconnaissance without blowing their cover.

And before anyone can react, they can strike a fatal blow to the system in a blink of an eye once activated.

New machine learning

However, hope is not lost in the face of evolving threats as history has shown that seemingly insurmountable challenges can be solved through the adoption of new technology. For example, during the Industrial Revolution, machines came to replace manual labor.

In today’s context, organized crime and nation-state groups are using automated attacks against corporate networks, and the assaults are of such severity and speed that human responses almost always cannot happen quickly enough.

Fortunately, thanks to recent advances in complex mathematics, organizations can now fight back using their own machine intelligence.

A machine learning approach is synonymous with the make-up of our human immune system, which is based on a notion of early detection and intervention to fight against viral infection.

Similarly, benign machine intelligence can act as an enterprise’s immune system, and is able to automatically differentiate what is inherent to the body, and what is manifestly ‘anomalous’.

The enterprise immune system is able to do so because it uses advanced algorithms in a mathematical framework to instinctively process and make sense of the torrential deluge of data in the system, and so establishing the network’s baseline ‘pattern of life’ or what is inherent abnormal.

Once the Enterprise Immune System comprehends a network’s ‘pattern of life’, it then makes logical, probability-based decisions against external and insider threats at machine speed and at scale.

Like the biological immune system, such an approach can instantaneously and automatically uncover infections.

The Enterprise Immune System can also undertake the necessary actions, such as creating digital antibodies, without the need for active human intervention.

Rather than rely on automated rule-based approaches which can only protect against known threats, organizations should also incorporate a machine learning approach to continuously monitor the network and quickly uncover emerging threats that have managed to slip past perimeter defenses.

Humans, for their part, should also let machine intelligence do the heavy lifting of detection and focus on complementary skillsets like high-level threat analysis and mitigation.

Via such high-level self-learning defenses, it is now possible to give companies a fighting chance to protect themselves against the relentless assault of advanced and automated cyber threats.

About the Author

Dave Palmer is the Director of Technology at Darktrace. A cyber security technical expert with more than ten years' experience at the forefront of government intelligence operations, Dave has worked across UK intelligence agencies GCHQ and MI5, where he delivered mission-critical infrastructure services, including the replacement and security of entire global networks, the development of operational internet capabilities and the management of critical disaster recovery incidents.

At Darktrace, Dave oversees the mathematics and engineering teams and product strategy. He holds a first class degree in Computer Science and Software Engineering from the University of Birmingham.

Dave is regularly approached for counsel on data breaches and threat actors. His insights on the recent Ashley Madison, Sony Pictures Entertainment and TalkTalk data breaches have been cited extensively.

For any further inquiries, please contact Alice Goodman at alice.goodman@darktrace.com.

IT'S NOT IF,
BUT WHEN.

Database Honeypots: Sweet and Simple Breach Detection

By: Dave Rosenberg, CTO of Products, DB Networks

Organizations are quickly coming to the realization that if they haven't already been a victim of a cyber attack, it's very likely they ultimately will. It's not a matter of "if" but rather of "when". A much larger concern to organizations is that once they've been attacked, cyber criminals can often operate undetected for very long periods of time.

Mandiant stated in the 2016 M-Trends that the average dwell time from breach to detection is presently on the order of 146 days. Cyber criminals can do a lot of damage over that extended length of time.

The key to quickly identifying system breaches is sufficient instrumentation and real-time analysis. The task of security instrumentation and analysis may appear daunting. An emerging strategy is to not only instrument at the perimeter but also deep inside the infrastructure. It's critical to instrument the likely goal of a cyberattack – breaching the organization's databases.

Databases hold the "crown jewels" of an organization, and this may include financial data, personal information, correspondence, as well as intellectual property. In some organizations the database infrastructure may even store highly classified government information. Regardless, databases are always a highly prized target for cyber criminals.

An often over looked yet simple security instrument is a database honeypot. Setting up a database honeypot results in an instrument any organization can employ to assist in identifying when a breach has occurred or is reoccurring.

Honeypots are useful decoys because once a cyber attacker has penetrated the organization's perimeter they typically begin reconnaissance to understand the network and all of the connected systems.

The idea with the honeypot is to trigger an alert to identify the cyber attack very early in the attack process, hopefully during the reconnaissance phase when the damage is minimal.

A database honeypot can be quickly established by simply creating a database table not to ever be accessed by anyone or any application.

Multiple honeypots can be created across the infrastructure, and the more honeypot traps an organization sets the greater the likelihood of exposing a breach. It's important for the database honeypot to appear legitimate and enticing.

While the most effective database honeypot will be unique to each organization, in general, financial information tends to make an enticing target. A honeypot table named EMPLOYEE_DIRECT_DEPOSITS as an example that may just do the trick. You don't need to actually populate the database honeypot with any data. Any attempt to read or update the honeypot table will trigger an alert, and that's the goal for this security instrument.

It's possible to use native database auditing facilities to monitor the database honeypot. However hackers may see that auditing is enabled and become suspicious. Another option is to employ non-intrusive continuous monitoring of database traffic such as the DB Networks DBN-6300.

Alerts on any access to the database honeypot can be created and because it operates on a SPAN port or network TAP its operation won't be visible to the attacker. You want to gather as much forensics data as possible to understand the origin and scope of the attack.

However, if you tip your hand, valuable forensics may be unobtainable as the attacker may begin to exploit other areas of your infrastructure where you lack adequate monitoring.

Should the database honeypot trigger, the highest priority alert needs to be sent to the security operation center for immediate action. This is potentially an extremely serious security situation. It's a clear indication there's nefarious activity deep into the IT infrastructure.

The alert could be the result of an insider nosing around where they shouldn't be or it could possibly be a cyber attacker you've ensnarled. In either case the highest level of response is necessary to triage the situation.

In the case of the cyber attacker, you not only know they have the ability to access your databases, but they have most certainly breached other networks and security mechanisms to reach that point deep into your IT infrastructure.

A simple database honeypot is certainly limited in its scope no question about that. However, the return on investment as a security instrument is quite large and most certainly should be considered as part of a database defense in depth strategy.

About the Author

Dave is DB Networks CTO of Products responsible for leading the advanced technical research and patent development. Prior to joining the company, Dave served as VP of Engineering at WireCache, where he and his team developed the industry's first general purpose, Oracle database accelerator appliance. DB Networks acquired this important technology in 2009 which brought Dave and WireCache team into DB Networks.

Dave brings more than 30 years of technology development experience, including ten years at VP level for Oracle Corporation's server technology.

Dave earned his B.A. in Mechanical Engineering/Fluid Mechanics from UC Berkeley, and served in the Air Force for six years, where he earned his M.S. in Astronautical Engineering from the Air Force Institute of Technology.(yes, he is a rocket scientist!).

IoT ASIA | 29 – 30 March 2017

SINGAPORE EXPO

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

Establish your presence and meet new customers at

Asia's leading IoT event!

www.internetofthingsasia.com | #iotasia

Industry Recognition

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

SINGAPORE EXPERIENCE AWARDS 2015 RECIPIENT
TRADE CONFERENCE ORGANISER OF THE YEAR
for CURATING SINGAPORE'S BEST EVENTS

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
TCAM Technology Pte Ltd

Top 10 Best Practices for Cyberbreach Post-Crisis Communication

By Rishi Bhargava

According to an article appearing in AT&T Cybersecurity Insights, 62 percent of all organizations surveyed admitted that they had suffered a breach in 2015. Furthermore, although 42 percent reported that the breach had a "significant negative impact" on their company, only 34 percent felt that they had an effective plan for responding to the incident. One critical element that is often lacking in an incident response plan is a clear strategy for communicating the cyberbreach with all parties requiring notification.

After a cyberattack, the following Top 10 best practices for managing your post-crisis communications can prove beneficial.

1. Silence is not golden after a cyberbreach. Organizations need to communicate quickly, but be wary of over-communicating. If necessary, issue a "hold statement" that conveys that the team is aware of the issue, is investigating the cyberbreach, and will provide more information as it becomes available.

2. Ad lib statements are not advisable. An effective incident response plan should include boilerplate prepared statements that have already been approved by stakeholders for use following a breach. Rely on these statements rather than off-the-cuff comments.

3. Deliver communications in clear terms that avoid overly technical terms or industry jargon. If the message lacks clarity, people might think the organization is hiding something. For similar reasons, avoid responding to questions with a terse "no comment".

4. All communications should maintain the same voice. This does not mean that only one person needs to handle all communications. It simply means that communications should deliver a consistent message and use a consistent tone.

5. Focus on the people affected by the cyberbreach rather than the breached organization. Breach notification should simply be a part of a customer relationship strategy, as well as a part of an incident response plan. Customers need to feel that the organization cares about the impact that the breach might have on them and that the organization will take care of their problems. Express concern for their inconvenience in a sincere manner without acknowledging any wrongdoing by the company.

6. Do not overlook employees. They need to be kept in the loop and provided with any guidance that they might need.

7. Have an effective means of communication. Consider dedicating a section on the existing website or creating a separate website where customers and the media can find

current information. Organizations might consider using an intranet site for employees, vendors or others who already have access to the intranet.

8. Take a proactive approach to communicating the positive steps that the organization is taking to respond to the cyberbreach. Report on the recovery or corrective measures, as well as the progress of your investigation.

9. Keep promises. If an organization has promised employees that they will be provided with statements that they can use to respond to calls from customers, make sure to follow through. If a press conference has been promised at a specific time, ensure that the spokesperson is there. If customers have been promised additional information as soon as it is known, deliver it in a timely manner. Avoiding the press or your customers will only contribute to the suspicion that the company has something to hide.

10. Maintain a comprehensive communication plan. Last but not the least, the above points should be captured in a comprehensive communication plan which is available to all the stake holders inside the organization.

Cyberbreaches continue to occur at an ever-increasing rate. How a company handles communications after a breach can have a significant impact on public perception as well as customer relations. These communication best practices are critical for creating a positive perception about the company in time of crisis. It is also a must to have these processed documented and tracked to see if they are followed appropriately. Conducting mock exercise and analyzing the responses from different teams for these can help in being better prepared for when the real attack occurs.

About the Author

Rishi Bhargava is Co-founder and VP, Marketing for Demisto, a cyber security startup with the mission to make security operations - “faster, leaner and smarter”. Prior to founding Demisto, Rishi was Vice President and General Manager of the Software Defined Datacenter Group at Intel Security. A visionary and technology enthusiast, he was responsible for delivering Intel integrated Security Solutions for datacenters. Before Intel, Rishi was Vice President of Product Management for Datacenter and Server security products at McAfee, now part of Intel Security. As an intrapreneur at McAfee, he launched multiple products to establish McAfee leadership in risk & compliance, virtualization, and cloud security. Rishi joined McAfee by way of acquisition in 2009 (Solidcore, Enterprise Security Startup). At Solidcore, he was responsible for Product Management and Strategy. As one of the early employees and member of the leadership team, he was instrumental in defining the company's product strategy and growing the business; Rishi has over a dozen patents in the area of Computer Security. He holds a B. S. in Computer Science from Indian Institute of Technology, New Delhi and a Masters in Computer Science from University of Southern California, Los Angeles. Rishi is passionate about new technologies and industry trends and serves as an active advisor to multiple startups in silicon valley and India.

