

## 10 PRACTICAL SECURITY TIPS FOR DEVOPS

**AVOIDING AN IT DISASTER:  
SMART SECURITY FOR SMART METERS**

**THE STANDARDIZATION OF TOKENIZATION  
AND MOVING BEYOND PCI**



**THE ART OF WAR APPLIED TO  
WEB APPLICATION SECURITY**

# THE NEXT GENERATION CLOUD SECURITY PLATFORM



Bringing Continuous Security to the Global Enterprise

Get a free trial at [qualys.com/trial](http://qualys.com/trial)

# TABLE OF CONTENTS

Page 05 - **Security world**

Page 11 - The Art of War applied to web application security

Page 16 - Signature antivirus' dirty little secret

Page 20 - Review: Tresorit for Business

Page 26 - Making IoT security a reality

Page 30 - **Malware world**

Page 33 - Report: Hack In The Box

Page 42 - Avoiding an IT disaster: Smart security for smart meters

Page 45 - The standardization of tokenization and moving beyond PCI

Page 49 - 10 practical security tips for DevOps

Page 53 - Identifying the insider threat

Page 55 - **Events around the world**

Page 56 - EMV's impact on increasing card-not-present fraud: Now what?

Page 59 - Identity crisis? Honoring the IAM legacy while taking action and embracing the future

Page 68 - Report: Infosecurity Europe 2015

Page 74 - IoT, interoperability, and identity



- **Christiaan Brand**, co-founder and CTO of Entersekt
- **Martin Bergenwall**, Executive VP of the Mobile Security Business Division at INSIDE Secure
- **James Brown**, Director, Cloud Solutions Architecture at Alert Logic
- **Steph Charbonneau**, CTO at TITUS
- **Rob P. Faber**, Enterprise Security Architect and Consultant
- **Neeraj Khandelwal**, Senior Product Manager, Engineering at Barracuda
- **Paul Madsen**, Senior Technical Architect within the Office of the CTO at Ping Identity
- **Ulf Mattsson**, CTO at Protegrity
- **Richard Moulds**, VP Strategy at Thales e-Security
- **Corey Nachreiner**, Director of Security Strategy and Research at WatchGuard.

**Visit the magazine website at [www.insecuremag.com](http://www.insecuremag.com)**

### **(IN)SECURE Magazine contacts**

Feedback and contributions: **Mirko Zorz**, Editor in Chief - [mzorz@net-security.org](mailto:mzorz@net-security.org)

News: **Zeljka Zorz**, Managing Editor - [zzorz@net-security.org](mailto:zzorz@net-security.org)

Marketing: **Berislav Kucan**, Director of Operations - [bkucan@net-security.org](mailto:bkucan@net-security.org)

### **Distribution**

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.



## Let's Encrypt CA to issue its first cert

Let's Encrypt, a non-profit certificate authority (CA) set up by the Electronic Frontier Foundation, Mozilla, Cisco, Akamai, IdenTrust, and researchers at the University of Michigan, is finally ready to issue its first certificate, scheduled the week of July 27, 2015.



"We will issue the first end entity certificates under our root under tightly controlled circumstances. No cross-signature will be in place yet, so the certificates will not validate unless our root is installed in client software," explained Josh Aas, the Executive Director of the Internet Security Research Group, which runs the CA.

"As we approach general availability we will issue more and more certificates, but only for a pre-approved set of domains. This limited issuance period will give us time to further ensure that our systems are secure, compliant, and scalable."

General availability is scheduled for the third week of September, when certificate requests for any domain can be gotten. "A cross-signature from IdenTrust will be in place for general availability, so that our certificates will validate automatically for the vast majority of consumers," he added.

The CA's root and intermediate certificates have been generated earlier this June, and the security audit of its software and Automated Certificate Management Environment (ACME) protocol has obviously come to a satisfactory end.

Let's Encrypt's goal is to make the process of switching web servers from HTTP to HTTPS quick and easy.

## Shadow IT is prevalent in government agencies

Despite clear benefits of cloud services, federal agencies are slow to migrate to the cloud due to security concerns. As a result, employees adopt cloud services on their own, creating shadow IT. The average public sector organization uses 742 cloud services, which is about 10-20 times more than IT departments expect, say the results of a new Skyhigh Networks' report.

Despite the security initiatives in place – such as FedRAMP, FISMA, and FITARA – many government employees are unaware of agency rules and regulations or simply ignore them and use cloud services that drive collaboration and productivity. Under FITARA, Federal CIOs must oversee sanctioned cloud services as well as shadow IT. This new requirement underscores the uncertainty about how employees are using cloud services within their agencies. Agencies

cannot rely on the security controls offered by cloud providers alone. Analyzing more than 12,000 cloud services across more than 50 attributes of enterprise readiness developed with the Cloud Security Alliance, the report found that just 9.3 percent achieved the highest CloudTrust Rating of Enterprise Ready. Only 10 percent of cloud services encrypt data stored at rest, 15 percent support multi-factor authentication, and 6 percent have ISO 27001 certification.

Compromised credentials can also mean disaster for Federal agencies. According to a study from the University of Cambridge, 31 percent of passwords are used in multiple places. This means that for 31 percent of compromised credentials, attackers can potentially gain access not only to all the data in that cloud service, but all the data in other cloud services as well. The average public sector employee uses more than 16 cloud services, and 37 percent of users upload sensitive data to cloud file sharing services.

## Users care about their privacy, but feel powerless to protect it



Users are resigned to the loss of privacy, but not because they feel they are getting good value for their data, but because they believe marketers will eventually get it anyway, a new study by University of Pennsylvania researchers has shown. The results are in conflict with the claim that marketers have been repeating for years, which is that Americans give out information about themselves as a tradeoff for the benefits they receive.

"To the contrary, the survey reveals most Americans do not believe that 'data for discounts' is a square deal," the researchers noted. Another finding of the research is that the more users know about ways marketers can use their personal information, the more likely they are to agree to the exchange of data for discounts. In short, they are resigned, and believe it impossible to change things. "Rather than feeling able to make choices, Americans believe it is futile to manage what

companies can learn about them. Our study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened," the researchers noted.

"To further question marketers' emphasis on Americans' use of cost-benefit calculations, we found that large percentages of Americans often don't have the basic knowledge to make informed cost-benefit choices about ways marketers use their information," they added.

"The futility over information control we are seeing in the public sphere is disrupting a compact that commercial marketers made with Americans through the past century," they point out, and predict Americans might come to reject the legitimacy of marketing and consumer commerce, and the rise of social tensions. But the situation can be remedied, the researchers pointed out, and offered a few suggestions on how to go about it: corporate transparency, active dissection and reporting on the implications of privacy policies, and the ability to know the contents of our profile compiled by companies.

## What's driving security budgets and technology purchases?

IT security and IT leaders and their staff members do not agree on security objectives, according to findings from a new global Ponemon study. One of the key findings from the study was that more than 50 percent of the respondents surveyed stated that their organization's board of directors and C-Level executives are frequently not briefed, nor are they given the necessary information to make informed budgeting decisions regarding security priorities and the investments in technology and personnel required.

"It's remarkable that despite widespread attention many senior executives are not yet fully briefed on security priorities. This may be explained by the fact that so few are actually held accountable. While this perception exists, organizations will continue to experience incidents and the loss of trust from impacted customers," said Raj Samani, VP and CTO EMEA at Intel Security.

Another alarming finding was that 58 percent of the study's respondents said they did not think or were unsure if their organization possessed sufficient resources to achieve compliance with security standards and laws.

## Brain's reaction to certain words could replace passwords



You might not need to remember those complicated e-mail and bank account passwords for much longer. According to a new study, the way your brain responds to certain words could be used to replace passwords.

In Brainprint, a newly published study in academic journal Neurocomputing, researchers from Binghamton University observed the brain signals of 45 volunteers as they read a list of 75 acronyms, such as FBI and DVD. They recorded the brain's reaction to each group of letters, focusing on the part of the brain associated with reading and recognizing words, and found that participants' brains reacted differently to each acronym, enough that a computer system was able to identify each volunteer with 94 percent accuracy.

The results suggest that brainwaves could be used by security systems to verify a person's identity.

According to Sarah Laszlo, assistant professor of psychology and linguistics at

Binghamton University and co-author of "Brainprint," brain biometrics are appealing because they are cancellable and cannot be stolen by malicious means the way a finger or retina can.

"If someone's fingerprint is stolen, that person can't just grow a new finger to replace the compromised fingerprint — the fingerprint for that person is compromised forever. Fingerprints are 'non-cancellable.' Brainprints, on the other hand, are potentially cancellable. So, in the unlikely event that attackers were actually able to steal a brainprint from an authorized user, the authorized user could then 'reset' their brainprint," Laszlo said.

Zhanpeng Jin, assistant professor at Binghamton University's departments of Electrical and Computer Engineering, and Biomedical Engineering, doesn't see brainprint as the kind of system that would be mass-produced for low security applications (at least in the near future) but it could have important security applications.

"We tend to see the applications of this system as being more along the lines of high-security physical locations, like the Pentagon or Air Force Labs, where there aren't that many users that are authorized to enter, and those users don't need to constantly be authorizing the way that a consumer might need to authorize into their phone or computer," Jin said.

## Hackers can tamper with medical drug pumps, leading to fatal outcomes

Researcher Billy Rios has discovered serious vulnerabilities in several types of drug infusion pumps manufactured by US-based company Hospira - vulnerabilities that can be exploited remotely by attackers looking to take control of the medical devices, and to effect changes that could threaten patients' lives.

This is not the first time that Rios has discovered vulnerabilities in Hospira's pumps: in May 2014, he reported to the Department of Homeland Security and the FDA several vulnerabilities that made it possible for an attacker to change medication dosage limits on the company's PCA 3 Lifecare line of pumps.

The FDA eventually, a year later, released a security advisory about those first vulnerabilities, as they were also discovered by another researcher and their existence made public. In the year between the initial discovery and the publication of the advisory, Hospira has failed to patch the flaws.

In fact, when Rios first contacted them in 2014, they refused to test the other infusion pumps they sell for the vulnerabilities. This spurred Rios to continue with the research, and he purchased additional pumps to test them himself.

"What I found was very interesting, many of Hospira's infusion pumps utilize identical software on their infusion pumps' communications module, making them vulnerable to the exact same security issues associated with the PCA 3," he noted.

These vulnerabilities include the ability to forge drug library updates to the infusion pump, the existence of an unauthenticated telnet shell to root the communications module, the use of identical hardcoded credentials, private keys and encryption certificates across different device lines, and outdated software.

The newly discovered vulnerabilities would allow an attacker to remotely alter the devices' firmware, as they accept unsigned, unauthenticated updates. The connection to the device can be made via the devices' communication modules, which are connected to hospital networks.

## IT admin errors that lead to network downtime and data loss

Kroll Ontrack released its most recent list of common IT administrator errors that can lead to data loss and network downtime:

- Failure to document and execute established IT, retention and backup procedures
- Failure to backup effectively
- Delay in infrastructure or security investments
- Failure to adhere to and maintain relevant security policies and/or keep OS and security controls up to date
- Deleting data that is still in active use.

The company recommends IT departments follow these best practices in light of data loss, to ensure the best chance of an effective resolution:

- Avoid panicking and rushing to action. If data loss happens, companies should not restore data to the source volume from backup because this is where the data loss occurred in the first place.
- Be confident in skills and knowledge. IT staff must help leadership avoid making decisions that do more harm than good.
- Have a plan. Staff should follow established ITIL processes and ensure data centre documentation is complete and revisited often to ensure it is up to date.
- Know the environment (and the data). IT staff must understand what their storage environment can handle and how quickly it can recover.
- When in doubt, call a data recovery company. While the manufacturer or vendor may be a good starting point, the value of data and the potential for data loss when getting a system back up and running may not be top of mind.

## MEDIAN SALARY U.S., By Certification Status



### FEMALE

**NO** Certification \$110,000

**ANY** Certifications \$130,000



### MALE

**NO** Certification \$127,000

**ANY** Certifications \$131,000

### Privacy profession: An equal playing field for men and women?

In the midst of the public debate around the lingering gender gap in salary and professional achievement, the International Association of Privacy Professionals (IAPP) revealed that in the privacy and data governance fields, women are similarly compensated and reach similar career heights as men. In fact, the single most predictive indicator for salary and achievement is professional certification.

The survey, which looked at 1,253 privacy professionals around the world, found the privacy field to be evenly split 50-50 between male and female professionals. The salary figures also demonstrated an even split with female privacy professionals making nearly equal pay to men.

In the US, men in the privacy profession were paid a median annual salary of \$130,000, compared to women who were paid \$125,000. For privacy professionals in Europe, women were found to have a higher median salary than men, with men being paid a median annual salary of \$92,600, and women being paid \$100,100.

The slight pay gap between male and female privacy professionals in the US lessens for those professionals who obtain a certification. The survey showed among certified

professionals, men made a median salary of \$135,000 compared to \$132,500 for women.

In the US women and men were also found to have similar titles and positions in their firms. In fact, women are 33% more likely to have a seat in the C-suite than men. Women were almost identical to men in the likelihood of holding a VP- level position (slightly less likely), legal counsel-level position (slightly more likely) and director-level position (even).

Female and male privacy professionals had similar levels of experience in privacy as well. In fact, although salary levels were comparative, women in the privacy field were found to have slightly less experience than men in the profession, with 39 percent of women having less than five years, compared to only 35 percent for men.

For the 15 percent who had more than 15 years of experience, a salary gap opened up, with men making an average of \$181,000 compared to \$156,300 for women. Additionally, only 25 percent of women privacy professionals held a master's degree compared to 39 percent of their male counterparts.

“A career in privacy places you at the forefront of shaping and defining how technology will impact our daily lives. Diverse voices are needed in this debate and it’s exciting to see so many women excel in the field,” said Nuala O’Connor, President and CEO of the Center for Democracy & Technology.

## IoT developers concerned about privacy and data protection

An impressive 65 percent of Internet of Things (IoT) apps in production today are generating real revenue. The study results, undertaken by Progress and Harbor Research, also reveal developers expect this figure to rise to 80 percent by 2018. The industries that currently lead in IoT development include smart homes, wearables, automotive and sports/fitness.

### Security and privacy

Developers around the globe agreed security and personal privacy, data privacy and protection from malicious attack, and general integration and data management are the top challenges in designing, deploying and engaging customers with IoT apps. They also confirmed these are the biggest challenges in monetizing IoT apps.

While IoT may be a game changer in many respects, from a security perspective the game changes little, according to Tsion Gonen, Vice President of Strategy for Identity and Data Protection at Gemalto. "At its most basic level, security for the Internet of Things depends on our ability to identify devices and their masters, and protect the data that those devices and masters manage and share. A trusted device is one we can reliably identify and associate with a manufacturer or provider. The devices should be able to communicate with the masters, as well as other devices of the same type. A trusted master is expected to securely communicate with dependent devices, and issue firmware/software updates to those devices in a way that provides

assurances that the code is authentic and unmodified."

"Encryption is the foundation of trust for IoT. Communication between devices and their masters requires encryption as it validates who can talk to whom and validates what is sent as being valid. In addition, as sensitive data travels through the cloud and IoT environment, it should be encrypted to prevent interception. Likewise, stored data should be transparently and seamlessly encrypted to prevent theft," Gonen added.

Survey respondents believe commercial vendors (31%) and the open source community (24%) have the greatest power to help overcome these top challenges. They have little faith in the potential contribution from government (8%) or industry bodies (7%).

"As IoT enables some vendors to generate a revenue stream past the point of purchase through bundled services, security and privacy issues will always be a cause of concern," according to Alon Lelcuk, Vice President of Research and Development, Security at Radware. "Robust security and privacy protection are not mutually exclusive of this new technology. The moment we allow these devices into our lives and our homes we invite a level of vulnerability and increase the threat landscape. If it's important for vendors to monetize IoT and provide products and services to make our lives easier, then implementing security protocols such as device based authentication and access control to protect our personal privacy and information is just as critical."

## (ISC)2 Security Congress 2015 and ASIS 2015

Proudly colocated for the fifth year in a row, (ISC)2 Security Congress 2015 and ASIS International 61st Annual Seminar and Exhibits (ASIS 2015) expect more than 19,000 professionals worldwide from both the information security and operational security disciplines to join together September 28 -

October 1 in Anaheim, CA. Offering more than 80 education sessions along with networking and career advancement opportunities, (ISC)2 Security Congress 2015 will include topics on best practices, current and emerging issues, and solutions to challenges.

(ISC)2 members are eligible for special discounted pricing and will have opportunities to attend exclusive member events, including a networking reception and town hall meeting.



## The Art of War applied to web application security by Neeraj Khandelwal

**"Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike him where he has taken no precautions." – Sun Tzu**

Over the years, almost all applications have slowly transitioned from the desktop to the web, requiring just a generic browser and credentials for access. Web applications are at the center of today's IT world, from mobile banking, HR portals, payroll, partner portals, ERP, CRM tools to administrative interfaces, email, social media and more. Thus, web applications have become the new perimeter. That being said, they are notoriously more difficult to secure than the network. Attackers know that web application security is poorly understood and enforced, and following Mr. Tzu's advice, this is where they have been increasingly focusing their attacks.

The 2015 Verizon Data Breach Investigations Report highlights that web application attacks account for more than 30% of the attacks in certain industries, with Financial Services, Information and Public entities leading the pack. Last year, the report also highlighted that most of these incidents took months or even longer to discover, and were reported by an external entity in the majority of cases. Data from Zone-H suggests that in the last five years, around 5.5 million sites were defaced, at an

average over one million per year. The Online Trust Alliance estimates that websites serving malware-laden ads increased by 200% last year, to over 209,000 incidents, generating 12.4 billion malicious ad impressions.

*"By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided." – Sun Tzu*

Here are the steps of an attack:

- 1. Find your public dispositions:** That is, what types of applications you are running and the infrastructure they are running on.
- 2. Devise appropriate strategies** for attacking different types of applications.
- 3. Commercial and open source software will be attacked** with known exploits, assuming patches are missing or delayed.
- 4. Bespoke software will be targeted** for common application vulnerabilities, assuming poor coding practices.
- 5. Underlying infrastructure will also be profiled** and targeted using the web applications as a conduit (e.g. Shellshock).

Apart from directly probing your perimeter, attackers also use popular search engine caches for their recon activity. Those caches can expose a goldmine of information about your software and configuration weaknesses (e.g. Googledorks) that are leaked out to search engine crawlers.

Commercial and open source applications and infrastructure receive wide attention from attackers and security researchers, but they still fall the most. One of the most alarming revelations in the Verizon DBIR 2015 report is that 99.9% of the exploited vulnerabilities were compromised more than a year after the CVE was published. Similarly, HP's 2015 Cyber Risk Report found that 44% of confirmed breaches in 2014 resulted from exploiting known vulnerabilities that were two to four years old.

What this highlights is that most organizations struggle to cope with the daunting process of server patch management and easily fall victims to known vulnerabilities. After all, why should an attacker invest in finding zero-days when there are hundreds of thousands of unpatched systems on the Internet?

As for bespoke software and your own customized application code, there are no signatures or patches. The code may be written by current employees, ex-employees, contractors, integrators or third-party outsourced developers, most of whom have never had a day of formal security training. To make matters worse, this code is in a constant state of flux, being updated daily by web developers responding to business needs, not security requirements. Attackers target such applications using automated tools that exploit common flaws introduced during development cycles, such as the OWASP Top 10.

*"Speed is the essence of war." – Sun Tzu*

There is a constant barrage of software updates, patches, security advisories and threat bulletins, and attackers know that if they can exploit vulnerabilities faster than whitehats can patch them, they can hit gold.

As a consequence, most CVEs in 2014 were exploited in the wild within a few days of disclosure, and Metasploit modules for many of

them became available in a couple of weeks. The fact that most of them were exploitable over the network without requiring any authentication was not very encouraging.

Though this threat intelligence is available to the attackers and whitehats at the same time, attackers have a distinct advantage. They can weaponize this information stream much faster, as they are not hampered by the change control processes and maintenance windows that the defenders have to struggle with.

Moore's law predicted exponential growth of computing power. Unfortunately, attackers are beneficiaries of this law too. Today, there are about 1 billion sites on the Internet. A few years back, scanning for them using commodity hardware would have taken months. However, a new breed of freely available tools like masscan, scanrand, unicornscan and zmap can now scan the entire Internet from your commodity quad-core desktop processor, at home, on a decent ISP connection, in just three minutes!

These tools can also aid in delivering attack payloads. For example, masscan was used to deliver Shellshock exploits on the Internet in a day or two after its disclosure.

While continuous vulnerability scanning has been touted of late, it fundamentally remains a reactive approach. The scan > identify > fix > test > deploy cycle leaves a big window of opportunity for the attackers. A more proactive approach is needed to stem the tide.

*"All warfare is based on deception." – Sun Tzu*

The latest trick in the attacker's playbook is to attack you through someone you trust. This is reflected in mass-compromises of random websites, which are then used to attack the eventual victims. The compromised websites become "secondary victims" that facilitate the attack.

Distributing malware or staging phishing attacks through these "secondary victims" can result in the installation of backdoors on the visitors' machines and the theft of sensitive data like credentials, financial information or intellectual property. Building spam, DDoS

and click-fraud botnets is another motivation.

The Verizon DBIR report indicates that in 70% of the attacks where the motive was known, there was a "secondary victim" that paved the way for the attack. And the most common vector by far is "strategic web compromise" of the secondary victim. The majority of these attacks were not part of targeted, espionage-style campaigns, but just opportunistically compromised servers.

So, if you're thinking that you have nothing of value for attackers, think again. Your web presence has intrinsic value that can be monetized or leveraged by attackers in creative ways and make you an unwitting "accessory to a crime." Once this happens, search engines will flag you, and your business and brand is bound to suffer.

*"To rely on rustics and not prepare is the greatest of crimes." – Sun Tzu*

## Knowing your attack surface involves comprehensive knowledge of all the applications running in your organization that are remotely accessible

So why do we fail so miserably in patching our Internet-facing applications and servers? The simple answer is that it's hard and it requires significant planning, time, and energy.

While the attackers are racing to weaponize new vulnerabilities, the vendors have to develop and push out the patches and updates, and organizations have to assess the risk, regression test the patches, ensure critical business applications are not broken, schedule the maintenance windows, install the patches and pray that everything goes smoothly. Clearly, whitehats are handicapped to begin with, even when there is intent to win the patching race.

To complicate matters, the rate of new CVEs is continually increasing. On [cvedetails.com](http://cvedetails.com), 2014 witnessed 7,945 new CVEs ("only" 5,191 were recorded in 2013). Scaling the remediation process across an entire enterprise, getting timely buy-in from the stakeholders, overcoming conflicting priorities and sometimes dealing with buggy patches can prove to be overwhelming.

*"If you do not know your enemies nor yourself, you will be imperiled in every single battle." – Sun Tzu*

So far, we have been focusing on knowing the attacker psyche and tactics which is essential for modeling risk. But an equally important endeavor is to be fully aware of your own attack surface.

Knowing your attack surface involves comprehensive knowledge of all the applications running in your organization that are remotely accessible. This includes inventorying all the servers across all different groups within the organization and tracking the versions of operating systems, application software, middleware, programming frameworks, databases, encryption modules, plug-ins, and so on, installed on them.

Unless you know this, you cannot assess the risk from new exploits, you cannot decide if it is relevant or critical for your organization, and you cannot plan a response. In short, you are in peril.

Even if a seemingly insignificant server is compromised, attackers will use it as a staging point to collect sensitive information and to move laterally within the network looking for higher profile targets.

Custom web applications create a greater dilemma. For these, there are no patches or updates. Nonetheless, almost all legacy and new web applications are riddled with bugs and vulnerabilities. How do you fix something that you don't even know is broken?

*"To be prepared beforehand for any contingency is the greatest of virtues." – Sun Tzu*

While most exploits target servers and applications, they have to travel through the network to get to the victims. This makes the network an obvious place to detect and block exploits, while patching and hardening applications happens in the background. While network firewalls are ubiquitous, they operate primarily on the network layer with no visibility into application layer traffic.

IPS and IDS solutions incorporate some application layer signatures, but they operate on a packet level, rather than an application session level, thus missing several important ex-

ploits. Both of these have blind spots in encrypted traffic (e.g. HTTPS), which can make up 50% of an average enterprise's traffic. Furthermore, these are completely signature-based solutions that rely on blocking known exploits whose signatures have been released by the IPS/IDS vendors.

Web application firewalls (WAFs) are becoming industry-standard solutions to secure HTTP and HTTPS applications. They combine blacklisting with whitelisting and anomaly detection mechanisms to identify and block exploit traffic. Due to these mechanisms, most new web-based attacks are blocked before they reach the target applications, without requiring new updates or signatures. Most WAFs have a reverse proxy mode that can inspect SSL traffic, thus removing blind spots in your security posture. Some also come with application acceleration features that help speed up the page loading times of your web applications.

## **IPS and IDS solutions incorporate some application layer signatures, but they operate on a packet level, rather than an application session level, thus missing several important exploits.**

*"What the ancients called a clever fighter is one who not only wins, but excels in winning with ease." – Sun Tzu*

This is not to say that WAFs should replace your existing security tools and patch management processes. In fact, they are a complimentary solution that provides a safe harbor while the root vulnerability is mitigated. That having been said, fixing the root causes might not be always feasible in legacy or outsourced applications, so WAFs can be invaluable in those situations.

Most importantly, WAFs solve the "you don't know what you don't know" conundrum posed by insecure custom web applications, since they inspect each and every HTTP construct for known and unknown vulnerabilities before it hits the web applications.

Overall, consider deploying a web application firewall so that developers and remediation teams can breathe easy and you can win the web application security battle against your adversaries.



# Watchful

Keep IT secret.

Watchful helps keeping information safe from security breaches or disclosure, resulting from malicious wrongdoing or inadvertent misuse.



Are you controlling  
**INFORMATION  
DISCLOSURE?**



## RightsWATCH

data-centric security

A layered Information protection solution to keep data safe and secure regardless of whether it is at rest, 'on-the-fly', or even if it's totally outside your network perimeter.



## TypeWATCH

e-biometrics security

An advanced Persistent Security mechanism, using state-of-the-art e-Biometrics, to continuously verify that the people using your systems are who you think they are.

Do you want to know more? See us today at [www.watchfulsoftware.com](http://www.watchfulsoftware.com)

# Signature antivirus' dirty little secret

by Corey Nachreiner



**If you rely only on traditional, signature-based antivirus, you are going to get infected—and probably often! Antivirus was, and still is, a valuable addition to your layered security strategy, but only if you understand its limitations, which have become more and more prominent over time.**

## What's wrong with signature-based AV?

You probably know signature-based antimalware solutions work by recognizing patterns in known files. If a human or automated system identifies a particular file as malicious, it's relatively easy to find some pattern that uniquely identifies that specific file, whether it is a file checksum (hash), a binary pattern, or even a more complex algorithm that looks for multiple "signs" or patterns. However, this detection methodology suffers from two issues (which even its inventors realized years ago).

**1. Signatures only help after you know something is malware** – Signatures are reactive. They're great at the prevention part, but worthless for initial detection; you can't write them until after you've discovered something bad. This means unless the signature writer (AV company) identifies malware as such, some initial victims will get infected.