6TH SCADA WORLD SUMMIT

Quote **"CYBER DEFENSE"** to qualify for extra **10% discount*!**

*discount applicable to 2-day summits.

- Main conference: **9 & 10 November 2016**
- Post Conference Workshops: **11 November 2016**
- Pre-conference Workshops: **8 November 2016**
- Venue: **Kuala Lumpur, Malaysia**

What Makes 6th SCADA World Summit 2016 A Must-Attend Event!

Recipe for Success Hear from **Cross-industry SCADA Professionals and Project Owners** share their experiences in managing SCADA system integration, upgrading and maintenance within an energy efficient environment through various large scale projects globally

Interactive Discussions Join **exclusive panel discussions featuring SCADA industry experts** as they share their challenges and perspectives in eliminating cyber security threat and adopting smart applications to elevate SCADA system operational efficiency

Eye-opening Presentations Gain strategic insights from **over 20 industry experts** on overcoming major challenges in managing SCADA system including **Cyber security risk, complicated SCADA system integration and upgrade, achieving accuracy on real time data acquisition, improving connectivity between MTU and substations, data management and protection, reducing human errors in SCADA operation and amongst others**

In depth Workshops Attend the **6 Expert-Led Pre-Summit Workshops** to grasp the nuts and bolts in achieving effective SCADA system management

Researched & Developed by: EQUIP GLOBAL

Media Partners: GAS Gas Association of Singapore, AISA Australian Information Security Association, APSM Asia Pacific Security Magazine, Australian Security Magazine, CHIEF IT, CSEAN Cyber Security Experts Association of Nigeria, CDM Cyber Defense Magazine, GeoConnexion The local geoinformation serving the World, Gulf Oil & Gas gulfoilandgas.com, Offshore VN, SGCyberSecurity.com, WorldOils, Global Information, Inc.

PHONE: 65 6376.0908 EMAIL: enquiry@equip-global.com
WEB: http://www.equip-global.com/6th-scada-world-summit-2016

Companies in Middle East Using DNS for Data Transport will become Cybercrime Targets

Rod Rasmussen, vice president of cybersecurity at Infoblox

Malicious DNS tunnelling is a big problem in cybersecurity and companies in the Middle East should be aware of this. The technique involves the use of the Domain Name System (DNS) protocol to smuggle sensitive corporate or personal information out of a network, and to enable malware command and control communications in and out.

Indeed, as the Infoblox Security Assessment Report revealed recently, two in five enterprise networks showed evidence of DNS tunnelling in the second quarter of 2016.

However, all is not necessarily as it seems. Close scrutiny of apparent DNS tunnelling traffic repeatedly reveals an amount of anomalous activity which appears harmful but is, in fact, being sent intentionally by users and services on enterprise networks, and tended not to be malicious in nature.

Exploiting the DNS protocol

Typically DNS queries are very small data packets, and their intended purpose is not to transport any data other than that needed to perform name-resolution services. And, although the introduction of authentication mechanisms such as DNSSEC and DKIM may have changed the landscape over recent years, their primary intent is also only to serve up information on a domain name, rather than transporting any other data.

But, there is sufficient flexibility in the DNS protocol that unrelated data can be inserted into a DNS query and then sent in to or out from a targeted network.

DNS signalling, the most basic form of this technique, typically involves using a cryptographic hash function to encode information into query strings or response records. Performance tends to be quite slow though, as the restrictive size of DNS packets mean a large number are required even for a small amount of data.

This is taken a step further by DNS tunnelling which, by employing surprisingly basic techniques, uses DNS queries to encode other protocols such as http, ftp or SMTP, over a DNS session.

For the sake of simplicity, and given their essential similarity, both of these techniques can be viewed under the header of DNS tunnelling.

“Legitimate” DNS tunnelling

Within an enterprise, the use of DNS for legitimate communications can often set off false alarms with networking and security teams on the lookout for malicious DNS tunnelling. Most companies that employ this unsanctioned use of DNS tend not to advertise the fact and this can present a challenge to security teams looking for insidious use of the protocol. After all, legitimate and malicious use can look practically identical at first glance.

Of course, those using DNS in this way are generally taking creative shortcuts rather than deliberately abusing their organisation’s networks.

It all started around twenty years ago, when paywalls in certain hotels and airports blocked direct access to the internet via standard protocols such as HTTP. It was noticed, however, that DNS wasn’t blocked and tools including NSTX, Dnscat and iodine were subsequently released allowing web sessions and email to be tunnelled through a user’s DNS connection.

Over the years these tools have evolved to provide full VPN services over DNS, with dozens of examples freely available on GitHub and elsewhere.

Not a wise use of the protocol

As well as setting off false alarms and raising concerns around theft-of-service, DNS tunnelling, even as a means of legitimate communication, is not a wise use of an organisation’s DNS protocol. Indeed, using DNS to transport data is misusing the protocol to deliberately circumvent measures put in place by the network operator.

It could be used to proxy past workplace productivity filters designed to block Facebook or personal email services, for example, or for something more sinister that could represent a risk to the whole company.

However, it appears there are a large number of commercial products which use DNS signalling as a means of providing data transfer services.

For example, at around the same time that DNS tunnelling was becoming popular as a technique, some manufacturers of customer presence equipment (CPE) were experiencing issues in sending updates out to their various consumer-grade Wi-Fi routers or cable and DSL modems across consumer and SMB networks.

It transpired that there was some inconsistency on the various types of traffic allowed through certain ISPs, and setting up proper connections through NAT-based routers was proving less than straightforward.

DNS was seen as being a viable alternative and it wasn't long before some of the CPE companies were using the protocol to perform software updates and other maintenance tasks with their installed base.

Today, most enterprise-grade networks will handle such tasks using proper communications and authentication channels. Internal departments and branch offices can often have cheaper CPE equipment, however, meaning that these signals are being transported over DNS – even in an enterprise network.

Elsewhere, the need for nearly continuous communication with their customers has seen some anti-virus (AV) vendors set up file hash identification routines via DNS.

While this is undeniably a quick and effective way of determining whether a suspect file is infected or not, it can potentially open up a network to malicious communications.

Circumventing controls

Essentially, the main problem with DNS tunnelling techniques is that they circumvent controls put in place by a network team, opening up security, compliance and operational concerns while, at the same time, overloading the DNS protocol and anomaly detection systems put in place to examine DNS traffic.

Businesses are increasingly trying to protect their DNS as its importance becomes clearer, and are beginning to realise how much extraneous DNS traffic is running on their networks.

It's perhaps optimistic to expect the practice to stop completely, but efforts could be made to persuade IT vendors and manufacturers to become less reliant on it, and ultimately make it less difficult to secure this valuable and vulnerable protocol.

About the author

Rod Rasmussen is vice president of cybersecurity at Infoblox. As co-founder of internet security company IID (a company recently acquired by Infoblox), Rod is widely recognized as a leading expert on the abuse of the Domain Name System (DNS) by cyber criminals.

CI CONNECT

Cyber Security Connect North America

Nov. 15, 2016 | Marriott at Metro Center | Washington, DC

An Invitation-Only Forum for Senior Executives in Cyber Security across North America. Hear from industry experts, including:

Nickolas Savage
Supervisory Special Agent (SSA)
Federal Bureau of Investigation (FBI)

Vivek Khindria
Director, Information Security
Bell Group of Companies

Jon Boyens
Senior Advisor for Information Security and Program Manager, ICT Supply Chain Risk Management, **National Institute of Standards and Technology (NIST)**

Drew Morin
Director, Federal Cyber Security Technology and Engineering Programs
T-Mobile US, Inc.

Rob Fry
Senior Security Architect
Netflix

Richard Starnes
CISO
Kentucky Health Cooperative

TO APPLY, PLEASE VISIT: **CanadianInstitute.com/Cyber**

The Evolving Role of Today's CFO to Chief Protection Officer

By Drew Del Matto, CFO at Fortinet

No one expected the torrential flooding of Louisiana in August of this year. Some homeowners scrambled to gather what belongings they could and escape, while others were confident that the flood wouldn't affect their neighborhood and did nothing. Many of the latter then had to be rescued by understaffed emergency crews, whose agencies also failed to estimate the size of the disaster. If everyone could have foreseen the level of severity and planned accordingly, some of the $8 to 10 million in damage could have been mitigated and an entire region's citizenry could have been kept safer.

Of course, it's not always possible to anticipate how severe a weather emergency will be, but proper planning can go a long way toward lessening its effects. The same reality can apply to an organization that experiences a security breach. CFOs and Board members are always keeping an eye on costs and are focused on proper budgeting and spending to meet bottom-line targets. However, if a meaningful security breach happens, expense control can go out the window as companies desperately try to beef up previously lacking security defenses. Even worse, the brand is affected and top-line sales are lost.

Though the price of keeping organizations secure continues to rise, budget allocation for security simply hasn't kept up. The typical company only spends between one and five percent of revenue on IT security, which seems small when compared to the risk of lost sales and productivity, as well as brand damage associated with a breach.

Consider the cautionary tale of the catastrophic data breach of a national retail chain that is now common knowledge. Following disclosure of their security breach, the company's sales declined, causing the company to miss their Q4 guidance. Customers were terrified about their financial privacy, the company's stock fell and the CEO was fired as a result. There have been many since, from medical and government organizations to all types of global businesses. Each time, valuable information is lost, and sometimes C-level leaders lose their jobs or face tough scrutiny.

Surprisingly, most organizations today continue to operate in reactive mode. We need to step away from merely managing breaches and start working to develop a culture of security, moving out of reactive and into proactive mode. Culture starts at the top – the C-suite must set the standard for governing the organization's cybersecurity posture.

In fact, circumstances have changed to such a degree that one could argue the role of the CFO has transformed and could very well be called the CPO – Chief Protection Officer. If you think about it, cybersecurity potentially puts a company's finances and value at risk, challenges compliance and regulations strategies, and increases the need for mature strategies to safeguard a company's data and overall security. As a strategic business and risk management executive, a CFO should have significant oversight and guidance in these areas. They are no longer IT-only considerations.

Security as a Stewardship Issue

The Board is ultimately responsible for data and intellectual property. If that is the case, then treating cybersecurity as an exclusively IT issue is not just inappropriate but bad business as well.

When it becomes the Board's role to go beyond merely turning a profit and on to protecting and overseeing a company's assets—both tangible and intangible—then the most critical assets are data, IP, reputation, customer trust and loyalty. As we see all too frequently, poor security can undermine or destroy all of these and create a loss of value through unnecessary volatility.