**2. Bad guys can obfuscate executables almost endlessly** – Some might think a particular executable program always looks the

same on a binary level (barring its creator changing something and recompiling). However, the truth is you can repack and obfuscate the same executable using many different techniques. In the underground world, black hats refer to this as packing and crypting. Without going into technical specifics, they essentially jumble up an executable on a binary level, so it looks different and even has a different checksum, but still runs. The malware does the exact same thing, but its old signature no longer catches it.

These problems are not new. Researchers, and antivirus experts have known about them for decades. However, these weaknesses have become much more prevalent over time. Here's why.

## What's AV's dirty little secret?

First, threat actors, and their motives and methods, have changed over time. When AV was born, you could basically categorize black hats into two profiles—script kiddies and unorganized cyber criminals.

For the most part, these types of attackers didn't customize malware or do targeted attacks. They were indiscriminate, spamming as many folks as they could or designing malware that would mass scan the Internet and infect any victim opportunistically. This was good news for legacy AV since the malware associated with these attacks quickly hit the threshold necessary for AV companies to notice it and write a signature.

However, now that organized criminals have entered the fray, and customize malware for specific targets (such as Point-of-Sale malware), today's threats do not spread as widely and affect as many victims as quickly. This means it takes much longer for new malware to hit the threshold where AV companies might notice and analyze it.

In short, signature-based AV has always had a vulnerability window—a period of time before protection gets implemented—but that window is getting wider and wider as attackers get smarter about limiting their malware.

Second, and more importantly, today's malware has become much more evasive. Packing and crypting, and other AV evasion techniques, have existed for quite awhile. In fact, I think security researchers discovered many of the techniques before the bad guys did. However, these techniques are technically hard. You have to understand a lot about programming, executable standards, and assembly in order to obfuscate an executable program without actually "breaking" it. Years ago, this relegated these tricks to the most sophisticated attackers.

However, criminals are nothing if not opportunistic. If researchers release new proof-of-concepts, or other attackers use cool new techniques, smart criminals will quickly copy and adopt them. Worse yet, malware-as-a-service (MaaS) has taken off lately. Advanced hackers now create and sell tools that essentially give easy access to less sophisticated criminals.

Today, you can find many packers and cryptors on the underground that allow the least savvy attacker to get his malware past many AV products, even if it was previously recog-

nized. It's gotten so bad that many of the malicious servers distributing malware automatically repack their payloads regularly. This packing and crypting or evasion problem is the primary reason signature-based AV is no longer very effective—it's the dirty little secret.

Have you ever noticed how many variants of the same malware you see nowadays? An AV vendor might list a new threat called Bad32; and a few hours later they have Bad32.b; before you know it they're up to Bad32.azytd12d. This isn't necessarily because Bad32 has changed much, but is often because the attackers are repacking it.

The latest malware growth trends also help illustrate the problem. For example, AV-Test reported that there were over 140M new malware variants in 2014. Do you really think attackers wrote that many unique trojans, worms, etc.? No way! Rather, they repackage the same threat over and over, so it can continually evade signature-based AV.

How big is the AV efficacy problem? Well, according to Damballa, AV misses 70 percent of new malware during the first hour after its submission (and remember submission to AV vendors is different than its actual release into the wild).

### **What can I do to catch evasive malware?**

After hearing legacy AV is that bad, you may wonder what you can do. Behavioral malware detection, sometimes called next generation sandboxing, is the solution.

Although it's become pretty easy for bad guys to obfuscate their malware files, it's much harder for them to obscure their malware's behavior. If you can run or open a suspicious file in an emulated or virtualized environment (often called a sandbox) you can see what it does and decide whether or not it's bad right away. This is pretty much what human analysts did in the past; only today we can automate the process and do it close to real-time.

Behavioral analysis is not a new idea, but it too has weaknesses or disadvantages. For example, it takes a lot of computing resources to run a suspicious file in a virtual environment

and analyze its code. In fact, the more convincingly you emulate a victim system, the more this sort of analysis costs. On the flip side, the less convincingly you emulate a real system, the less effective the behavioral analysis becomes. On top of that, legitimate programs sometimes do similar things to malicious ones. This could lead to false positives, or good files that are blocked as malware. However, unlike signature-based AV, the weaknesses with behavioral detection become less prevalent over time. Moore's law steadily increases our processing capabilities, and virtualization technologies have become more robust, making sandboxing much faster than it was years before.

Furthermore, the breadth of malicious behaviors we recognize today has grown signifi-

cantly, allowing us to fine-tune behavioral detection and lessen false positives. In short, advanced malware protection has moved from the realm of the experimental and into the reach of even the smallest business.

**If you want to block today's malware, adopt advanced threat protection**

Signature-based AV can't keep up and fails to catch the latest malware on a regular basis. Behavioral or heuristics-based malware detection helps, but basic implementations found in host-based solutions are only partially effective. If you really want to protect from today's highly-evasive, constantly morphing threats, I highly recommend you add an advanced malware detection or next-generation sandbox solution to your existing layers of defense.

Corey Nachreiner is the Director of Security Strategy and Research at WatchGuard ([www.watchguard.com](http://www.watchguard.com)).

FRESH SECURITY NEWS

[www.twitter.com/helpnetsecurity](http://www.twitter.com/helpnetsecurity)



**ENDPOINT  
PROTECTOR**

Data Loss Prevention at its best

Get your complete security in a simple appliance with powerful and rock solid foundation for your sensitive data.



## Device Control

### **Protect the entire network**

USB monitor and lockdown for Windows, Mac and Linux.



## Content Aware Protection

### **Precise control over transfer of documents on Windows and Mac OS X computers**

Enforce corporate policy by ensuring documents containing confidential data are not shared via online applications outside the company.



## Enforced Encryption

### **Additional security for data copied on USB devices from Windows and Mac OS X computers**

Make sure that users copy sensitive data only to encrypted USB devices to avoid data leakages in case devices get lost or stolen.



## Mobile Device Management

### **Control iOS and Android devices to secure corporate data**

Secure your mobile devices and keep a close eye on sensitive enterprise data both inside and outside companies' walls.



[www.endpointprotector.com](http://www.endpointprotector.com)

Phone: +40-264-593 110

E-mail: [feedback@cososys.com](mailto:feedback@cososys.com)

Cososys Ltd. • Haiducului St.6 400040 Cluj-Napoca, Romania



## Review: Tresorit for Business by Berislav Kucan

**In the cloud computing era, companies need to be proactive on secure collaboration and file sharing. Tresorit for Business is a solution that, among other things, helps organizations manage, protect and prevent leaks of their corporate data.**

The service provides end-to-end encryption for data in motion, along with all the enterprise functions related to managing user behavior and enforcing the policies for sharing the data in the most secure way possible.

### How does Tresorit work?

One of Tresorit's major advantages is a patent-pending security system where both the encryption and decryption is done on the client side. In the "Snowden era" it is important to note that Tresorit doesn't store any aspect of the crypto process that could make anyone else able to access your files.

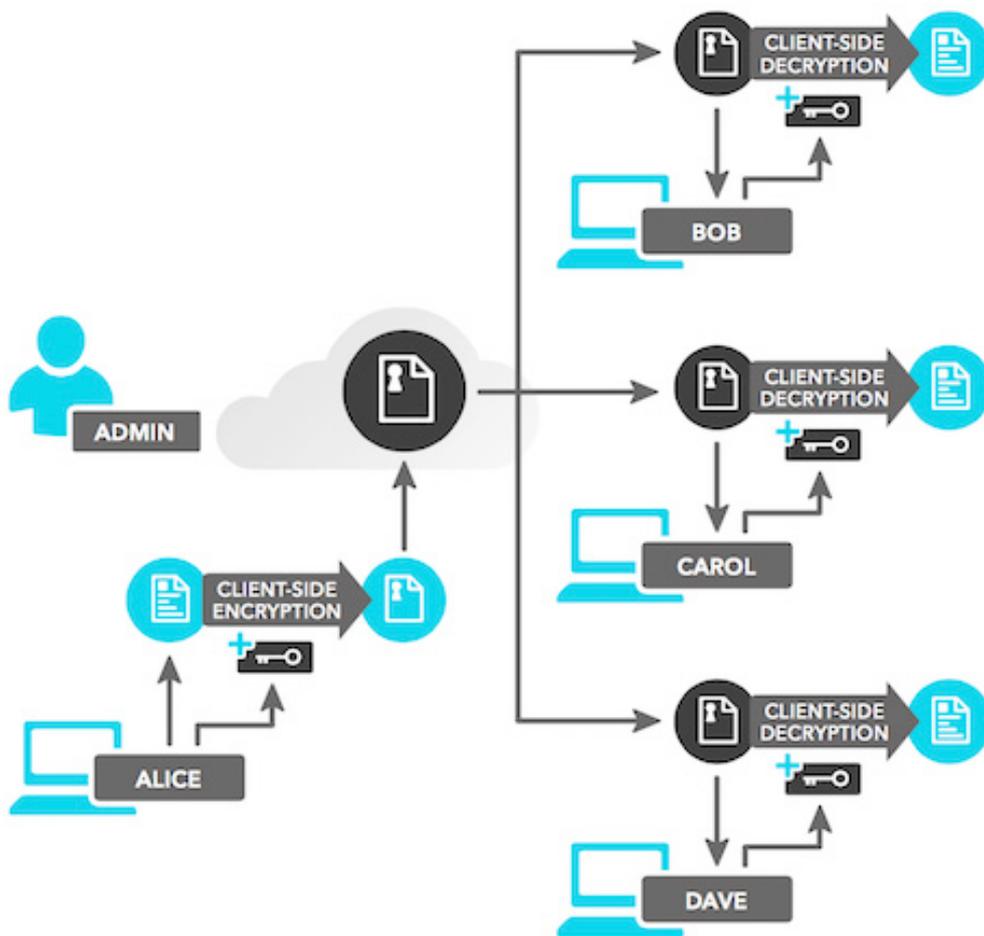
Also, the company handles the data under strict Swiss privacy laws. Their datacenters, made disaster proof and protected by 24/7 physical security, are located in the European Union and are HIPAA and ISO27001:2013 compliant.

All files uploaded to the cloud are encrypted, client-side, with AES-256 encryption. File operations are authenticated by using RSA-2048 signatures applied on SHA-512 hashes.

Transport Layer Security (TLS) is used between the client's workstation and the Tresorit cloud service. Invitation and key agreement is done with ICE and ITGDH. The latter is a key management protocol that allows a group of users to agree on a shared group key, which can be used to protect shared data stored remotely in the cloud.

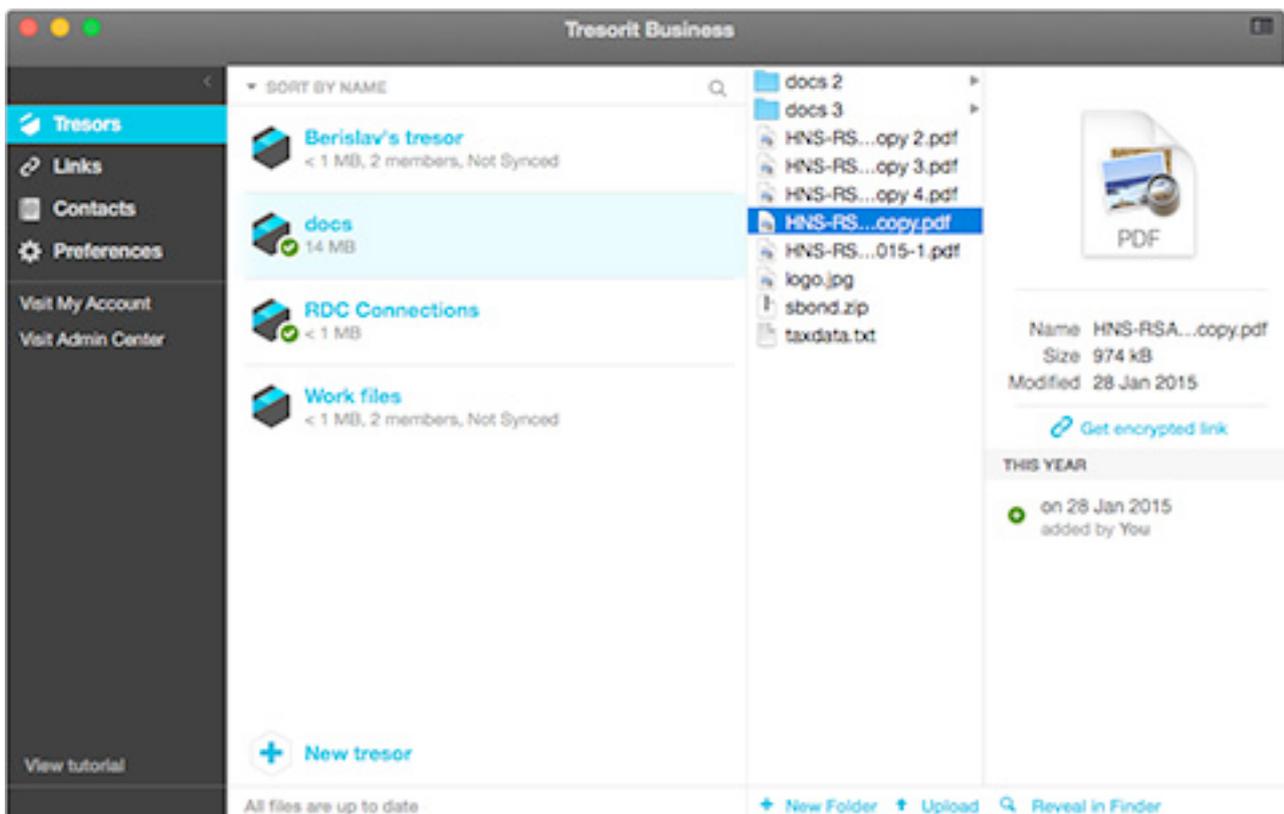
### Tresorit applications and web access

The Tresorit desktop application is available for Windows and OS X systems, iOS- and Android-running mobile devices, as well as Windows Phone and Blackberry devices. Tresorit is also among the first apps offered on the Blackphone Silent Store.



I'm an OS X user, so I am basing my experience on the Mac version of the product. The installation was pretty straightforward and the application itself looks clean and is easy to use. There aren't many options here, as the

functionality from the client perspective is focused on encrypting and sharing files and managing encrypted links. I'll go into more details on these links later on.



From a client's standpoint, generating and storing data begins with creating specific Tresors. Tresors are placeholders for the files that they will manage. Every Tresor corresponds to a local folder, which the user can work with even outside Tresorit.

The files inside the Tresors/local folders are unencrypted, but when they are synched to the cloud, their online versions are encrypted. Versioning history, as well as detailed specifications about activities (added, edited, deleted, etc.) is available for all the files. Tresors shared by other users will become visible inside the application.

One of the things that I considered to be a major negative aspect of Tresorit was fixed just a couple of weeks ago, when the company introduced web access to the encrypted files. If it seems strange that web access is called a new feature in 2015, check out a blog post from 2013 (<http://tinyurl.com/oduhy54>), in which security-minded developers of Tresorit specified that they couldn't guarantee the highest level of security for web access, so this feature was put aside until this could be achieved. A new blog post (<http://tinyurl.com/qhy94bq>) explains how they implemented the whole "zero knowledge" (your data cannot be seen by them) concept into the web access interface.

## Administration and policies

The administration web interface has three tabs: activity, users and devices, and groups and policies.

*Activity:* This is a textual and graphical overview on high level Tresorit usage within the organization. There are pie charts with specifics on storage per user, as well as operating systems used. The activity section provides a snapshot of which user logged from what device and IP address. Have in mind that the location is approximate, as it is used based on an IP range and is mostly there to identify possible compromised accounts (i.e. accessed from another country).

*Users and devices:* Settings related to managing users on your account, checking usage stats and the devices they are using to use Tresorit. From here, every user and their device can be suspended or activated, or they can be added to a specific group.

*Groups and policies:* Typical set of functions where the administrator can set up rules, such as timeout policies for logged in users, IP filtering, two factor verification, ban specific platforms, etc.

Allowed IP addresses		
Contractor #22	23.12.233.1	23.12.233.133
Contractor #23	121.22.34.1	121.22.34.244
Proxy	78.0.19.246	78.0.19.246

Enter IP rule name      Start IP      End IP

## Digital rights management

While I didn't use and test this option, it's good to know it exists.

Tresorit DRM complements Tresorit's existing cloud-storage solution by offering more control to businesses by extending security to documents once they have been shared, and during collaboration. The DRM aspect of Tresorit is powered by the Microsoft Windows Rights Management Services (RMS) technology. By

using DRM enabled Tresors, senders and receivers are prevented from saving, printing, copying or taking screenshots of DRM protected files.

## Two-factor authentication

With the majority of data moving online, two-factor authentication is a function that every service of this type should provide to users. Tresorit offered the two-step verification option for Business users in November 2014.

The service can be enabled from the "Security" tab of the account settings and will become active the next time you log in manually or install Tresorit on a new device. I stressed the phrase "log in manually," because you can

access the web based admin interface without authenticating by clicking a link from the Tresorit application. This link is, of course, not static.

#### 2-STEP VERIFICATION

Verify code

[Other verification options](#)

Two-step verification options include a mobile app (such as Google Authenticator for iOS), text message to a cellular phone, voice call, and email. If you enable the mobile application, the system will automatically add the email option by default. As it is stated: "For security reasons you must have two active options for 2-Step verification. If you deactivate this option, we will no longer ask for your authentication code when you sign into your account."

I understand that this is probably enforced because of usability, but for those of us who are paranoid, this could be viewed as a security risk. Mobile app, voice call or text message are authentication methods that are (at least) a bit harder to compromise than email, so automatically adding email as an alternative to a mobile authenticator is subpar.

### Encrypted links

I've been using the Tresorit service for a couple of months now and one of the things I en-

joy on a daily basis is a seamless, secure file-sharing process called Encrypted Links. When sharing files over email, and especially larger files, I used to use one of the cloud data service providers such as Box.com or Dropbox. This is a good solution for low-key data files, but I never uploaded anything remotely personal in unencrypted form. Even though those are legitimate businesses, we all know that there are a number of risk factors with data that is stored in the cloud without an extra layer of security. SSL access to the service doesn't cut it.

Tresorit provides a good alternative with Encrypted Links, because you can simply "right click" on any file on the computer and create an encrypted cloud copy of it instantly. You can set up an expiration date for the link, limit the number of times the file can be downloaded (I always use 1 when sending a file to someone; you never know who is "out there") and you can even password-protect the file for extra protection.

Create Encrypted Link to boxes.jpg

Configure & click Create

Expires: in 10 days, on 11/ 4/2015

Number of downloads limited to 4

Create

The newly created link is automatically copied to your clipboard and is ready to use. With the latest update, Tresorit finally changed the look of the links: a month ago the link would be very long (typically around 240 characters), and now they use a shortened version (just over 40 characters) that looks much better when you send it via email. (A three-line-long web link with "random" characters? XSS was always the first thing on my mind.)

These linked files use the same encryption as the "regular" Tresorit synched files, but the system creates a temporary decryption environment - a lightweight version of Tresorit - in the recipient's web browser. From a technical point of view, this is done in a way that makes sure that the Tresorit server cannot access the sent data and the data can only be decrypted by the recipient on her end.

The Encrypted Link option is currently not available in all web browsers. The company specified that older Internet Explorer browsers are not supported due to security reasons, and on my OS X, I cannot use Safari with it - just Chrome and Firefox. It should be noted that Javascript has to be enabled for the browser decryption process. Opening en-

rypted links on some mobile devices is potentially possible, but not currently officially supported.

All of the encrypted links you've created will be listed in the appropriate section of the Tresorit application.

### Pricing

Tresorit for Business is priced at 20 EUR per month for an organization of up to 200 users. This includes 1000GB storage per user, unlimited sharing and activity history, remote wiping of documents, priority support and live training. Enterprise plans for larger organizations can be set up with the sales team.

### Final thoughts

Tresorit for Business is a great product that is simple to use and provides a high level of security for data in transit. The system is being developed actively, so every now and then new features are released. Security is obviously extremely high on the list of priorities of the Tresorit team, and I will definitely keep using it.

Berislav Kucan is the Director of Operations for (IN)SECURE Magazine and Help Net Security ([www.net-security.org](http://www.net-security.org)).





# SOLUTIONARY®

AN NTT GROUP SECURITY COMPANY



## Services and Intelligence to Optimize Security and Mitigate Risk.



Managed Security Services

Targeted Threat Intelligence

Security Log Monitoring

Log Management

Critical Incident Response

Professional Services

Visit [Solutionary.com](http://Solutionary.com) for More Information



## Making IoT security a reality by Martin Bergenwall

**We must challenge the status quo to ensure that we do not trade our personal security and privacy for convenience and business opportunity.**

The Internet of Things (IoT), which is connecting thermostats, home security systems, power grids, automobiles, medical devices and a plethora of business devices to the cloud, is seen by many as a tremendous advance for personal convenience as well as a new frontier of endless business opportunities.

IoT promises to enable consumers and businesses to remotely control everything in their home or offices, from the temperature to the lights, locks and security systems; to monitor health including blood pressure, heart rate, steps taken or calories burned; and to gather massive amounts of data on anything from location to shopping habits.

Many of these IoT offerings are still in the embryonic stage, but the number of connected devices is predicted to grow from an estimated 5 billion today to some 25 billion by 2020.

### **Security concerns grow along with IoT potential**

IoT also introduces new security risks. Many are wondering if the promise of IoT can be realized if we continue to treat security as an afterthought—and if so, at what cost? Today seventy percent of devices use unencrypted network service. Seven of ten devices enable an attacker to identify valid user accounts through account enumeration. Six out of ten devices that provide user interfaces are vulnerable to a range of issues such as persistent XSS issues and weak credentials.

If these trends continue, how will we keep our critical infrastructure safe? How will we turn the tide against attackers who want to use our personal information for malicious purposes or financial gain? And what privacy—if any—will we retain?

## An illustrative case

Home surveillance systems are one of thousands of IoT applications that are growing in popularity. Adding security cameras to home entertainment networks, which already provide customers with a high bandwidth Internet connection, a TV monitor to view video feeds, DVR storage and network control intelligence in the router, is a natural extension of services with huge revenue potential for home entertainment companies. Nearly half of the 115 million US households are connected to the Internet and two-thirds have a DVR.

By linking security cameras and adding appropriate software to the router, users are able to display video streams, as well as store and remotely access live or recorded feeds via the Internet to monitor their homes—whether they are in the home (e.g., to monitor an infant from another room) or away.

To enable monitoring services, the cameras are plugged into home entertainment centers using Ethernet cables, which then transmit their signals to a switch/hub. However, without sufficient security, this connection is vulnerable to Man-in-the-Middle attacks. Burglars

can tap directly into the cable and display a static photo in place of the live video stream—as featured in many popular movies, including *Oceans 11*, and television shows like *Mission Impossible*. So what was once considered a safety feature now becomes a safety flaw.

Perhaps even more concerning is the possibility of home cameras and monitoring systems being hacked by a stalker or someone with nefarious intentions. It's one thing for a parent to monitor an infant from another room, but what happens when a stranger breaches the system—turning on cameras in any room to watch or record the activities of the entire family?

It is often easy for consumers and IoT solution providers to dismiss security concerns in favor of convenience and increased revenue, but lawsuits against home entertainment security systems providers have already been filed and won after the hacking of monitoring systems led to successful burglaries. Additionally, parents have discovered hackers talking to them or their child through baby monitoring systems. And a website was discovered that made 73,000 camera feeds available on the Internet.

# UNLESS SECURITY IS VIEWED AS A CORE FUNCTION INSTEAD OF AN ADD-ON, WE'RE BOUND TO REPEAT THE MISTAKES OF THE PAST

## Why security is often an afterthought

News headlines of new vulnerabilities, exploits, credit card fraud, and/or viruses abound as we continue to see the escalation of technological exploits, which keep pace with technology advances. Unless security is viewed as a core function instead of an add-on, we're bound to repeat the mistakes of the past. But rarely do technology solution providers approach a design or system problem with the intent to include security from the start.

Often even basic security principles - such as strong passwords - that have been taught for

over 20 years don't make it into the product development cycle. To win the race to market with new, innovating IoT solutions, companies are accelerating development cycles, which means that security is either forgotten, severely limited, or poorly implemented. In other cases, developers of legacy embedded systems don't consider security controls because their systems were originally isolated from networks. As these systems become increasingly networked and remotely managed, they are vulnerable to new attack vectors, which must be considered at the beginning of the product development lifecycle.

## Keys to better security

The protection of IoT depends on a new security model and standards. Our current security models for PCs and smartphones are not applicable to IoT devices. Most devices have limited processing and storage capacity.

Many "smart" products fall into an "install and forget" status under the management of consumers.

Internet security is at an important crossroads, coming from the world of "connected security" to that of "embedded security," where the only true protection lies. Security is moving from a

world where any device/object was considered "secure" when connected to a smart card, to a world of security embedded at the heart of the system, at the heart of the main processor of the device.

In addition to a new security model, new standards are critical for ensuring secure and interoperable IoT devices. The consumer IoT market is loosely regulated and lacking security and safety standards. Other markets, such as medical, manufacturing, automotive and transportation, have security and safety standards that must be updated to include IoT devices.

# ONCE A BREACH THAT JEOPARDIZES LIVES AND SAFETY OCCURS, IT'S ALREADY TOO LATE.

## Example of a deployed IoT security solution

When technology providers embrace security as a core function of their offering, they can innovatively deliver convenience and security.

Stronger passwords are a first step, but new hardware and software designs that embed security at the heart of the system are necessary to prevent breaches. In the case of the home security monitoring system, these security challenges were solved by:

- Embedding a security module in the cameras and in the router. This dedicated, hardware-based security supports attack-resistant mutual device authentication.
- Securing communications using the MACSec security protocol to protect data-in-transit over the Ethernet communications link.

The combined security module and MACSec solution provides end-to-end security so that all connected devices are authenticated, secure key exchange is assured, and all data

transferred between devices is secure, authenticated and integrity checked.

This solution is broadly applicable and can be used to secure many forms of devices that connect to a network using Ethernet or Wi-Fi.

## Defining the way forward

Our computing needs are changing, and security must become proactive instead of reactive. While some IoT devices are a novelty, many are critical to the safety of humans, property and resources. Once a breach that jeopardizes lives and safety occurs, it's already too late. As an industry and as individuals, we must resolve to do better.

We must work together to see that new security models and standards that address the unique security demands of IoT are implemented. And we must demand products with security built in, including those that encrypt data and communications.

Martin Bergenwall is the Executive Vice President of the Mobile Security Business Division at INSIDE Secure ([www.insidesecond.com](http://www.insidesecond.com)). Mr. Bergenwall joined INSIDE Secure from AuthenTec in 2012 where he was in charge of Product Management for software products in the Embedded Security Solutions division. Prior to this, Martin headed up the R&D software teams in the Embedded Security Solutions division of SafeNet then later AuthenTec.



# ARE YOU ADEQUATELY PROTECTED AGAINST DDoS ATTACKS?

**DOSarrest's fully managed, cloud-based DDoS protection service guarantees website availability and keeps attackers out!**

Traffic scrubbing centers in  
**London, NYC,  
LA and Singapore.**

DOSarrest has been  
**protecting websites against  
DDoS attacks since 2007**

DDoS attacks are larger and more sophisticated than ever before. It can paralyze your website, leaving you unable to process transactions, accept payments, and disseminate information. A combination of attack methods can lead to data loss, ID theft, and fraud.