Boards and executives, as stewards of their organizations, have a critical responsibility to their customers, their intellectual property and their shareholders to ensure the safety and security of their data and systems. This ultimately comes down to thinking about security as a stewardship issue to be addressed directly by the Board.

Stewardship: Taking the Long View

Therefore, the CFO and Board members, must lead the charge in search of proactive approaches to security. Although there are ways that security staff and organizations can mitigate the damage resulting from increasingly frequent and sophisticated attacks, as the old saying goes, an ounce of prevention is worth a pound of cure.

Some organizations still hold the notion that it costs more to secure their data than to

recover from a breach. This is not, however, a sustainable or responsible approach. Breaches will become more frequent, attacks will become more persistent and sophisticated, and the costs of reacting to these breaches will continue to increase. Clearly, brands, jobs and share prices are all at risk.

The Board and the C-suite are responsible for three separate but interconnected elements of an organization: the business itself, customer data and shareholder interests. Stewardship goes far beyond making money or ensuring the financial success of an organization. It means caring for the long-term interest of the company and thinking holistically about the diverse stakeholders touched by the business. When it comes to security, though, the traditional stewards of the organization are not always equipped with the necessary perspective, skills, or knowledge. The wrong focus can, in fact, create a perfect storm of imperfect stewardship in which security is viewed as a cost center rather than an essential element of risk management.

Managing Risk

It’s not possible to eradicate all potential risk; it is just a part of life. Where there is profit to be made or leverage to be gained, organizations and their customers will come under fire and, as a result, there will always be attacks and attempts at data breaches. This is especially true in cybersecurity, given the low cost of generating a breach, the difficulty in locating and prosecuting hackers and the lucrative reward of a successful breach to cybercriminals.

However, managing risk is certainly possible. This has always been a key function of the Board – assess risk and make appropriate tradeoffs to manage it, considering the impact across the organization. Security is no different and, in conjunction with the CISO and the rest of the C-Suite, the Board must consider security versus many other factors, including cost, performance, agility, autonomy and empowerment, strategic initiatives, projects and planning, and go-to-market.

Rising to the Challenge

It is also important to note that policy and information governance are two of the most critical areas for consideration. These are areas where the Board and senior leadership can really make a substantial contribution to an organization’s security. The technical details can be worked out by a well-funded, savvy, empowered IT department, and HR and other line of business staff can address specific elements of policy and procedure. However, high-level decisions on policy and approach to information security need to come from the offices of C-level executives.

In a world of professional cybercrime syndicates, nation-state hackers and hacktivists, everyone finds themselves on one side or the other when it comes to cybersecurity. Thinking about data safety in terms of long-term stewardship will give the cyber stewards a leg up and help their organizations to respond swiftly with a well conceived strategy when a breach occurs.

About the author:

Drew Del Matto brings over 20 years of financial management experience and expertise in the network security market. Prior to joining Fortinet, Drew held a variety of senior management roles at Symantec including acting chief financial officer, as well as senior vice president and chief accounting officer. Drew also served as Symantec’s corporate treasurer and vice president of finance business operations, responsible for all treasury functions, various aspects of mergers & acquisitions, pricing and licensing, financial planning and analysis, and revenue operations. Prior to Symantec, Drew held senior finance leadership roles with Inktomi Corporation and SGI Corporation. He began his career as a CPA in public accounting with KPMG LLP.

How Can You Tell If Your WordPress Site Has Been Hacked?

WordPress is the foundation of a large chunk of the web, which makes it an obvious target for criminals and hackers. If attackers find a vulnerability in WordPress, they have a key that opens millions of websites.

Each WordPress site represents processing power, bandwidth, and a potential audience, all of which are useful to criminals.

And because WordPress tends to be used by less technically able users who may not appreciate the importance of choosing a good password or regularly updating their content management system, it's a good bet that a significant proportion of WordPress sites are easy pickings.

All of which means that WordPress site owners need to be aware what a hacked WordPress site looks like. Hackers use bots to scour the web for vulnerable sites, and, over its lifetime, the average WordPress site will be targeted dozens of times.

If you're unlucky or careless about security, your site may well be hacked at some point. You're unlikely to know about it until it's too late — hackers are sneaky and they go to great lengths to ensure that no-one, and especially not the site's administrators, discovers that the site has been compromised.

Nevertheless, there are numerous tell-tale signs that all is not well.

Google Tells Your Users The Site Is Hacked

It's unfortunately often the case that owners of compromised sites discover there's a problem because their users are informed by Google Chrome or another web browser.

Google carries out frequent malware scans of the sites in its index, and if it finds that a site has been compromised and is serving malware, it will display a prominent warning to visitors.

From your perspective, the site may look perfectly fine, but Googlebot and ordinary users probably see something different to what you — as a logged-in administrator — can see.

Increased Resource Use

Hackers target websites for various purposes: sending spam email, distributing malware, carrying out DDoS attacks, and so on. All require bandwidth and processing power.

If your site's resource use suddenly skyrockets without an obvious reason, there's a good chance it's being used by a malicious third-party.

Odd Search Engine Results

Black hat search engine optimizers use hacked sites for backlinks and to spam search engine results. A hacker may add lots of keyword-stuffed pages to your site in the hope of attracting traffic and sending it to their domain. The pages won't be visible to logged-in users, but they may be visible to everyone else.

Unusual Redirects

If your site has a decent-sized audience, the attackers may redirect visitors to sites they control, often spam advertising sites or sites loaded with malware.

If your users report anomalous redirects to other sites, it's a strong indicator that your WordPress site has been compromised.

Altered Files

If hackers are to do anything useful with a compromised site, they have to make some alterations to its files, usually by adding PHP or JavaScript files that make the site do what they want.

WordPress Security Plugins

As you can see, there are lots of ways you *could* find out that your site has been compromised, but the signs are obscure and, in all likelihood, you won't notice anything at all until it's too late.

WordPress plugins like Sucuri Security and Wordfence are designed to make it easier for you to find and fight attacks. Both include Web Application Firewalls, malware scanners, and file integrity monitoring tools that actively analyze a site for signs of attack and compromise.

WordPress is a fantastic content management system, and with a little care, it's as secure as could be hoped for. But in the hostile environment of the web, you need to be on your guard.

About the Author

Graeme Caldwell -- Graeme works as an inbound marketer for Nexcess, a leading provider of Magento and WordPress hosting. Follow Nexcess on Twitter at @nexcess, Like them on Facebook and check out their tech/hosting blog, http://blog.nexcess.net/.

IN SUPPORT OF THE GOVERNMENT'S ICT SPEND OF USD $20 BILLION OVER THE NEXT 5 YEARS

EXPO COMM™ INDONESIA 2016

BROADBAND – CYBER SECURITY – SMART CITY INFRASTRUCTURE

9-11 NOVEMBER 2016 | JAKARTA CONVENTION CENTER

DELIVERING SMART SECURE CITIES THAT ENABLE OUR DIGITAL ECONOMY

Hosted by

Ministry of Communications and Informatics

ATSI ASOSIASI PENYELENGGARA TELEKOMUNIKASI SELURUH INDONESIA
Association of Indonesian Telecommunication Providers

Supported by

KADIN INDONESIA
Indonesian Chamber of Commerce and Industry

Coordinating Ministry of Economic Affairs

WANTIKNAS Dewan Teknologi Informasi dan Komunikasi Nasional
National ICT Council

APEKSI
Association of Indonesia Municipalities

Sponsored by

Telkom Indonesia
the world in your hand

ARIM Technologies

Organized by

infrastructure asia
A Tarsus Group Company

Tarsus
Tarsus Group plc

Co-Organized by

EJK E. J. Krause & Associates, Inc.

Media Partner

CDM CYBER DEFENSE MAGAZINE

WWW.CONNECTINDONESIA.NET

PART OF Indonesia Infrastructure Week

Layered Security

Two locks are better than one

By David Share, Director, Amazing Support

Imagine you had a million dollars (or pounds). Heck, let's go crazy and say you have a billion dollars. Without a doubt you would want to safeguard your treasure trove as tightly as possible. How many locks would you create? How many people would you hire to stand guard?

How many gates and walls would you erect? Everyone would answer slightly different, but it would pretty much equate to the following response: as many as I possibly could. Which begs to question, what kind of value do you place on your information, and what would you do to protect it?

The fact is that in this day and age information has significant value. Indeed, it can encapsulate the life of an entire person in just a few kilobytes of data. However, the sad truth is that the overwhelming majority of this information and data is poorly protected.

In today's standards it is like protecting a billion dollars in cash with a zip-tie. It will keep your valuables safe and sound until someone with a bit of persistence, some technical ability and the right set of tools comes along and liberates it from you.

At this point in technology and culture, almost everyone is used to a basic layer of security. Whether it be a pin code, password, key card or key fob, people are used to entering, saying or swiping their way to gain access. In theory it should be easy for them to add a second layer of security to their routine. But, this is easier said than done.

Two pieces of behavior makes the switch all that much harder: habit and convenience. People have been using single layered security for decades now and the habit has been cemented into their minds.

People are naturally resistant to change and like to stick with the familiar. Change is made difficult by the mere fact that doing something once is usually easier than doing something twice. For many entering a code once is pretty convenient, but they put up a fuss when asked to enter another password.

In order for layered security to be adopted, peoples views regarding this must be changed. After all, the process cannot be made any easier.

Everyone at this point is quite familiar with the first layer of security. Enter a pin code or password and access is granted. A secondary layer to authenticate identity simply requires the user to enter a secondary piece of information.

Companies and services like Google have been using this for over a decade now. Say you want to access your Gmail account. First you enter your login credentials and your password. Before you gain access to Gmail secondary authentication is required.

For many this comes in the form of a code received via text message directly to the user's phone.

Enter this secondary code and you ill then gain access to the account. Don't have access to a phone? Not a problem. Secondary authentication can take shape in several forms from texts, to emails, to automated voice messages, all the way to a human operator calling to give a code.

When told of its efficacy in deterring attacks and breaches, many users are left surprised and can't believe that they did not implement this security measure much sooner.

Adding another one or two layers of security may seem like a minor inconvenience to a lot of people, but the benefits of doing so are inversely proportional to the risks they are exposed to.

The math is pretty easy; the more layers of security you need to access your data, the more security measures an attacker needs to bypass to gain access to your data. If it's a little difficult for you to gain access, it makes it ridiculously difficult for attackers to gain access.

About The Author

David has held positions as Operations Director and Head of IT in legal and professional firms for more than 10 years. He is a Director and co-owner of Amazing Support, a Microsoft Silver accredited and specialist Managed IT Support and IT Services company.

David actively helps SME businesses receive better Managed IT Support and IT Services in the London and Hertfordshire areas.

He also assists overseas companies who are looking to expand their business operations into the UK and helps with their inward investment IT process. A professional member of The Chartered Institute for IT (BCS) and an event speaker promoting business start-ups and technology awareness.