US/CAN Toll Free: **1.888.818.1344** \* Press 1 for Sales

UK Free Phone: **0800 086 8812** \* Press 1 for Sales

Singapore Toll Free: **800 - 101 - 1796** \* Press 1 for Sales

Email: **sales@DOSarrest.com**

**Head office:**  
Vancouver, B.C., Canada



## Malware world

### MalumPoS can be customized to target different systems

A new Point-of-Sale RAM scraper is being offered for sale, and is currently designed to collect data from a very specific type of PoS systems: those running on Oracle MICROS (often used in the hospitality and retail industries, mostly in the US).

"Aside from Oracle MICROS, MalumPoS also targets Oracle Forms, Shift4 systems, and those accessed via Internet Explorer. Looking at the user base of these listed platforms, we can see that a major chunk is from the US," Trend Micro researchers noted.

It's also interesting to see that, at the moment, MalumPoS is trawling the PoS' RAM for data about Visa, MasterCard, American Express, Discover, and Diner's Club payment cards - data for other cards is ignored. MalumPoS has many similarities with Rdasrv, the family

of RAM scrapers that in 2011 started the PoS malware run, making it possible and likely that the author(s) is one and the same, or they are somehow linked.

"What is clear is that the persons operating MalumPOS had prior information about their target's environment as they are able to customize binaries based on the target's POS systems, plant them within the target's environment, and manually collect the stored data," the researchers pointed out.

The malware employs several detection prevention techniques, including using an old time stamp for the collected files, loading some of the APIs dynamically, and using filenames that users associate with well-known, legitimate software (e.g., NVIDIA Display Driver). It's good to note that the malware can be reconfigured to target any other PoS system and be made to target specific environments, so the threat it presents can escalate in the near future.

## Kaspersky Lab reveals cyberattack on its corporate network

In early spring 2015, Kaspersky Lab detected a cyber-intrusion affecting several of its internal systems. Following this finding the company launched an intensive investigation, which led to the discovery of a new malware platform from one of the most skilled threat actors in the APT world: Duqu.

The attack exploited zero-day vulnerabilities and after elevating privileges to domain administrator, the malware was spread in the network through MSI files. The attack didn't leave behind any disk files or change system settings, making detection difficult.

Kaspersky Lab researchers discovered the company wasn't the only target of this threat actor. Other victims have been found in Western countries, as well as in countries in the Middle East and Asia.

Most notably, some of the new 2014-2015 infections are linked to the P5+1 events and venues related to the negotiations with Iran about a nuclear deal.

The threat actor behind Duqu appears to have launched attacks at the venues where the high level talks took place. In addition to the P5+1 events, the Duqu 2.0 group launched a similar attack in relation to the 70th anniversary event of the liberation of Auschwitz-Birkenau. Similar to the P5+1 events, these meetings were attended by many foreign dignitaries and politicians.

Upon discovery, Kaspersky Lab performed an initial security audit and analysis of the attack. The audit included source code verification and checking of the corporate infrastructure. The comprehensive audit is still ongoing and will be completed in a few weeks. Besides intellectual property theft, no additional indicators of malicious activity were detected.

The analysis revealed that the main goal of the attackers was to spy on Kaspersky Lab technologies, ongoing research and internal processes. No interference with processes or systems was detected.

## Preliminary conclusions

1. The attack was carefully planned and carried out by the same group that was behind the infamous 2011 Duqu APT attack. Kaspersky Lab believes this is a nation-state sponsored campaign.

2. Kaspersky Lab strongly believes the primary goal of the attack was to acquire information on the company's newest technologies. The attackers were especially interested in the details of product innovations including Kaspersky Lab's Secure Operating System, Kaspersky Fraud Prevention, Kaspersky Security Network and Anti-APT solutions and services. Non-R&D departments (sales, marketing, communications, legal) were out of attackers' interests.

3. The information accessed by the attackers is in no way critical to the operation of the company's products. Armed with information about this attack Kaspersky Lab will continue to improve the performance of its IT security solutions portfolio.

4. The attackers also showed a high interest in Kaspersky Lab's current investigations into advanced targeted attacks; they were likely aware of the company's reputation as one of the most advanced in detecting and fighting complex APT attacks.

5. The attackers seem to have exploited up to three zero-day vulnerabilities. The last remaining zero-day (CVE-2015-2360) has been patched by Microsoft on June 9, 2015 (MS15-061) after Kaspersky Lab experts reported it.

"Spying on cybersecurity companies is a very dangerous tendency. Security software is the last frontier of protection for businesses and customers in the modern world, where hardware and network equipment can be compromised. Moreover, sooner or later technologies implemented in similar targeted attacks will be examined and utilized by terrorists and professional cybercriminals. And that is an extremely serious and possible scenario," commented Eugene Kaspersky, CEO of Kaspersky Lab.

## On Windows 10, apps can actively defend users from malware

With Windows 10, Microsoft will be adding a new layer of protection against dynamic script-based malware and non-traditional avenues of cyberattack: the Antimalware Scan Interface (AMSI).

AMSI is a "generic interface standard that allows applications and services to integrate with any antimalware product present on a machine."

The interface is there for application developers and antivirus vendors to use. The former can have their app call it if they want some extra scanning and analysis of potentially malicious content.

"While the malicious script might go through several passes of deobfuscation, it ultimately

needs to supply the scripting engine with plain, unobfuscated code. When it gets to this point, the application can now call the new Windows AMSI APIs to request a scan of this unprotected content," Lee Holmes, MMPC Principal Software Engineer, explained.

"While we've been talking about this in the context of scripting engines, it doesn't need to stop there. Imagine communication apps that scan instant messages for viruses before ever showing them to you or games that validate plugins before installing them."

Third-party developers of antimalware products should seriously consider implementing support for AMSI, as their engine can gain insight into the data that applications (including Windows' built-in scripting hosts) consider potentially malicious. Users do nothing, except from benefiting directly from the developers' decision to use AMSI.

## The threat that Stuxnet presents for nuclear power plants is far from over, as there are still 153 distinct machines infected with it around the world.

### 153 machines still infected with Stuxnet

The threat that Stuxnet presents for nuclear power plants is far from over, as there are still 153 distinct machines infected with it around the world.

The discovery was made by researcher Peter Kleissner, whose company managed to acquire two domains used as a Stuxnet C&C server in 2013 and 2014. This allowed them to see how many systems are still infected and regularly "phone" back to the C&C.

The fact that Stuxnet's C&C protocol is not adequately secured allowed the researchers to discover data about the infected machines, including whether Siemens SCADA software is installed on them, and the project path of a found SCADA program.

Nearly half (47 percent) of all these infected machines are located in Iran. The rest are located in India (23 percent), Indonesia (8

percent), Saudi Arabia (7 percent), and the rest of the world.

Of the 153 infected machines, 6 have SCADA development software installed. 5 of these are in Iran, and three of them have having a Siemens Step 7 project path set to "C:\Program Files\Siemens\Step7\S7Proj\04082\_19\040825.s7p" - meaning they are likely an industrial machine (but not necessarily at a nuclear power plant).

"It is inevitable that existing malware infections lower the overall security of the particular machines and the entire networks and therefore make it easier (or possible at all) for anyone else to intrude the system," Kleissner explained.

"Just as Kleissner & Associates' C&C domain control enables us to control any remaining Stuxnet infected machines, any capable intelligence service (or individual with the knowledge and skills) could seize control and potentially cause considerable damage leveraging the remaining infections."

# Report: Hack In The Box Security Conference, Amsterdam 2015

by Zeljka Zorz



The very idea of a hacker conference is unappealing to many, but Hack In The Box is not a typical one. For many years now, it has been an event that draws hackers, researchers, and IT sec leaders, and let's them mix and exchange their ideas and point of views in a very informal setting.

Hack In The Box is, first and foremost, an event where you can learn a lot about all different kinds of things and topics. There are hands-on trainings, presentations of the latest research, keynotes, briefing sessions at the Haxpo - an expo for the latest tech and innovation with workshops open to visitors looking to try their hand at hardware hacking, social engineering, lockpicking and more.

Coders and developers can participate in a developer hackaton, hackers can take part of a Capture the Flag contest. HITB is also a place where your knowledge can grow and your talents can be discovered.

There is literally something for everybody.



## If we want strong encryption, we'll have to fight for it

As digital rights lawyer and special counsel to the Electronic Frontier Foundation Marcia Hofmann correctly noted in her keynote at the conference, the issue of encryption is like a pendulum: sometimes, like in the wake of the 1990s crypto wars, it swings towards strong encryption, but it could now swing in the other direction.

One could argue that it swung in the other direction without us knowing: while we believed ourselves relatively safe, the documents leaked by Edward Snowden revealed that governments actively worked at subverting encryption efforts.

After the public exposure of NSA's and GCHQ's MUSCULAR operation, which was aimed at tapping the overseas fiber-optic cables used by Google and Yahoo to exchange data stored in their many data centers in the US and abroad, tech companies began seeing governments as adversaries, and have started working on encrypting their users' communications.

And, as they already witnessed the government's power to force them to hand over data and make them keep quiet about it, they have decided to opt for encryption systems that made it impossible for them to hand over the encryption keys.

The US and UK governments reacted by raising a campaign (still ongoing), trying to paint encryption as something only criminals use, and started lobbying for mandated backdoors. Smartphone encryption is particularly offensive to them, it seems, and even the Washington Post Editorial Board joined in the discussion, saying that Apple and Google could use their "wizardry" and "invent a kind of secure golden key they would retain and use only when a court has approved a search warrant."

But as EFF's Jeremy Gillula explained, "there is no such thing as a key that only law enforcement can use—any universal key creates a new backdoor that becomes a target for criminals, industrial spies, or foreign adversaries," and can be stolen.

This idea of a backdoor for law enforcement is a bad idea now as it was when it was first trotted out in the '90s, and it's the infosecurity community's duty to speak up against it again and again and to try to make the point across.

So far, there hasn't been a concrete proposal on how this thing could be accomplished, but when (if) one is presented, it's important for security experts to offer technical critiques of this and any other proposal to weaken security.

It's also critical for the infosec community to offer concrete input on the negative effects of security-related export restrictions, Hofmann says, and they have an opportunity to do so right now, as the US Department of Commerce has recently published its proposed implementation of the December 2013 changes to the Wassenaar Arrangement regarding intrusion and surveillance software, and has asked for the public to comment on it.

As always, there are four forces that exert pressure on what security looks and will look like: norms, the market, the architecture, and the law.

Encryption has become widespread and easy to use by default and, what's more, expected by consumers. Privacy and security have become selling points, and have and are likely to lead to more re-assessments of business models. Business opportunities in encryption-friendly countries have blossomed.

The biggest force the security community is now running against is the law.

As providers are working on making it so that they can't be pressured by law to give access to encrypted data, the government and law enforcement have been forced to shift the pressure on users.

Ultimately, that doesn't work as well, and they are actively working on shifting the pressure back onto the providers.

Aside from critiquing flawed proposals, the security community, tech companies and digital rights activists have the possibility - and, I would say, the obligation - to put forward legal challenges to laws that could hurt users,

researchers (see the aforementioned Wasseenaar Arrangement) and others.

It all really comes down to what kind of world we want to live in, says Hofmann.

She comes down on the side of strong encryption, but is conscious that online security is a fight that will probably have to be fought again and again, and that's why it's important for the security community - as the civil libertarians in the first crypto wars did - to keep fighting.



### Future attacks: Hiding exploit code in images

Successfully hiding messages in images has already been done, but is it possible to deliver an exploit in one - and run it?

Saumil Shah, founder and CEO of Net-Square, has demonstrated at Hack in the Box Amsterdam 2015 that it's possible, and has posited that such attacks are more than likely to crop up in the near future, as he can't be the only one who thought about this, tried it and succeeded.

His research was motivated by his love of photography and browser exploits, and his desire to explore innovative means of exploit delivery. The advantage of using steganography for this is based on the fact that, if done right, the message is completely hidden and, as he pointed out, "you can't stop what you

can't see." Also, what could be more innocent than a lovely image?

He is not the first one to try and hide exploits in images. But he created Stegosplit, a technology that lets attackers deliver executable JavaScript code via images, and trigger them, too.

The technology opens the door for attacks executed as simply as pointing users to sites containing a booby-trapped image or delivering the image via email. By virtue of simply viewing the image, the exploit code is triggered and can deliver malware on the victim's computer.

"A single file can be rendered as a perfectly valid HTML file, executed as a perfectly valid Javascript file, and displayed as a perfectly valid image, all at the same time," he explains.

"Stegosploit is the result of malicious exploit code hidden within pixels of the image carrying it. The image however, is a multi format container, which also contains the code required to decode the steganographically encoded pixels to execute the exploit."

This type of attack won't show in network traffic, he pointed out. It will be invisible to the naked eye, and the image will "autorun" in the browser. In order to make the attack payload look harmless and not trigger defenses, Shah split it into two parts: dangerous pixel data (exploit code), and a safe decoder.

Exploit code is encoded into the bit layers of an image's pixels - the result is called Imajs (a combination of image and JavaScript), and they work on browsers that support HTML5 Canvas (current versions of Mozilla Firefox, Google Chrome, Internet Explorer, Safari, Konqueror and Opera), which allows in-browser decoding of steganographically encoded images.

As far as he knows, no means of malware detection have been able to successfully identify these images for what they are.

Shah has been experimenting with encoding exploit code in JPGs and PNGs. PNGs are better for this, he says, as JPGs have a problem with compression and, therefore, losing information vital to make the exploit work. But

still, JPGs are way more popular, and there is a way around the "lossy compression": iterative encoding.