Married with a son, you will often see him riding his bicycle around the Hertfordshire towns! David regularly participates in charity bike rides for the British Heart Foundation.

David can be reached online (email giveme@amazingsupport.co.uk , Twitter @davidmshare), and at our company website http://www.amazingsupport.co.uk/

CYBER SECURITY EXCHANGE ASIA

27-29 November 2016 ■ Phuket, Thailand

DID YOU KNOW?

- **75bn USD** - is how much the worldwide **cyber security market** is currently worth and expected to **grow two fold** by 2020
- **$32.95bn USD** is how large the **Asian cyber security** market is expected to grow by 2019
- **$200bn USD** is the forecast for connected devices by 2020
- **$30bn USD** is the predicted growth for the **global managed security services market** by 2020

MAJOR TOPICS TO BE COVERED AT CYBER SECURITY EXCHANGE ASIA

1 **Detecting an attack**, how to and how not to address a data breach

2 **Discussion of the Asian regional** cyber security policy

3 **Ransomware** - best practice risk assessment, prevention and response

4 **The role of the Chief Risk Officer** in an organisation's cyber security strategy

5 **How to get the most out of your systems** using your staff

6 **Strategies for implementation** with the convergence of IT, OT and physical security

SOUNDS INTERESTING? WE WANT YOU!

Come be a part of **Cyber Security Exchange Asia 2016, 27-29th November 2016 in Phuket, Thailand**, as we bring together 45 CIOs, CISOs and Heads of Cyber Security from across Asia, to discuss the challenges faced. Visit **www.cybersecurityexchangeasia.com** to find out more information on this unique event.

If you would like to request an invitation to see if you qualify to attend this event, email **enquire@iqpcexchange.com** referencing code **CSCDM_Del**

OR

If you would like to have 30 minute pre-scheduled meetings, to offer your solutions to these CISOs and Head of Cyber Security, email **enquire@iqpcexchange.com** to find out what opportunities are available referencing **CSCDM_SX**

+65 6725 9921 | **enquire@iqpcexchange.com** | **www.cybersecurityexchangeasia.com**

The packet analysis as a helpful way of network monitoring

By Milica D. Djekic

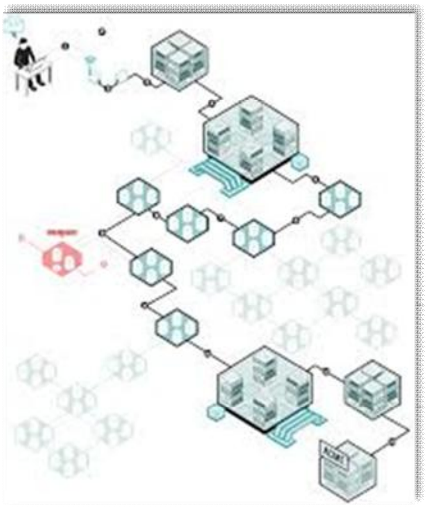
The internet packets are the sets of information being created and transmitted to carry on a message through the network's communications. These packets may consist of many bytes and they would also get some details regarding source and destination data as well as much more useful information describing the packet.

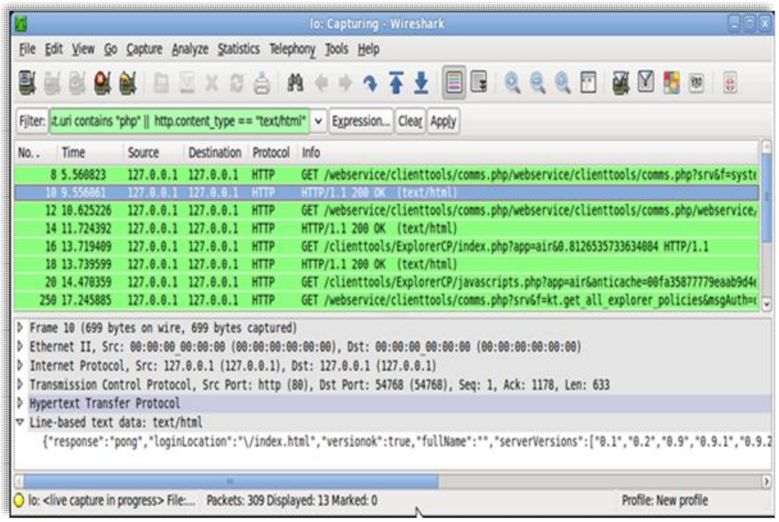
One of the most convenient tools being used to a packet analysis today is a Wireshark offering many good functions and capabilities. This tool could get used for a hacking as well as defense purposes. It takes only few days of training to learn how to take advantage over that application. Through this article, we intend to discuss how such software could get used as well as provide a bit closer look to a smart packet analysis.

In order to get an appropriate insight into a situation within the network's communications – it's so important to deal with the both – software and hardware.

Dealing with the hardware is from crucial importance because that part of operation would define which segments of the packets could get captured and transmitted to an analysis.

Sometimes the beginners may deal with the equipment so unskillfully and instead of capturing someone's network's traffic; they would simply capture their own network's communications.




lo: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: st.uri contains "php" || http.content_type == "text/html"

```
No. .  Time        Source     Destination Protocol Info
     8 5.560823    127.0.0.1  127.0.0.1   HTTP     GET /webservice/clienttools/comms.php/webservice/clienttools/comms.php?srv&f=syst
    10 9.556061    127.0.0.1  127.0.0.1   HTTP     HTTP/1.1 200 OK  (text/html)
    12 10.625226   127.0.0.1  127.0.0.1   HTTP     GET /webservice/clienttools/comms.php/webservice/clienttools/comms.php/webservice,
    14 11.724392   127.0.0.1  127.0.0.1   HTTP     HTTP/1.1 200 OK  (text/html)
    16 13.719409   127.0.0.1  127.0.0.1   HTTP     GET /clienttools/ExplorerCP/index.php?app=air&0.8126535733634084 HTTP/1.1
    18 13.739599   127.0.0.1  127.0.0.1   HTTP     HTTP/1.1 200 OK  (text/html)
    20 14.470359   127.0.0.1  127.0.0.1   HTTP     GET /clienttools/ExplorerCP/javascripts.php?app=air&anticache=00fa35877779eaab9d4
   250 17.245885   127.0.0.1  127.0.0.1   HTTP     GET /webservice/clienttools/comms.php?srv&f=kt.get_all_explorer_policies&msgAuth=

▷ Frame 10 (699 bytes on wire, 699 bytes captured)
▷ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▷ Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 54768 (54768), Seq: 1, Ack: 1178, Len: 633
▷ Hypertext Transfer Protocol
▽ Line-based text data: text/html
    {"response":"pong","loginLocation":"\/index.html","versionok":true,"fullName":"","serverVersions":["0.1","0.2","0.9","0.9.1","0.9.2
```

lo: <live capture in progress> File:... Packets: 309 Displayed: 13 Marked: 0 Profile: New profile

The Figure on the right would suggest how the packets would travel through the network and use some of the storage devices on that way to stay there for a while.

The parts of the network receiving and sending the packets are called the routers and so commonly they would use the switches to make such a transmission more efficient.

As we said – the most frequent software being used to packet analysis is a Wireshark.

That tool is so simple to get applied and it may offer many advantages once you make a decision to configure your network dealing with the internet traffic and sniffers being equipped with the software and physical gadgets.

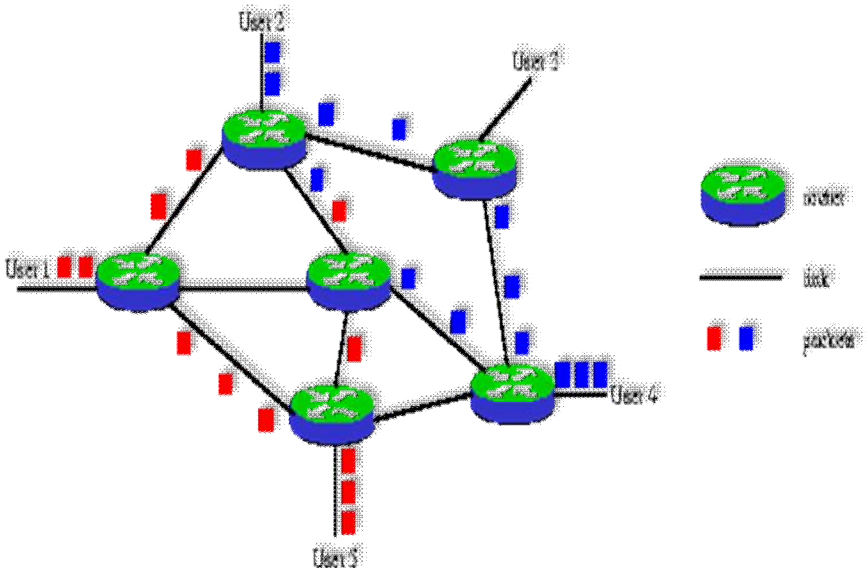
The Figure on the left would demonstrate how Wireshark capturing option appears.

We would strongly encourage everyone being interested to learn more about this tool to take advantages over many web resources offering an opportunity to learn and explore everything you want to know about this software.

As we already mentioned - Wireshark is quite convenient to ethical hacking purposes and defense applications.

One more thing being used in a network communication is a protocol. The protocol is a set of the rules that computers use to communicate with each other.

The most typical protocols are TCP, UDP and IP. Dealing with the protocols is more like dealing with the standard human communication.



There would be some common rules – similarly as in the person – to – person communication.

For instance, the good analogy could be – Person 1: *“Hi! How are you?”*; Person 2: “*Good, thank you. Yourself?”* and Person 1*: “I am fine, thank you!”* Practically, that’s how the protocols communicate between each others. It’s quite simple, convenient and clear!

Many Wireshark’s experts would suggest you to have a look at that how the packets of the information got transmitted.

For instance, if you notice that some of the packets within that environment would indicate that it has done a re-transmission, it would non-doubtly suggest that there must be some error with the sending and receiving options.

On its way from a source to a destination – the packets may straggle to get delivered. Sometimes the routers as the devices in a communication network could cause a concern.

Please have a look at the Figure on our right and try to notice that the entire network would deal with the routers, users, links and packets being sent and received.

If you choose the physically appropriate locations to put your sniffers there, you would so easily get in a position to read that internet traffic.

Finally, a described approach would seek some technology to get used as well as software in order to get your network traffic being monitored.

As we said – this method could be helpful to monitoring purposes, while the Wireshark would most commonly get used to hacker's operations as one of the network penetration's testing tools.

Anyway, all of those would include a defense purpose and require from such equipment to get applied smartly and effectively.

Using some tools to a packet analysis may get the quite interesting business to get done, so we would strongly recommend to everyone to try to play with these tools and test their capacities.

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.

Adding Efficiency to Security

By Dave Thompson, Senior Director, Product Management, LightCyber

The words “operational efficiency” and “security” are generally not commonly used together. I’m amazed that after 20 years in the networking/network security industry, vendors get away with hyperbolic messaging in the place of substantive objective evidence of value. A fundamental problem for measuring an organization’s operational security effectiveness is the industry’s lack of a metrics to define what “success” looks like. Simply put, how much time and resources should be spent on security, and how do you measure operational success?

Despite the fact that IT security product spending has grown rapidly to nearly $30 billion dollars in spending per year, industry vendors haven’t been held accountable to justify the costs of new security solutions. The result is that security practitioners are left with expensive solutions that are not proven to help them achieve their mandate – to provide effective protection of critical infrastructure, and to rapidly detect and respond to intruders that get in. As a result, security practitioners generally feel overwhelmed and underappreciated, and that has to change.

One of the primary challenges for the security industry, is the overwhelming and growing volume of alerts coming from the growing volume of incumbent security solutions (IDS, Sandbox, SIEM, or otherwise). The staggering volume of alerts wastes time and resources spent triaging and researching the predominant volume of false positives. Increased staffing has become challenging, with a worldwide shortage of a million security professionals. At the same time, organizations have limited budgets and couldn’t continue to linearly increase staff to meet the growing volume of security alerts.

How does a security operator even know where to start with that level of alerts, especially considering that a large majority of these are false-positives? Today, two-thirds of the security staff’s time is wasted due to the gross inefficiency of their tools, according to the Ponemon study, and only 4% of all alerts can generally be investigated. There is a likelihood that several of the 96% of those ignored alerts may convey something important. These kinds of statistics would be completely unacceptable in other parts of IT industry. Even major league baseball would be appalled by such averages!

The flood of alerts overwhelm security organizations, making it nearly impossible to spot anything that is truly representative of a real network attack.In short, the overwhelming majority of security tools purchased today are primarily focused on detecting the evidence of malware based upon some static definition of an attack, such as a signature, hash, domain, determined list of software behaviors, etc. These systems have obvious operational benefits, but also some serious shortcomings that must be addressed to achieve acceptable operational efficiency.

First, since the overwhelming majority of malware that is seen (in email, at the perimeter, et al) does not actually “detonate” on a vulnerable host, it is not operationally relevant to the security practitioner. This enormous false positive problem creates “analysis paralysis” for the average security team and consumes cycle for triage and research.

Second, since these systems inherently can only detect “known” malware, they are unable to detect new attacks, new malware variants, and the infamous “zero day” attacks. Given the growing volume of malware variants targeting individual organizations, this is an enormous security loophole exposing significant “false negative” risks.

Last, since these systems are built to identify malware (hashes, signature, et al) and its manifestations (file activity, C&C domains, et al), they are fundamentally incapable of detecting attacks that don’t employ malware, like insider attacks, credential attacks, or those stages of external attacks that don’t employ malware. This an enormous blind spot for security teams.

In order to realize “operational efficiency in security operations” that is meaningful and measurable, we as an industry must deliver tools that overcome these serious shortcomings. We need to focus on the two operational metrics that are most important to security operators: *efficiency* (volume of alerts) and *accuracy* (usefulness of alerts). We need systems that can solve the false negative and positive problems, and eliminate the blind spot around credential-based attacks. We need new systems that employ machine learning to complement the “known bad” models with new “learned good” models that aren’t susceptible to the same alert accuracy and efficiency problems. Security vendors must step up and take responsibility for delivering products that demonstrate operational success, and publish operational metrics that substantiate those claims. The industry can no longer afford to hide behind marketing fluff and hyperbolic claims. As one CISO recently put it, “We need tools that can slap us across the face and tell us what’s going on. We don’t have time to go looking for security events.”

About the Author

David Thompson, Senior Director of Product Management, LightCyber

David Thompson serves as the Senior Director of Product Management for LightCyber, responsible for assessing customer and market requirements, conducting sales and channel training and enablement, market education, and overall solution definition. He has been with LightCyber since late 2014.

Mr. Thompson has over 15 years of experience focused on information security. Prior to joining LightCyber, he served in Product Management leadership positions for OpenDNS, iPass, Websense, and Voltage Security (now HP). Prior to running product management at Voltage Security, Mr. Thompson was a Program Director at Meta Group (now Gartner) responsible for security research topics including encryption, PKI, remote access, and secure network design. Mr. Thompson holds a bachelors of science in Physics from Yale University.

IMPROVING QUALITY AND SECURITY WITH BINARY ANALYSIS

by Bill Graham, Technical Marketing Consultant, GrammaTech

Introduction:

Companies serious about quality, safety, and security need to manage the risks in their supply chain, including software such as commercial of the shelf (COTS) and free and open source software (FOSS).

In addition, existing and legacy code may have undetected vulnerabilities. Static analysis, especially analysis of binary files, provides an easy-to-adopt and efficient approach to improving the quality and security of the reused and third-party software.

Beyond Static Source Analysis

CodeSonar's binary analysis technology can evaluate object and library files for quality and security vulnerabilities. Although the possibility of investigating and fixing the issues is often limited, it does provide a bellwether of the quality and security of the code.

Customers of COTS products can go back to technical support of the vendor and ask for confirmation and analysis of the discovered vulnerabilities.

Binary analysis really shines when used in a hybrid fashion with source analysis. Source code analysis can use more information about the intent and design of the software than binary analysis. But whenever an external library is called, including standard C/C++ libraries, source code analysis can't tell if the use of the function is correct or not (assumptions are made, of course, for well known functions like strcpy()).

By combining source and binary analysis, a more complete analysis is possible. For example, if an external function takes a pointer to a buffer and a buffer overflow is possible with misused parameters, hybrid static analysis can detect this problem.

Information Flow and Tainted Data Analysis

Static analysis (binary and source-based) can track data flow through an application from source to sink (where it is finally used). Tainted data, that which is unchecked or unfiltered, can create unwanted behavior and purposely disrupt a system.

Inducing buffer overflows, for example, by entering large strings as user input can be a safety and security hazard, if unchecked.

Binary analysis furthers this capability by continuing the data flow trace into binary code, where such analysis is impossible with source-only analysis.

Tool Chain Errors and Backdoors

Binary analysis augments static source code analysis by detecting tool-chain induced errors and vulnerabilities. Backdoors have been placed in C/C++ compilers in the past and remain virtually undetected for years.

Binary analysis allows developers to evaluate the results of source-based and binary results to make sure quality and security issues are not introduced by the tool chain.

Multiplatform Support

Binary analysis is hardware CPU architecture-dependent, as one would guess, given the nature of binary code. GrammaTech CodeSonar's Binary Analysis supports both the x86 and ARM platforms, which cover a large majority of embedded, mobile and embedded devices in the marketplace.

Conclusion:

It's critical that potential vulnerabilities, quality and safety defects are detected and accounted for before code is used in a final product. Proper supply-chain risk management requires due diligence for reusing code, whether that's in-house, free or open-source, or from commercial vendors.

Binary analysis provides an important tool for evaluating quality, security, and safety before it becomes part of your product.

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 @Bill_Graham and at http://iot.williamgraham.ca.

North Africa Banking Technology 2016 Exhibition

8-9 NOVEMBER 2016
CAIRO INTERNATIONAL
CONVENTION CENTRE

CUTTING EDGE BANKING TECHNOLOGY

50+ PROMINENT MENA BANKERS SHARE THEIR EXPERIENCE AND PERSPECTIVES!

SPEAKERS INCLUDE:

J.P.MORGAN CHASE
Ahmed Afifi
Egypt & North Africa Head -
Global Trade & Loan Products

ABU DHABI ISLAMIC BANK
Amr El Zomor
Head Of AML Compliance &
Corporate Governance

ABANK
Ahmet Ertan Algan
Unit Head: Digital Banking
and Card Payment Systems

COMMERCIAL INTERNATIONAL BANK, EGYPT
Mohamed El Sabban
Group Head, Digital Banking,
Consumer Banking Group

SECURE YOUR COMPLIMENTARY PASS NOW

WWW.NORTHAFRICABANKING.COM

Sponsors:
Infosys® Finacle
wacom BUSINESS SOLUTIONS
Profile Software
Login

Media Partner:
CDM CYBER DEFENSE MAGAZINE

For more information contact:
Kaleesha Rajamantri
+44 207 111 1615
kaleeshar@irn-international.com

Organised by:
irn International Research Networks

Privacy Babel: Making Sense of Global Privacy Regulations

In the world of data privacy, the European Union General Data Protection Regulation has grabbed all the headlines. As much of a landmark piece of legislation the EU GDPR is for any company or organization that stores or processes EU citizen data, it's by no means the only one that global organizations must now navigate.

US regulators such as the FCC and FTC are stepping up their game to regulate digital identity, while in Canada, Australia and Singapore as well as Russia, privacy requirements are tightening up—and getting some teeth.

While in the US, federal agencies like the FTC, FCC and even even sectoral regulatory bodies like the SEC, CFPB, FINRA have become more vigilant around privacy enforcement, individual states are also becoming more proactive in around privacy and consumer data protection.

The latest example is the expansion of the Florida breach notification requirements under FIPA (**The Florida Information Protection Act)** which now mandates that the state Attorney General is notified in the event of a breaches, and that covered organizations consult with local law enforcement.

Globally, **some 65 countries** have either passed new privacy legislation in the last year or have legislation pending—including China and Brazil. The impetus for the growing emphasis on data privacy and protection is more widespread consumer unease about the impact of digital business on the privacy of their data—compounded by ongoing breaches to extract personal data.

Regulators and legislators across the globe are intensifying efforts to spell out requirements for collecting, storing, processing and sharing consumer and customer data.

The Cost of Negligence

Regardless of the jurisdiction or the point of departure for regulators, the point of commonality is that organizations must demonstrate responsibility and transparency in the storage, processing and transfer of private data, and operate on the basis that are now custodians of personal and private data.

Along with clear statements of intent for data collection and consent from consumers and customers, organizations must provide a privacy policy.

The specifics of the legislation—whether in terms of consumer rights such as the "right to be forgotten", data retention requirements or the need for data privacy officers—may vary widely by jurisdiction, along with the ability to actually enforce the legislation or regulations and impose penalties.

Although the severity of fines and penalties varies from country to country, what is common is that penalties have grown in size and regulators have become more comfortable using them.

In this context, the EU GDPR heralds the most significant change for data privacy in the digital era, but not only because of the technical requirements or even the stipulation for data protection officers under certain circumstances.

Instead, it's the magnitude of the penalties for violations, and the expressed willingness of regulators to impose the fine when the rules come into force of up to 4% of the total worldwide annual turnover of the preceding financial year.

In tandem with more explicit requirements on their responsibility across jurisdictions, organizations must also conform with the expanding definition of what constitutes personal data—whether biometric data in the case of the EU GDPR or MAC addresses or cookie IDs in the case of new privacy regulations proposed by the FCC in the US.