In addition to all of this, the exploit code delivered via an imajs can be triggered months after the file is received or seen. "We can 'time-shift' payload delivery using caching," Shah added. This could turn out to be a digital forensics incident response nightmare - how far would you go back to search your logs for evidence about the attack? And how would you find it? For all effective purposes, the entire file is a valid image file.

A temporary quick-fix prevention of this kind of attack can be to re-encode all images - resize them, turn them into BMPs and back, etc. This is one of the reasons why the exploit wouldn't work if the imajs was uploaded to Facebook - the social network automatically process the images, and this would result in information loss.

But the real, definite solution will have to come from browser developers, and soon, he noted.

For more details about his research, you can check out the talk slides or, better yet, the video of a previous talk on the same subject Shah gave earlier this year on SyScan'15 Singapore (note: at the time, he still hadn't managed to embed both the attack code and the decode in the image).



## IoT is full of gaping security holes, says Shodan creator

John Matherly's Shodan, a search engine that finds Internet-connected devices, can be used for many things: gauging the impact of policies and network security efforts (e.g. patching), finding malware C&C servers, checking how a company we want to do business with is handling security, checking which devices our competitors are deploying (market research), and much more.

For Matherly, Shodan is a means to measure things that couldn't be measured before. And with the advent of the Internet of Things, the available searchable data set will keep growing day by day.

"The Internet of Things is happening. The world is becoming hyper-connected, whether we want it or not - security be damned!" Matherly pointed out to the audience at Hack In The Box conference.

An Internet connection is being added to "pretty much everything," whether it's a good idea and or not. "Who needs to Tweet from their fridge?" he wondered aloud, but admitted that sometimes an Internet connection for certain devices can be helpful.

Securing the Internet of Things will be an enormous endeavor, but it has to be done. The stakes are much higher - security failures can lead to serious real-world consequences.

Still, making administrators take unsecured IoT devices offline or securing them well is difficult, as Shodan can't really tell who's their owner (dynamic IP addresses tell you little).

But, generally, manufacturers are still not that interested in security, he says. Many of the IoT devices they create are accessible over the Internet by default, often so that updates can be easily delivered and problems fixed remotely. Effectively, they open a backdoor to the device, without the users' knowledge.

Connecting to these devices is also often executed via insecure means. For example, the popularity of telnet for remote logins is still high, even though it provides no traffic encryp-

tion, (usually) no authentication option, and has many vulnerabilities.

Most users fail to realize that IoT devices - fridges, TVs, thermostats, cameras, billboards, and so on - now come with computers inside them, which means they will have many of the problems "regular" computers have. They see the fact that they are connected to the Internet as a great functionality, and fail to realize the dangers it brings.

They do not think about the huge amount of data these computers collect: usage data, health data, and more. It's interesting to note that users are usually not comfortable revealing some of this data to a person, but they are somehow comfortable giving it up to a computer.

They also fail to realize that this data is sold and used - anonymized, to be sure, but anonymization is not foolproof, as we're finding out - and occasionally stored in databases in the cloud without any protection, there for the taking for those who know how to find it.

And even if some users are worried about their privacy, and avoid having these devices in their home or on their person, there is little they can do about IoT devices that are not theirs and surround them when they walk down the street or visit a mall - cameras, trackers, beacons.

As an example of what data can be found laying around, and how easy it is to collect it, Matherly used Shodan to find license plate capture cameras all over the US. And given that many of them store these images insecurely in the cloud, he managed to create a database of over 63,000 license plates in mere 5 days.

He stopped there, and notified the authorities about this problem, but found out that they knew already - they have been told about it by other researchers years ago. And nothing has changed.

"IoT is still full of huge, gaping holes everywhere you look," he concluded.



## Rethinking security: Securing activities instead of computers

For many people involved in the infosecurity community, the notion of security is too often tied to the quality of code (resistance to specific classes of bug, for example) and effective patching - in short, to low-level security. But independent security consultant Eleanor Saitta believes that software developers and security engineers need to take a step back and look at the bigger picture.

"Security is not a property of a technical system," she noted in her talk at the Hack in the Box conference. "Security is the set of activities that reduce the likelihood of a set of adversaries successfully frustrating the goals of a set of users."

Software development teams that understand what users want and what adversaries they face are very rare, she noted. And security engineers forgot - or misunderstood - what their job is: not securing computers, but securing activities that lead to the realization of greater goals.

Nowhere is that more obvious than in situations high-risk users face, for example partici-

pants in the Occupy movement or dissidents around the world.

Saitta realized that a lot of what we know in the security world can't be effectively used if someone in the real world is targeted by a determined adversary.

As she vividly put it: if you're on a rooftop, trying to get a connection and successfully send out an encrypted message because your life or freedom - or that of others - depends on it, and you know that there are snipers waiting to take a shot at you - there is simply zero room for using a tool as complex as PGP.

"We forgot that our job was really to stop bad things from happening to good people," she pointed out.

Security tools should be created with users' needs in mind. We shouldn't work on assumptions or go by intuition - we should set aside our egos, and consult with the end users - learn about their goals and adversaries.

So, how do we go about doing that? The answer is: in an organized manner - with threat modeling, adversary modeling, and operational planning.

"A threat model is a formal, complete, human-readable model of the human activities and priorities and of the security-relevant features of in-scope portions of a system," Saitta defines. "An engineering tool that will help use define what we are trying to get the system to do."

Building a good threat model is not a trivial task, she warns, and that's why it's not done often. But there are tools out there that can help with this task, and already documented models that can be customized.

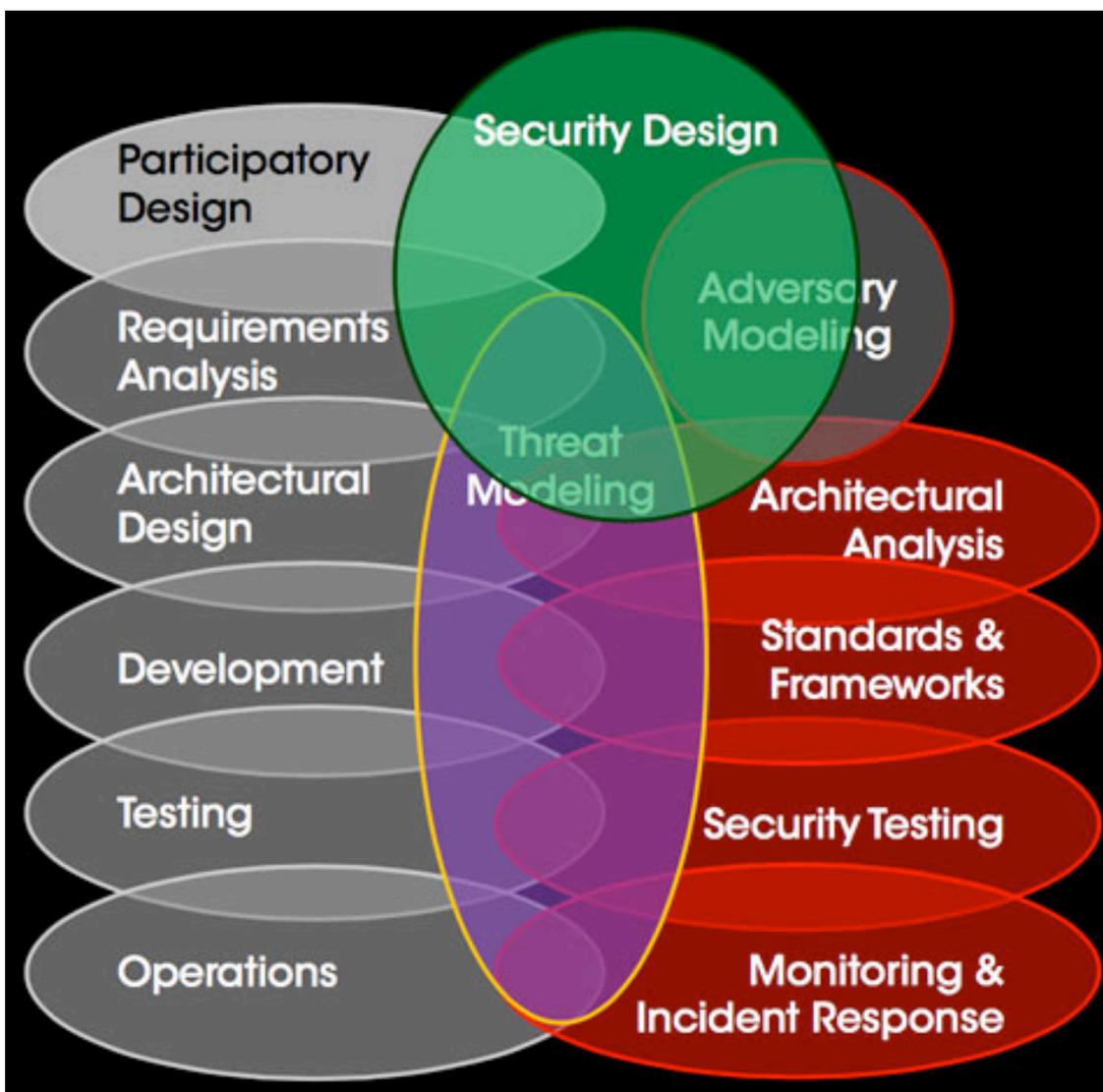
Operational planning will help us detail other things we need to take in consideration, such as resource management, risk analysis, and a whole set of different practices (task domain, communication, community, and so on).

Here is where we choose which invariants - things that systems attempt to maintain - are important to us: simplicity, confidentiality, availability, integrity, deployability, trust, interoperability, and many, many more.

The thing to keep in mind, though, is that every invariant has a planning cost, and influences other variants. In general, the fewer invariants, the easier the process.

Here is also where we make the important decisions: sometimes, for example, speed will be more important that security, effectively making a "bad" solution better than a "good" one. In the case of high-risk users, usable security is a must.

Threat modeling is where development and security engineering meet:



But for the mapping of the security task to be truly effective, we also need to do adversary modeling, and bring in users to have a say about the design of the solution.

All of this things together make for effective security design, and this is what we should be striving for, whether or not our solutions are meant for high-risk users.

## How to raise users' expectations about security and privacy?

Users do not seem to care much about privacy and security. When buying a new smartphone, for example, they rarely ask about security updates and how long the device will be supported. When downloading a new app, most of them don't even glance at the permissions it asks.

They effectively don't ask for security and privacy, and those two things consequently slip down the tech developers' and creators' list of things that are important when creating new "things".

"Nobody starts developing by saying 'let's make a secure product'," Runa Sandvik, security and privacy researcher and technical advisor to the Freedom of the Press Foundation, pointed out in her closing keynote at the Hack in the Box conference. "Security is not 'sexy'."

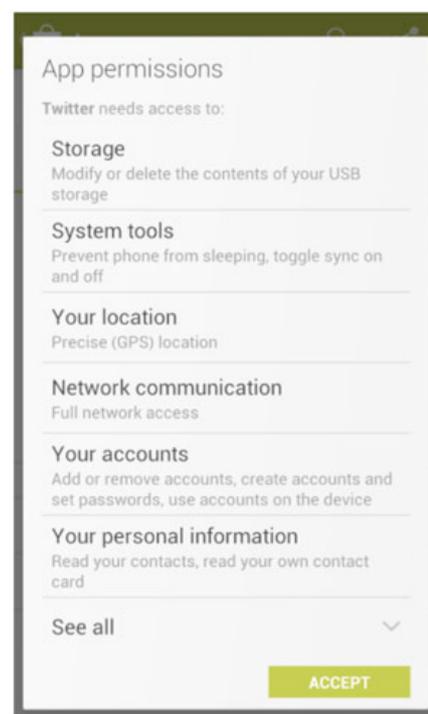
So do we make it sexy? How can we return the discussion on privacy and security? How can we re-calibrate users' baseline security expectations about online services, mobile devices, security cameras, and other Internet-connected devices? A group that could help change those expectations is the media, by shying away from sensationalistic pieces and poorly explained buzz-words like "NSA-proof."

Hackers are also partially to blame for this current situation, she believes: vulnerabilities are released to the world complete with a snazzy logo and fancy website, hackers become a brand, they change the way they interact with journalists and share their knowledge, they overhype the threat, and they are occasionally irresponsible.

But ultimately, it's the companies that should do most of the work, by changing what they make. Citing the example of Linux-powered rifles, she pointed out that just because one can make something, it doesn't mean one should. They should also change what they advertise and keep the focus on security features. Services should write clear security and privacy policies. When more and more of them effect this change, expectations will

change.

The public is slowly coming to the realization that their data has value. RadioShack selling customer data when they promised they wouldn't, Adult Friend Finder failing to protect sensitive data as it was expected of them - these incidents have been an unpleasant wake-up call for many. When it comes to changing users' behavior and use of devices and services, it's important for companies to clearly state the "rules of the road". "Transparency is key," she noted. When it comes, for example, to app permissions, this is not enough (why, exactly, are these permissions needed? There is no context):



Another important thing to remember is that you can't tell users what not to do - they will do it anyway if they really want to. Instead, companies should teach them how they can do what they want safely. Finally, introducing security requirements into contracts could also help raise security expectations.

Sandvik is aware that there's never going to be a privacy utopia. But if all those groups push in the right direction, and users attempt to explain their needs in a language companies can understand, definite improvements can be achieved.

A black and white photograph of a city at night, featuring several tall skyscrapers with illuminated windows. In the foreground, there are light trails from moving vehicles on a road, creating a sense of motion and activity. The overall atmosphere is modern and urban.

# Trusted Identities | Secure Transactions<sup>™</sup>

For Citizens, Consumers & Enterprises

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible.