In its recent enforcement decisions, the Singapore's Personal Data Protection Commission has argued that context matters: violations of personal data protection requirements when the data is "of a sensitive financial nature" is more likely to draw fines.

For companies looking to comply with new privacy regulations it will therefore be increasingly expected that they can find any personal data accurately and at scale.

It's A Matter of Shared Principles

Certainly, many regulations and requirements will more closely resemble the GDPR's provisions as they near approval and the governing principles will become a point of comparison.

However, it is important to understand that differences in approach will persist.

For instance, the EU GDPR takes a comprehensive stance, especially when compared with the US, where much more of a sectoral focus led by industry regulators is in play.

A clear example of this is the current battle being played out between FCC and FTC on who gets to define digital privacy.

Also, while the US does not currently have federal general privacy protection legislation in place that applies broadly to the private sector andcorporations[1] , many states have implemented consumer privacy protection laws, including California, Massachusetts and Florida.

The New York state legislature currently has a bill in committee for an Online Privacy Protection and Internet Safety Act, which includes a provision for a data breach group that would include the state attorney general, state officials and CIO and the Homeland Security commissioner.

In Australia, regulators and legislators have worked with enterprises to define self-regulatory frameworks and standards in order to ensure responsible protection of consumer privacy. The outcome is that guiding federal privacy principles are more focused on practical implications for the implementation of privacy policies and protections.

By contrast, Canada's PIPEDA (Personal Information Protection and Electronic Documents Act) emphasizes operating principles and hews more closely to the EU's comprehensive approach to the citizen's right to privacy.

the Privacy Act applies to federal agencies: stablishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

About the Author

Dimitri Sirota is a 10+ year privacy expert and identity veteran. He is currently the CEO & Co-founder of the first enterprise privacy management platform, BigID –and wears many hats as an established serial entrepreneur, investor, mentor and strategist.

He previously founded two enterprises software companies focused on security (eTunnels) and API management (Layer 7 Technologies), which was sold to CA Technologies in 2013.

No One Likes Passwords, So Why Are We Still Using Them?

Users Deserve Better, Websites Need to Deliver

By Charles Durkin, Chief Executive Officer, Privakey

Creating a new online account is a dreaded task for most internet users. Complexity and security concerns increase user anxiety with each new username and password combination. Despite tremendous advances in technology, the problem with online identity and authentication has been getting worse.

The internet's original design did not include an identity layer, forcing all online businesses to build their own homebrew service for identifying and authenticating users. The resulting proliferation of inconsistent and insecure usernames, passwords and "security" questions is now a bane for users worldwide.

Despite the complexity of creating and managing dozens of passwords, they remain highly insecure. Michael Chertoff, former Secretary of the Department of Homeland Security, stated recently that "passwords are the weakest link in cybersecurity today". Most experts agree with his assessment.

The password's primary security flaw lies at the core of the "shared secret" approach to authentication. As soon as a user successfully selects a password, regardless of its length and strength, it is stored along with other user account information. The databases of online service providers such as Yahoo, LinkedIn, and Twitter contain hundreds of millions of user login credentials.

Databases of stored passwords are a highly desirable target for hackers, because most users reuse the same password at many sites, including online banks and other financial institutions.

Cybersecurity experts frequently offer guidance on cyber hygiene. Their recommendations include the use of long, complicated passwords and frequent changes to them. Really?

Which users are actually going to follow such advice? The answer is very few — and those that do get help from a robotic password manager.

Password managers add another layer of complexity to the password problem and they do not eliminate the stored passwords from website databases.

Passwords have been around since the dawn of the computer age. It seems quaint now, but not long ago (last year?) many people were still using the name of their child or their pet as their password for most sites.

Most online service providers now have policies that require stronger passwords. They also caution users against password reuse.

While well intentioned, these policies are making users' lives more difficult and adding only limited improvements in cybersecurity. Poor user experiences are bad for any business and particularly harmful for online businesses.

Ideally, the login experience would be the same for every website, application or service accessed by the user. The experience would also be highly secure, and it would eliminate stored passwords. Standards organizations have developed digital identity specifications that meet these criteria, and real solutions are available.

Cloud based identity providers enable online service providers the opportunity to improve their users' experience, while eliminating the vulnerability of stored passwords. Yes, this means no more passwords! Eventually.

Over the next several years, professional identity service providers will begin to supplant the millions of home grown identity and authentication solutions that now dominate the web. These professional service providers will fill in the missing identity layer where it is needed.

The result will be the end of passwords and the beginning of consistent, convenient and secure login experiences across the internet.

About The Author

Charles Durkin is the Co-Founder, President, and Chief Executive Officer of Privakey, Inc. He co-founded the company in 2015, and is responsible for Privakey's strategy, communications, and execution.

Charlie has served in the same capacity for 8 years at Privakey's parent company, Probaris Technologies. Prior to joining Probaris, Charlie led a large Ecommerce and Business Intelligence consulting business at General Electric.

Charlie can be reached at cdurkin@privakey.com, @CharlesJDurkin, or at the Privakey website: www.privakey.com.

Next month: How does a password-free identity service work?

Latin CIO Summit

November 17-18, 2016, Trump Ocean Club, Panama City, Panama

Industry leaders from around the globe are confirming their places on the line-up for the Latin Chief Information Officer Summit. Join them in a two day event offering Latin America's leading decision makers of the industry a devoted environment for **unparalleled business and networking opportunities in a stimulating environment.**

Grow your business & sales in just 2 days
Network with high level executives during formal and informal time such as cocktails and dinner hours!
Target qualified buyers through our pre-scheduled one-on-one meetings format

EXPERT SPEAKERS ALREADY CONFIRMED ON THE LINE-UP INCLUDE

- EVP & Chief Information Officer, **Costco Wholesale Corporation**
- Chief Information Officer, **Xerox Corporation**
- Global Product Security & Services Officer, **Philips Healthcare**
- Chief Information Officer, **Georgia-Pacific LLC**
- VP, Global Technology Services, **U.S. Bank**
- Senior Vice President, Head of North America, **Syntel, Inc.**
- Chief Technology Officer – Americas, **HCL Technologies**

SOME TOPICS TO BE DISCUSSED ARE:

- The Role of the CIO
- Data Security
- Mobility and Network Connectivity
- Trends and Uses of The Cloud
- Big Data
- IT Working Together with Sales and Marketing
- Adapting to the Fast Forward Digital World
- Investing in Talent
- The future of Technology in Latin America

For more information please contact **alejandrad@marcusevansmx.com** or visit
http://events.marcusevans-events.com/latinciocdm

marcusevans®

Top 10 Data Security Issues in Large Enterprises

by Alex Hooper, CTO, Cisilion

Data breaches and other cyber security issues have made the headlines in recent years and enterprises must take precautions, because such problems can be incredibly costly. Indeed, a recent report from IBM estimated the average cost of an enterprise data breach to be in the region of $3.5 million.

Of course, in addition to the pure financial cost, issues with security can undermine public confidence and have long-term consequences. Here, we look at the top 10 data security issues that impact large enterprises.

1. Personal Mobile Usage

Research from BT shows that 68 percent of organisations have experienced a mobile security breach in the past year and smartphones present a particular risk, as users demand access to company networks, while simultaneously expecting privacy and freedom to use their devices as they like. Downloaded apps could be infected with Malware, offering a threat to network security, while misplaced or stolen devices could allow sensitive data to leak.

2. File-Sharing

Modern file-sharing technology is essential for many enterprises, but it presents its own risks. Apps like Google Drive and Dropbox present the very real possibility of data being shared beyond those who are authorised to access it. For instance, 33 percent of all employees admit to uploading sensitive data to a cloud-based storage system, according to Skyhigh Networks, while Hubspot report that 23 percent of documents are shared publicly; possibly by accident. The recent hacking of Dropbox involving over 68 million personal records has certainly acted as a wake up call for any businesses that are aware of their staff sharing some data on public cloud sharing sites.

3. Third Party Providers

An overlooked threat is connected to third party providers, who are often given remote access to the networks of large businesses. However, many third parties use the same login credentials to access multiple different clients. If those credentials are compromised, the hacker potentially has instant access to all of those clients' data.

4. Unpatched Software

It is interesting to note that many security breaches are completely preventable, because they exploit old vulnerabilities, which could be fixed with patches. In fact, the 2015 HP Cyber Risk Report revealed that 44 percent of all breaches came from vulnerabilities that are between two and four years old.

5. Unpatchable Software

Similarly, many enterprises do not have their finger on the pulse when it comes to unpatchable software. As an example, Microsoft ended support for Windows Server 2003 and Windows XP over a year ago, meaning there will be no further updates, even if security risks are found. Despite this, Forrester estimate there are still more than 10 million active users.

6. Phishing Emails

Although most enterprises issue warnings, phishing emails remain a threat. It is believed that 156 million phishing emails are sent every day, with 16 million making it past spam filters. Of these, 50 percent are opened and 10 percent of people who open a phishing email subsequently click on a link, according to Cyveillance. That means that 80,000 people still fall for phishing scams every single day and it could happen in your workplace.

7. Data Destruction

The destruction of sensitive data is essential for security purposes, yet it continues to represent a key threat for large enterprises. In fact, a report from Blue Coat found that data destruction was the second most serious 'shadow data' security threat around, accounting for 17 percent of the total risk.

8. Employees With a Vendetta

It may seem like a strange idea, but your own staff are one of the biggest possible threats to data security. Internal attacks from embittered staff or disgruntled former employees can do a lot of damage, especially if the staff member has intimate knowledge of your network. For this reason, privileged accounts should be restricted and should be terminated as soon as somebody leaves the organisation.

9. Wearable Devices

The rise of wearable technology like smart watches has added to the number of devices that IT departments need to be aware of. Most of these devices carry similar security risks to mobile phones, but they are also more discreet. As a result, staff may be able to access them in places where mobiles are restricted or banned.

10. A Lack of Planning

Finally, it can be argued that within big businesses, data breaches or security threats are inevitable. Assuming we are to accept this viewpoint, one of the single biggest issues is a lack of forethought. Enterprises can help to limit the damage by planning their response in detail, pinpointing exactly who would be involved and why. This response should then be tested to make sure it is robust enough.

Security Solutions

One of the most effective ways to protect your business is to invest in high-quality end user awareness training. Research shows that ill-prepared end users are the single biggest security vulnerability in any company, so equipping them with cyber security knowledge can help to prevent many of these problems from occurring.

Moreover, it is important to create a comprehensive security strategy, which should include the monitoring of any activity on company networks, and which should ensure that any sensitive data is kept secure. Knowing what is going on across your entire network is the best way to spot problems and take swift action.

All employees should be aware of the security strategy itself and how to comply with it. Meanwhile, as part of your strategy, you should also have a robust plan for dealing with any issues that do arise. Anyone involved in a planned response should be prepared and know exactly what to do in the event of a threat or breach.