To learn more, visit [entrustdatacard.com](http://entrustdatacard.com)





## Avoiding an IT disaster: Smart security for smart meters

by Richard Moulds

**After being labelled the “Government’s next IT disaster,” it would appear that not everyone is sold on UK government’s plans to roll out energy smart meters across the country. The smart meter scheme looks to install as many as 100 million smart meters in homes and businesses across the UK by 2020, giving consumers near real-time information on energy use, enabling new pricing models and incentives, all with the goal of saving money and reducing emissions.**

In a recent report titled “Not too clever: Will Smart Meters be the next Government IT disaster?” the Institute of Directors (IoD) said the scheme was “unwanted by consumers, devoid of credibility and expensive.” One of the main points to support the IoD’s objections to the scheme was that issues around cybersecurity remain unaddressed, especially when 56% of UK residents expressed their concern over smart meter data privacy.

The IoD is right to raise these security concerns. Poorly protected credentials and data stored inside smart meter devices leave them vulnerable to tampering, allowing attackers to manipulate energy use figures, cut off the power of specific meters and, in severe circumstances, even take them over completely. We have seen this happen in Spain already, as researchers revealed how easily hackers could fool the nodes sitting high in the power

distribution system to send false data to energy providers and consequently under-report energy use or divert billing to other users.

Whilst guidelines aimed at improving the security of smart meters have been set, is this enough to prevent determined cyber criminals from bypassing protections?

### **A connected tomorrow**

Improving security measures and protecting smart devices from targeted, sophisticated cyber-attacks and data breaches is becoming a more pressing issue as we face an increasingly connected world. From thermostats to fridges, cars to baby monitors, more and more everyday items are becoming connected to the Internet.

In fact, Gartner has predicted that in 2015, smart cities will use 1.1 billion connected “things,” with smart homes and smart commercial buildings representing 45% of this total (around 500,000). In 2017, this last number is expected to rise over 1 billion, with consumers introducing smart LED lighting, smart locking and smart TVs into their homes. All of this falls under the now rather overused term the “Internet of Things,” or IoT.

The more connected our technology becomes, the more data our devices and appliances can collect about us. The scale, complexity and geographic spread of IoT networks, coupled with this huge amount of data that passes through them, make smart devices very attractive to cyber criminals. Of

course, hacking light bulbs isn’t perhaps the most rewarding activity but there’s plenty of other situations where the prize is much greater. When you consider that personal data such as credit card details, health monitoring and geo-location records - not to mention high-value intellectual property and information, or commands driving critical national infrastructure systems - pass through the IoT network, it is no wonder such security risks are cause for concern.

The main reason for these fears is that the devices themselves often have very little protection, and this makes them a prime target for malicious hackers and cyber criminals. Even the most minor glitch or breach would have severe consequences.

## **The scale, complexity and geographic spread of IoT networks, coupled with this huge amount of data that passes through them, make smart devices very attractive to cyber criminals.**

Both the wider industry and the government need to look to technologies such as Public Key Infrastructure (PKI), a tried and tested method that has been used for years to secure communications. By encrypting data and using digital credentials to identify web sites, devices and users, PKI can determine access to sensitive systems and protect data from unwanted intruders. Tied to a pair of cryptographic keys, these digital credentials are kept safe, with the keys only able to be used by the device or user to which they belong.

### **Smart solutions for smart meters**

The smart meter plan has become a one-too-many trust issue. One organization interacting with millions of customers now becomes one

electric utility interacting with millions of smart meters. Mutual authentication, secure communications and high integrity messaging should become the core security foundation on which the proliferation of connected things and smart devices is based.

The government needs to take this into account if the smart meter scheme is to be successful in the connected world of tomorrow. The industry and regulators needed to start thinking and acting more quickly and sharply if they don’t want to leave the door wide open for cyber criminals. By putting security at the forefront of these smart devices, the government can avoid an IT disaster and instead enable consumers to take advantage of the benefits this smart technology offers.

Richard Moulds is the VP Strategy at Thales e-Security ([www.thales-eseecurity.com](http://www.thales-eseecurity.com)).

# Introducing **TITUS Classification Suite 4**

Flexible. Powerful. Secure.

---

## The Industry's Most Advanced Data Classification Solution

TITUS Classification Suite 4 offers an unprecedented level of flexibility and control to make your information protection program a success. From advanced data identification to fine-grained policy control, TITUS provides a security framework to protect your organization's most valuable information assets.



For more information visit [www.titus.com](http://www.titus.com)



## The standardization of tokenization and moving beyond PCI

by Ulf Mattsson

**Most of us strive to raise standards, to address more use cases, to deliver more interoperability, and to improve our knowledge through education and interaction with peers in our chosen profession. We also seek industry benchmarks to help us set goals and measure our performance.**

Having worked with several tokenization standards bodies in recent years, it has become clear that the case is much the same in the technology industry. Organizations look to deliver more advanced services to enable colleagues and customers while vendors are quick to respond with promises of best-in-class improvements and state-of-the-art innovation.

This seems especially true in the rapidly evolving cybersecurity space, with increasing numbers of start-ups and specialists all proclaiming that they are setting the bar to which others must aspire, that responsible organizations must pin their reputations to in these times of unprecedented digital villainy and revolution.

As CTO of a data security software company I stand guilty as charged because I believe in the need for such solutions and our ability to deliver. However, my role gives me empathy for the dilemma faced by many of my customers – how can we be sure which technologies

are right for our enterprises and go beyond standard to be exceptional?

The data security industry has never been one of such uncertainty as it is now. Headlines inform us daily of bigger threats, greater vulnerabilities and increasing amounts of red tape, so we increasingly look to strengthen our defense strategies with a data-centric approach to security.

Encryption has been the go-to technology for protecting data itself but organizations are increasingly adopting tokenization in order to secure their sensitive data without compromising in ways associated with traditional data protection.

Tokenization is a data security method that replaces sensitive data with fake or neutral data; it provides equal or better security than encryption and can retain data characteristics vital for business processes. Tokenization, however, is experiencing the same rites of passage as any other technology. There are many different models of tokenization, each

addressing a slightly different use case with more start-ups and experts, each claiming to offer the best solution and again leaving CTOs perplexed and wondering – how can we be sure?

We are seeking a benchmark to aspire to and go beyond.

One proposal that would set standards to alleviate concern is Tokenization Standardization. An open and universal tokenization standard could help to ensure sensitive information will be more secure throughout its lifetime.

If we look back at the evolution of encryption we can see that standardization was central to its mainstream acceptance by organizations regardless of vertical across the globe in a bid to advance and excel securely.

As RedHat put it in their security blog, “In 1973, the Nation Bureau of Standards (now called NIST) in the US put out a request for proposals for a block cipher which would become a national standard. They had obviously realized that they were buying a lot of commercial products without any good crypto support.”

Thirty years ago we were seeking similar reassurances as we are today. In 1977 a NIST backed encryption standard gave organizations the confidence to implement the technology internationally. In turn, widespread adoption of the standard led to advancements in data security as the industry sought to improve on the benchmark.

Despite the controversy that surrounds encryption today (NSA scandals), without these standards our data would not be as safe as it is currently. Many authorities consider encryption central to their data security regulations. Compliance with regulation is yet another driver for innovation.

Encryption of cardholder data is integral to the PCI Data Security Standard but the logistics of compliance have proved to be complex and unwieldy, disruptive to business processes and costly to audit.

Innovators set out to overcome these challenges in order to simplify compliance and reduce the associated costs and difficulties. The

result was tokenization. By substituting a non-sensitive equivalent for PCI data wherever possible throughout the enterprise, organizations can ensure data security and shrink the scope and expense of their compliance audit. The PCI community was swift to realize that while data encrypted with traditional algorithms has no business value and must be unprotected to be useful, in contrast preserving the format and essential business intelligence of the original data in the non-sensitive tokens, business processes and analytics may continue undeterred.

The PCI Security Standards Council endorsed tokenization technology, releasing guidelines for use in 2011, and this has resulted in a flurry of new tokenization technologies emerging, each addressing its own particular operational complexity and bringing unique advantages.

Tokenization can be a cost effective alternative or complement to existing encryption solutions and many organizations that are managing encryption products already have the skills required to employ this new technology. However, interoperability, performance and scalability are important factors for organizations with large or decentralized operations considering tokenization.

This technology is now available in-house either vaultlessly or vault-based, in the cloud via a gateway or as a service, and provided as a feature by payment providers and other third-parties. NFC-based mobile and contactless payments such as Google Wallet and Apple Pay use tokenization technology.

This diversity has in turn led to several standardization efforts, regulations and guidelines as business and technology stakeholders endeavor to protect the sensitive data they and their customers are increasingly generating.

Tokenization is currently involved in a standardization effort conducted by ANSI X9, the department responsible for the industry standards including payment card PIN management, credit and debit card encryption and related technologies and processes for financial cryptography and data protection.

In October 2013, EMVCo, a payment industry organization operated by MasterCard, Visa,

American Express and other payment networks, proposed a new framework for digital payments. The purpose of the framework was to provide specifications for a payment tokenization solution benefitting acquirers, merchants, issuers, and cardholders.

The initial version of the framework, published in March 2014, seeks to facilitate development of more secure payment technologies while maintaining compatibility with the existing payment infrastructure. This framework is building a more secure system for replacing card account numbers in the authorization of mobile payments using various devices, channels and types of merchants.

Despite these efforts to set standards in the validity and security of tokenization, it is not enough. Standards should also address the interoperability of differing tokenization solutions. Data tokenized with one service should be able to migrate to a different service without translating the data.

For example, EMV tokens are based on protocols different from other tokenization technologies and this leads to incompatibilities between systems. So potentially, those using Tokenization-as-a-Service and receiving EMV payment tokens from other sources may store multiple tokens for the same card number and thus need to map the different token schemes to each other. Large mapping tables may be required to make accurate analytics possible and some tokenization products would require highly available master or replicated databases. Other approaches are based on static mapping tables that can operate in a distributed network with replication between tokenization servers. These complexities are in conflict with the simplicity tokenization was initially developed to provide.

So now CTOs are asking a new set of questions. How can I be sure tokenization is secure? How can I be sure different token schemes will map together seamlessly across the enterprise? How can I be sure to avoid duplication and guarantee consistency?

In a bid to make answering these questions more straightforward, the Food Marketing Institute, Merchant Advisory Group, National Association of Convenience Stores, National Grocers Association, National Restaurant Association, National Retail Federation, and Retail Industry Leaders Association came together to call for the creation of a set of interoperable open standards for tokenized payments that would be managed by an independent body such as ISO or ANSI — rather than by the payments industry.

Merchants would also like ANSI or ISO to create an open standard covering private and personally identifiable information.

It's important to consider why merchants are calling for these measures. They believe that tokenization can ensure sensitive personal information protection beyond just payment card data. It can be applied to all types of data.

As consumers and professionals we are generating sensitive data at an exceptional rate in our interconnected world; as organizations we are keen to learn from it and share it; as data custodians we are obliged to protect it.

Just as “Privacy by Design” is a long term goal to securing and evolving the Internet of Things (IoT), ensuring an open standards process should be considered essential for the development of tokenization solutions which will easily and efficiently integrate with all hardware and software business environments, and which will be appropriate for all sensitive data.

These approaches are important for long-term development of solutions, but we urgently need to address changes in the threat landscape. These systems are increasingly collecting large volumes of sensitive data that will flow in to the cloud and big data. This is an issue that we need to solve from a data breach and compliance perspective. A data centric security approach can address these issues and we can start today by using best practices that are available.

Ulf Mattsson is the CTO at Protegrity ([www.protegrity.com](http://www.protegrity.com)). He is widely considered one of the founding fathers of tokenization and is an advisor to the industry's top analysts and stakeholders. Ulf is the inventor of more than 20 patented technologies in the areas of encryption key management, policy-driven data encryption, internal threat protection, data usage control and intrusion prevention.



# THE ULTIMATE THREAT INTELLIGENCE AND TRUSTED COLLABORATION PLATFORM

Your SIEM needs our intelligence. Level the playing field. Use the ThreatStream OPTIC™ platform to aggregate millions of unstructured cyber threats while gaining real-time visibility into your existing security infrastructure, and enable trusted collaboration through a community-vetted threat sharing platform.

Learn more at [www.threatstream.com](http://www.threatstream.com).

# 10 practical security tips for DevOps

by James Brown



**A lot of organizations are embracing DevOps and automation to realize compelling business benefits, such as more frequent feature releases, increased application stability, and more productive resource utilization. However, many security and compliance monitoring tools have not kept up. In fact, they often represent the largest remaining barrier to continuous delivery.**

By working with the DevOps team, you can ensure that the production environment is more predictable, auditable and more secure than before. The key is to integrate your security requirements into the DevOps pipeline; however, as part of that integration you will need to change the way you work.

A normal approach of checklists, templates, manual processes, etc. will not scale. With the speed of cloud deployments, you will need to automate and use tools and scripts. This will allow you to move as fast as the DevOps team needs you to.

You will hear the concept of “Infrastructure as Code” within DevOps. This is where the platform infrastructure is stored as a set of scripts that can be executed in a repeatable way. Security needs to be looked at in the same way, by moving to “Security as Code” or “Software Defined Security.” By moving from a legacy procedure in a Word document to a set of scripts, we can automate that document which means that it can be executed in a repeated and predictable way - it can be included into the DevOps pipeline. The benefits will start to show immediately. By automating many of the tasks, not only can you check that the DevOps pipeline has the security and compliance controls that you need, but you

can also run those scripts across production to ensure that the environment has not drifted. In an automated world, those checks can be run multiple times a day.

For security professionals it is key to understand that instead of validating the end solution you need to validate the pipeline. If you are happy that the pipeline is building the solution in a way that meets your security goals, you can be confident that this will be repeated every time a developer needs to get source code into production.