Finally, it is essential that your business stays on top of the constantly evolving world of mobile. BYOD policies can work extremely well, as long as businesses are vigilant and remain up-to-date with the latest technology, including wearable devices that may connect to work networks, such as smart watches.

About The Author

Alex Hooper is the CTO of Cisilion. He joined Cisilion in 2014, after previously running the global presales team at nscglobal. He brings over 15 years of experience of working for system integrators and service providers. His primary focus at Cisilion is developing a full breadth of networking and IT services to our customers and has a passion for creating value for our customers. Alex can be reached online at Twitter and at our company website http://www.cisilion.com/

Three Key Business Lessons From The Founder of a Big Data Security Company

By MacLane Wilkison, Co-Founder of ZeroDB

When startups mix with corporations we see an oil-and-water effect. There's often a gap in work practices, organizational structure and managerial outlook, not to mention the fundamental differences regarding the appetite for risk and experimentation.

For companies selling to financial services, however, it's even tougher. While startups are enthusiastic and nimble, established financial institutions are understandably conservative by nature. Large organizations have correspondingly large responsibilities—to their employees, management, stakeholders, customers, and regulators. It takes time for them to evaluate and sign off on the services that startups hope to supply—especially when it comes to matters of data security.

As such, it's crucial that startups selling to financial institutions are prepared for this reality from day one. Here are three lessons I've learned founding a big data security startup and selling to large enterprises.

1. Expect delays, talk to customers, and be transparent

Focusing on that one "killer" deal is probably a big mistake. Large contracts need approval from multiple departments in the same organization—and that means undergoing security reviews, talking to legal, negotiating with procurement, and securing a sponsor from the relevant business unit, all of which have the potential to turn you down.

Enterprises tend to take their time when it comes to making decisions; startups should be prepared for long sales cycles that can range from three to 18 months. To appropriate John Maynard Keynes' famous quote; the enterprise can stay undecided longer than you can stay solvent.

So what can you do to hasten the process and ensure success?

When you are establishing yourself in any market, it is extremely important to nail your problem statement and value proposition. The way to do that is by spending lots and lots of time talking to your customers. If you think you're talking to a lot of them, times that amount by ten, and you're getting close.

Make sure that you speak to your customers as early and as often as you can. This will help build the deep understanding you need to have of the problem you are trying to solve and will increase the likelihood of your value proposition being accepted and the contract signed. The last thing you want is to spend six months in endless meetings that end up going nowhere.

Be sure that potential clients are made fully aware of the Return On Investment (ROI) that they can expect. That means quantifying your value proposition and nailing the pitch. Speaking in economic terms can increase the business unit's urgency and help speed up the process.

2. Look beyond the established corporate market to other startups

If you run a great service, you can be sure that you will attract a huge client and your big, vindicating pay day will come. However, as I've explained above, selling to well established companies and multinationals is a slow and complex process.

In light of this, managing your cash flow requires a delicate touch and needs to be supported by other opportunities.

Don't get tunnel vision. Large banks and enterprises are far from the only clients available to data security providers.

Financial Technology—also known as *FinTech*—is booming on a global scale; bank spending on new technologies in North America is projected to reach 19.9 billion by 2017. The startups and businesses pioneering this sector also need protection from potential data breaches and attacks on sensitive information.

It makes sense to target smaller businesses in parallel with working through the enterprise sales cycle. Not only can these businesses make decisions far more quickly than huge institutions, but they will be more sympathetic to the startup reality. Supporting other startups will allow your business to get earlier traction with smaller customers and contracts.

3. Be in the right market at the right time

It's a great time to be in the business of data security. The volume of global data is growing exponentially. By 2020, "about 1.7 megabytes of new information will be created every second for every human being on the planet," according to a study cited by Forbes.

As a result, companies are increasingly dumping all their data in vast "data lakes." While a practical solution to data growth, these repositories present a great temptation for hackers that seek to steal sensitive information.

With many high profile hacking cases and data breaches in the media, responsible corporations--especially those which carry highly sensitive client information--are getting serious about tackling the problem.

Luckily, most of the banks and financial institutions we talk to have a good understanding of the risks they face. While this puts us in a good position, simply explaining the benefits of stronger measures for data protection won't cut it. You need to clearly explain how your product is different, why *now* is the right time to implement a solid security solution, and why you are the best choice given the plethora of other vendors vying for their business.

So how should you pitch your solution?

It's all about timing. Data security is not just about the here and now; it's about being one step ahead of the game. Large institutions have the potential to sign lucrative contracts that last for many years, so you must be able to have the flexibility and foresight to provide a clear solution for today's challenges, as well as to outline your plan for tomorrow's threats.

Final words

Be patient and flexible, make sure you have a strong understanding of the problem you're solving and the reality of enterprise sales cycles.

On top of that, make sure you're spending your time and effort in a growing market. In startups, a rising tide doesn't necessarily lift all boats, but it does lift the ones that are solving the right problem, at the right time, with the right solution. Our journey at ZeroDB has led us to discover that the sheer scale of Big Data - the volume, the threats to its security and those who would try to steal it - is more enormous than we could have ever imagined. It will take a global effort from startups and innovators all over the world to ensure that sensitive data is kept safe from theft, leaks and breaches.

About the Author

MacLane Wilkison is the co-founder and CEO of ZeroDB, a Y Combinator-backed startup that provides enterprise security and encryption for big data in the cloud.

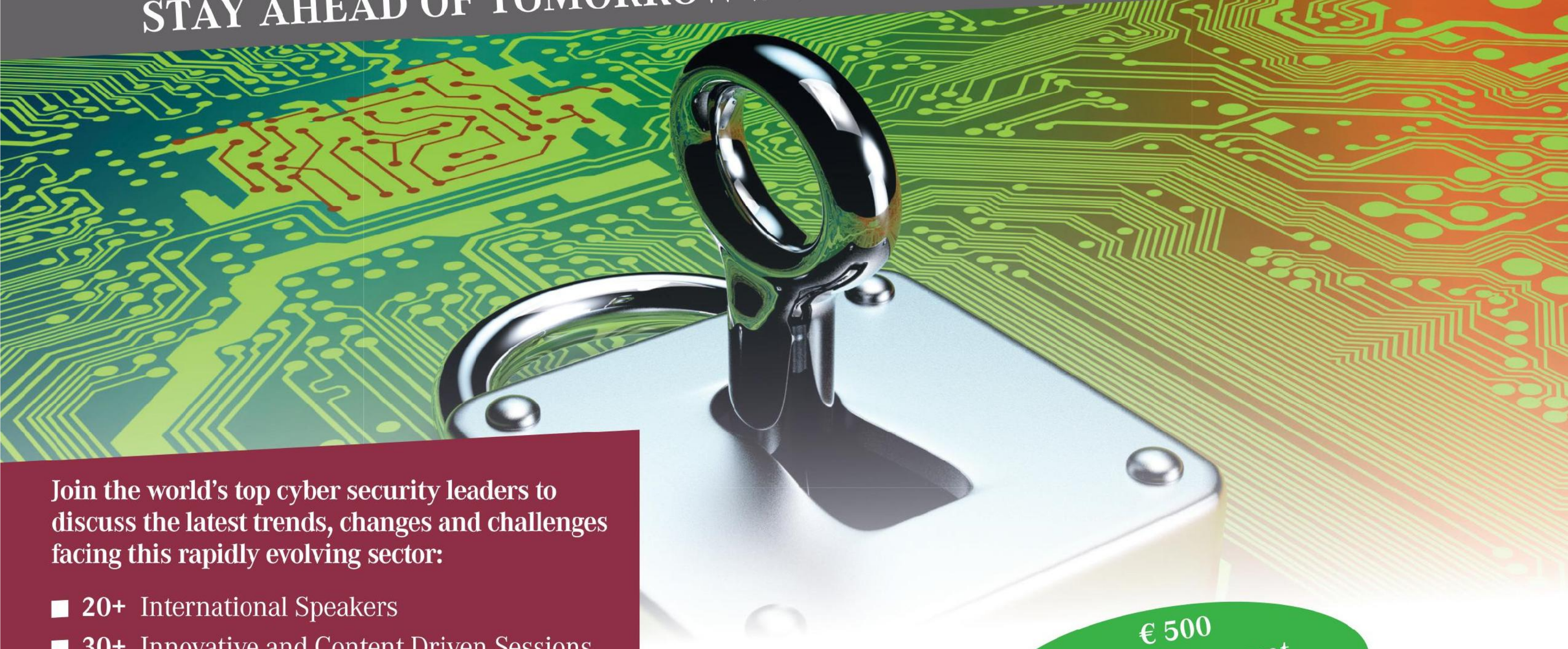
2nd ANNUAL SUMMIT

■ GLOBAL CYBER SECURITY LEADERS

EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

7th – 8th NOVEMBER, 2016| STEIGENBERGER AM KANZLERAMT | BERLIN

STAY AHEAD OF TOMORROW'S CYBERSECURITY CHALLENGES!



Join the world's top cyber security leaders to discuss the latest trends, changes and challenges facing this rapidly evolving sector:

- **20+** International Speakers
- **30+** Innovative and Content Driven Sessions
- **30+** Hours of Exclusive Networking

€ 500
Special Discount
with code GCSL4CDM

Speakers include:

Alexander Oesterle
Global VP Governance, Risk & Compliance and CSO,
SAP, Germany

Daniel Selman
Cyber Industry Deputy Head,
UK Ministry of Defence, United Kingdom

Stephan Gerhager
CISO,
Allianz Deutschland AG, Germany

Scott Stewart
Vice President of Tactical Analysis,
Stratfor, USA

Taiye Lambo
CISO,
City of Atlanta, USA

Volker Kozok
Assistant Branch Chief German MoD,
Bundeswehr, Germany

Kim B. Larsen
CSO,
Huawei Technologies, Denmark

Arieh Shalem
CISO,
Orange Telecommunication, Israel

Premium Partner
Warth & Klein Grant Thornton
An instinct for growth™

Promoters
EY Building a better working world
ThreatBook

Hosted by
MANAGEMENT CIRCLE®

Official Part of
Global Leaders Summit Series
EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

www.cybersecurity-leaders.com

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?

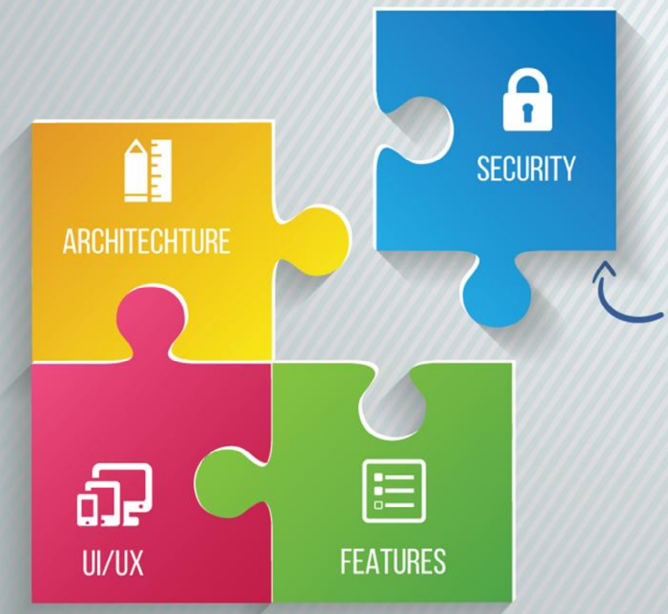
Your Enrollment includes :

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

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-intrusive 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

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

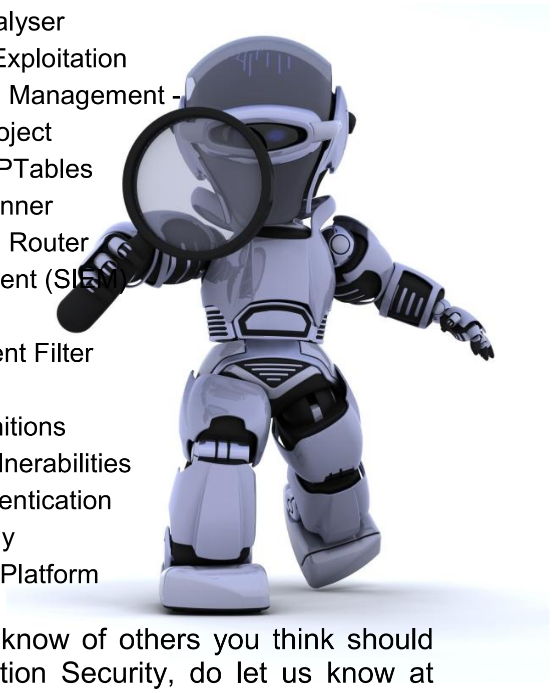
Top Twenty INFOSEC Open Sources

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)

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.

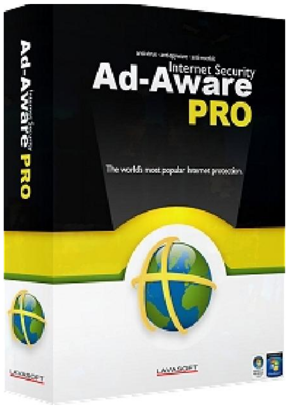
Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting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

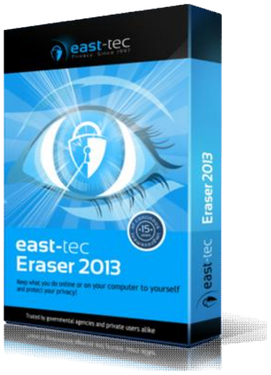
Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

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

SOURCES: CDM and NAISG.ORG

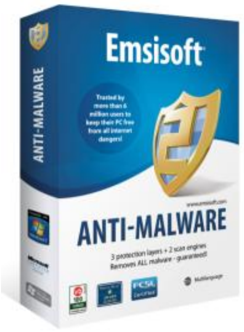




SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

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.



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.

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine October 2016

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/

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

RSA CONFERENCE
StillSecure
PORTCULLIS
Hawk Mobile Monitor
Monitor Mobile Devices Remotely From Your Computer
AFORE SECURE THE CLOUD. TRUST THE CLOUD.
NETCLARITY
solarwinds
Center for Internet Security
Software Developer's Journal
RSA CONFERENCE ASIA PACIFIC 2013 JUNE 5-6 | SINGAPORE
SWIVEL the power of knowing
CYBER SECURITY SUMMIT 2013
SnoopWall RECLAIM YOUR PRIVACY
KASPERSKY lab
dekart MAKE IT SECURE
INFOSEC WORLD
PWNIE EXPRESS
EncrypTight™ BLACK BOX WAN Encryption
GO ANYWHERE™
BLUESPACE

Email: marketing@cyberdefensemagazine.com for more information.

Cyber Warnings Newsflash for October 2016

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…

The most common malware, country by country

http://www.zdnet.com/article/the-most-common-cyberattacks-country-by-country/

Microsoft: Beware this fake Windows BSOD from tech support scammers' malware

http://www.zdnet.com/article/microsoft-beware-this-fake-windows-bsod-from-tech-support-scammers-malware/

CloudFanta Malware Targets Victims Via Cloud Storage App

http://www.darkreading.com/cloud/cloudfanta-malware-targets-victims-via-cloud-storage-app/d/d-id/1327289

Mirai malware simplifies internet attacks like last week's

https://www.japantoday.com/category/technology/view/mirai-malware-simplifies-internet-attacks-like-last-weeks

Cyber attack: hackers 'weaponised' everyday devices with malware to mount assault

https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault

This ransomware is now one of the three most common malware threats

http://www.zdnet.com/article/this-ransomware-is-now-one-of-the-three-most-common-malware-threats/

UC Santa Barbara Prof Lands Malware Award from Google

https://campustechnology.com/articles/2016/10/24/uc-santa-barbara-prof-lands-malware-award-from-google.aspx

XiongMai Technologies Admits Their Devices Are Susceptible To Mirai Malware

http://themerkle.com/xiongmai-technologies-admits-their-devices-are-susceptible-to-mirai-malware/

CIA Election AntiCheat Control malware preys on the fear of Voter Fraud

http://www.bleepingcomputer.com/news/security/cia-election-anticheat-control-malware-preys-on-the-fear-of-voter-fraud/

Nearly 6,000 online sellers are hit by malware that steals credit card numbers

https://www.internetretailer.com/2016/10/20/online-sellers-hit-malware-steals-credit-card-numbers

Discord VoIP Chat Servers To Host Malware

http://www.informationsecuritybuzz.com/hacker-news/discord-voip-chat-servers-host-malware/

AppRiver Releases Q3 Global Security Report: Malware Traffic Expanded For the Fourth Straight Quarter

https://globenewswire.com/news-release/2016/10/24/882121/10165747/en/AppRiver-Releases-Q3-Global-Security-Report-Malware-Traffic-Expanded-For-the-Fourth-Straight-Quarter.html

Ransomware Reaches the Malware Top 3 for the First Time

http://news.softpedia.com/news/ransomware-reaches-the-malware-top-3-for-the-first-time-509552.shtml

Malware lurks in many corners of ‘the cloud’

http://www.futurity.org/malware-cloud-hosting-1276682-2/

Android Malware: Ghost Push Trojan Still Threatens More Than Half Of Android Devices

http://www.techtimes.com/articles/182579/20161017/android-malware-how-ghost-push-trojan-still-threatens-more-than-half-of-android-devices.htm

Intel Haswell chips open to malware flaw

http://www.itpro.co.uk/security/27450/intel-haswell-chips-open-to-malware-flaw

Republican donor site malware skimmed credit cards for six months

http://www.zdnet.com/article/hackers-skimmed-credit-cards-from-republican-donor-site-for-six-months/

Why anti-malware protection isn't a 'thing' you can buy [Q&A]

http://betanews.com/2016/10/20/why-anti-malware-protection-isnt-a-thing-you-can-buy-qa/

Malware Authors Adopting the Freemium Model Spells Bad News for the Rest of Us

http://news.softpedia.com/news/malware-authors-adopting-the-freemium-model-spells-bad-news-for-the-rest-of-us-509546.shtml

Spotify blames malware attack on a single ad

https://www.cnet.com/news/spotify-users-hit-with-malware-attack/

Massive cyber-attack caused by hackers using smartphones, webcams

http://www.jerusalemonline.com/news/world-news/around-the-globe/massive-cyber-attack-caused-by-malware-that-affected-smartphones-24342

Internet of Things Malware Has Apparently Reached Almost All Countries on Earth

http://motherboard.vice.com/read/internet-of-things-mirai-malware-reached-almost-all-countries-on-earth

CDM

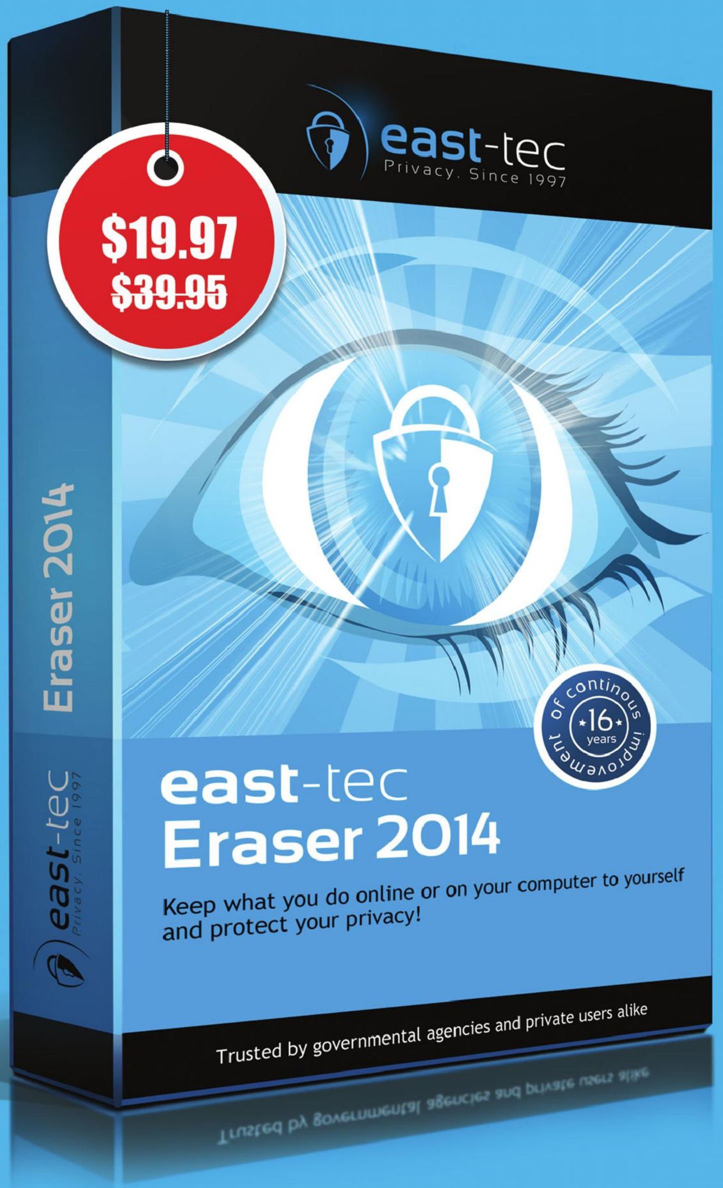
CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

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: 10/26/2016


$19.97
~~$39.95~~
east-tec
Privacy. Since 1997
Eraser 2014
of continous 16 years improvement
east-tec
Eraser 2014
Keep what you do online or on your computer to yourself and protect your privacy!
Trusted by governmental agencies and private users alike