## 1. Architecture and design

During the architecture and design phase, the development teams will be attempting to rapidly iterate against the requirements whilst building out the Cloud infrastructure. It is at this point that security teams need to get involved to understand the scope of what teams are looking at, and that different elements of the infrastructure need protection in different ways. Learn and understand the shared security model - Amazon S3 is very different to protecting storage on IaaS instances, the barriers between IaaS and PaaS are rapidly breaking down, and each has a different security paradigm. Threat modeling can be done against the different components. This will allow

security teams to define the threats against the different components, and what elements are going to be needed further up the DevOps pipeline to secure them.

**ACTION:** Work with the architecture to understand the cloud components being used, and the security controls required for each. Take this further by using techniques like threat modeling.

## 2. Static code analysis + code reviews

Code reviews are a common part of DevOps. The security team should educate colleagues on secure coding techniques so that they can include this into their secure code reviews. However, many of these items can be validated by using static code analysis. This is where the source code or a partially compiled version of the source code can be checked for potential vulnerabilities. Many potential security vulnerabilities can be picked up at this point, and if they fail the checks - it breaks the build. Developers will quickly change coding techniques to meet the requirements.

**ACTION:** Understand what the current code review process is and ensure that there are security elements within that. Likewise investigate what static code analysis tools are available and if they can be used.

## 3. Audit of Chef scripts / CloudFormation scripts

You will hear the phrase “Infrastructure as Code” a lot in the DevOps world. This is where the infrastructure is built in a highly automated way using scripts and configuration files. The advantage of this for a security professional is that automated checks can be run against these scripts. If a developer creates an infrastructure script to create a storage bucket with public access to the internet, this can raise an error. Combine this with the threat modeling where you have identified potential issues and you have a very powerful tool to validate the infrastructure every time a developer makes a change.

**ACTION:** Use the automation tools to ensure that the infrastructure is being built to meet the security standards.

## 4. Security testing post build

Automated builds and unit tests running after check-in are a core part of DevOps. This is where security teams can add-in security testing tools to automate the validation of the build. The reason why automated build and testing is so key in DevOps is that the shorter the time between a developer checking in code and a test failing - the less time it will take for the developer to fix the issue. The same holds true for security vulnerabilities, running testing at the end of the project can inject significant delays as developers struggle to identify the issues and fix the bug. Identifying the issue within minutes of a developer checking the code in reduces the time taken to identify and fix the issue.

**ACTION:** Investigate automated security testing tools and integrate them into the build process.

## 5. Harden your OS deployment

Let’s move from “Infrastructure as Code” to “Secure Infrastructure as Code.” If you are creating and building servers via scripting, also add the scripts to lock down the box as well. The risk of applying OS hardening at the end of the project is that the application stops working. If it is applied at the beginning of the project, firstly, issues are identified up front, and secondly, if the hardening has to be relaxed, it can be identified early, and security teams can work with the developers to find another way of performing the function. If it occurs late in the project, the development team will force the issue through if they can’t find a good solution.

**ACTION:** Review the automation scripts to ensure that the OS is being deployed in a secure way and any changes to this standard are controlled. Use resources like the SANS Linux Security Checklist or CIS Benchmark.

## 6. Harden your cloud deployment (standard AMIs, Security Groups, IAM roles, MFA tokens)

Cloud services can deliver incredibly secure infrastructures *if* done correctly. However it is also very quick and easy to open up security

holes. You need to review how your company is using the cloud. This includes the segregation of roles – do your developers have the rights to change the production environment? If so, why? I am sure you do not let your server administrators walk around using Domain Admin accounts; so why should developers have root access in the AWS Console? You need to review everything from the development environment through to production.

**ACTION:** Review how teams are accessing the console and what permissions that they have. People should only have the permission they need to do their job, and if they have significant permissions they should be using two factor authentication.

## 7. Deployment of security tools

Once you get to deploying applications to production, are you going to be able to keep up with multiple teams deploying multiple applications to production? In the same way you can use automation to ensure that security is as you require it, you can ensure that your security tools are deployed at the same time.

You should be looking at deploying network detection for threats on your network, monitoring of HTTP for attacks as well as monitoring log files. There are solutions that allow you to monitor these three different feeds as well and at the same time have a 24x7 SOC investigate the threats and escalate if required.

**ACTION:** Script the deployment of your security tools so that all environments have a baseline coverage.

## 8. Vulnerability scanning of OS and applications

One of the most common attack vectors is exploiting the vulnerabilities in the OS or applications that are running on the servers. As part of a DevOps pipeline, servers can be checked for vulnerabilities. In addition, you can use a solution which has an analytics engine. Then this information feeds into it, allowing potential attacks to be rated with the additional data of what software you are using; this will help reduce false positives.

**ACTIONS:** Run regular vulnerability scans against the environments and remediate any vulnerabilities.

## 9. Phoenix upgrades

Instead of deploying patches to production, you should be burning and redeploying servers as required. This not only increases your agility to roll out new versions, but also increases your ability to rapidly respond to security issues. You can deploy a new patched version across your entire cloud environment rapidly and safely; and with the “phoenix upgrade” strategy you also reduce the risk of technical debt and configuration drift.

**ACTIONS:** Work with the DevOps team to support those using phoenix upgrades and ensure this gives you the ability to patch security issues and roll them out.

## 10. On-going and real time audit of the production environment

Visibility post deployment is often down to the level of auditing that has been put in place. You should have standard auditing levels across different server roles and applications. Your goal is to get a level of auditing that can be fed into a security tool to provide the data that is needed, but not swamp your servers with too much auditing. Once all of these elements are in place, it will allow you to audit production to ensure that at any point in time you understand what state production is in, and if it has drifted from its defined security profile. The cloud is often referred to as a programmable datacenter. Developers can use it to create huge IT systems in very short timeframes, and you can use this same power to audit these systems multiple times a day.

**ACTION:** Work with the development team to set logging levels and use a tool like Chef to ensure that your configuration does not drift.

The evolution of DevOps should be extended to embrace security – providing speed and agility to securing critical applications, assets and services in a more predictable, auditable and secure way.

# Your Data is Showing... *What's your Plan?*

Enterprise organizations are in possession of more sensitive information than ever before and data breaches are inevitable. The new priority of CISOs around the globe is how to "secure the breach" so organizations can ensure that any data obtained from a breach is encrypted and therefore useless.

Learn how to  
Secure the Breach in 3 steps!

[www.securethebreach.com](http://www.securethebreach.com)





## Identifying the insider threat with Steph Charbonneau, CTO at TITUS

Interview by Mirko Zorz

**In this interview, Steph Charbonneau, CTO at TITUS, talks about what global organizations can do in order to realistically address the insider threat, and offers advice to CSOs in large organizations.**

### **What are some of the often overlooked behavioral indicators of malicious threat activity coming from within an organization?**

Identifying malicious insiders can be very difficult for organizations. These insiders have usually been at the organization for several years, and carry out their attacks over an extended period of time. They typically leverage their authorized access to information, files, etc, and more often than not they act on their own.

From time to time, co-workers may first notice that there is an issue. For example, they may notice a co-worker printing a large number of confidential documents, or an employee actively trying to work around security controls. Associating visual markings and security warnings to user activity can help to notify co-

workers and managers to any suspicious behavior.

Typically, it's the everyday behavior that organizations need to monitor – the activities that users are authorized to do, but that can be tracked to identify anomalies over time. With technology such as data classification, activities carried out by users as they work on email and documents can be monitored, tracked, and analyzed for any anomalies.

**While organizations need to share data in order to function efficiently, it's a challenge to control the data flow between employees, partners and customers. Since the insider threat doesn't necessarily have to be malicious, but simply unintentional, what advice would you give to CSOs in large organizations that are under increasing**

## pressure to make sure their data stays confidential?

When workers are unfamiliar with correct policy procedures and there are no systems in place to train, inform, and remind them, they engage in risky information handling. Insider breaches are both a technological issue as well as a human and cultural problem. You can install technologies to prevent uploading data to a cloud service, but if your users don't understand the value of the data they are using they are likely to see the technology as an impediment to their workflow, and actively seek methods to circumvent security.

To effectively secure data, senior executives need to set the foundation for a culture of information protection. Executive support is crucial to ensure that any data protection initiatives that are undertaken are followed through with by employees from across the organization. Having this top down approach will ensure that all employees know that senior leadership is behind any initiative.

In addition, organizations also need to engage and involve people further down in the organization as change leaders. Identify some key people in every group of users who can be the experts on your information protection initiative. Users oftentimes find it embarrassing to call up IT for help or advice; they prefer to ask their peers one-on-one. You will diminish user pushback and accelerate implementation if you involve these internal peer champions.

Implementing a technology such as data classification within your organization will assist with the data sharing function, while helping to ensure that sensitive information does not leave the organization – either maliciously or unintentionally. Classifications can be applied as visual markings, which alert end users to the sensitivity, and persistent metadata associated with the classifications helps to inform security technology systems of data sensitivity.

The process of classifying has the added benefit of acting as a constant reminder to workers that the information they handle has

value and its protection is essential. The entire security ecosystem then has the knowledge it needs to manage the information according to security policy.

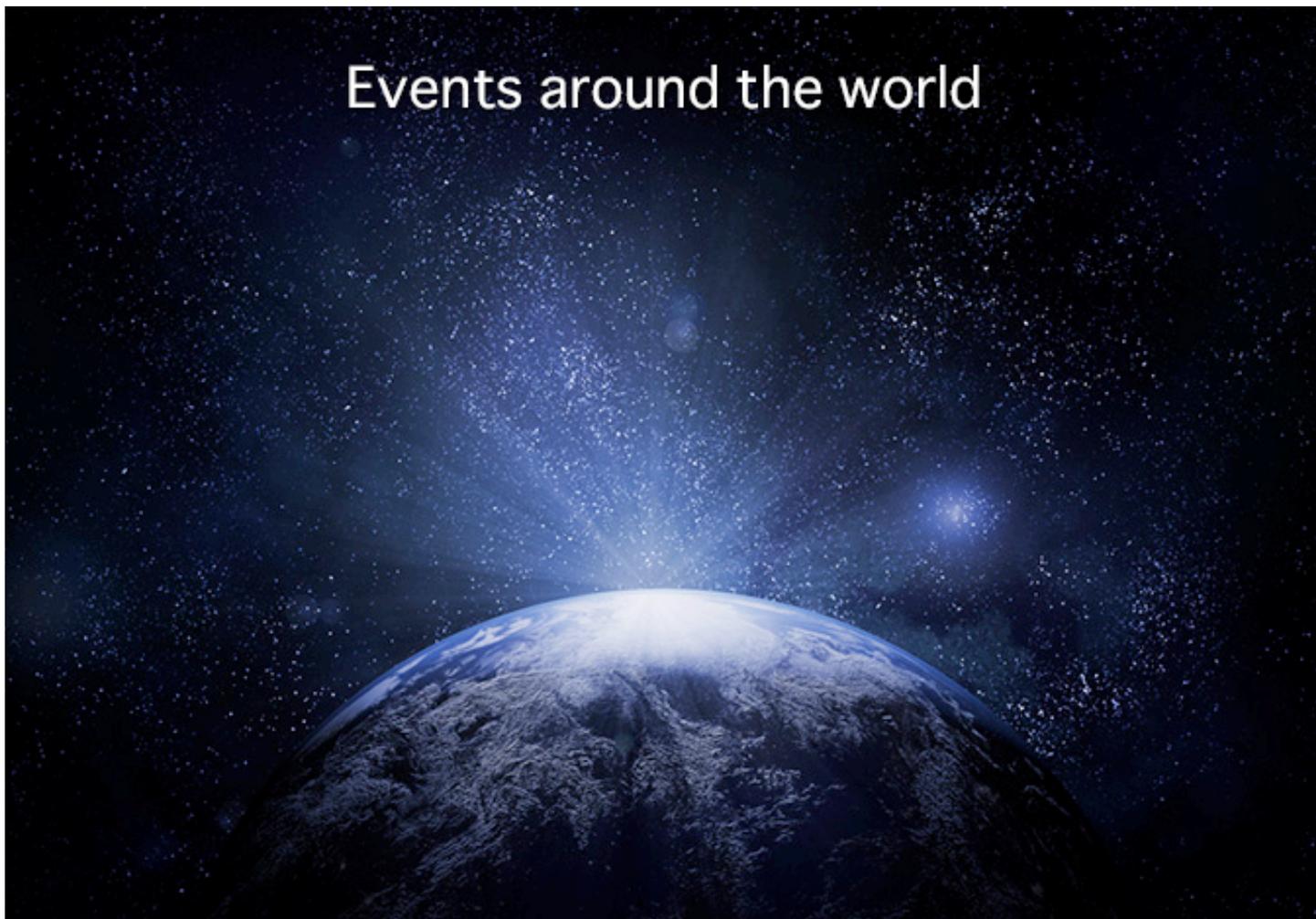
## A myriad of vendors offers products that promise to address this threat. However, preventing a determined insider from leaking data outside the organization is far from easy. What can global organizations do in order to realistically address the insider threat? What deterrent methods work best?

People typically change their behavior when they think they're being watched. It is best to let people know as they are working with the data that they have a responsibility to behave appropriately. Don't overwhelm the user with security enforcement, but let them know that their actions matter and have visibility. If users see messages while they are working which remind them about corporate policy for sharing particular information, they will be more likely to "follow the rules" and ensure that they handle data properly.

Locking things down, on the other hand, makes people find other ways - and then you lose visibility into what they're doing. It's better to provide users with access, and then monitor what they are doing. Ideally, you provide gentle education for the 99% of users who just need some guidance and accountability for safe data handling, and then add enforcement for more targeted use cases where the consequences of data loss are most severe. These varying levels of policy enforcement can go from passive, where you are simply logging behavior, to educational, to blocking and enforcement where necessary.

Organizations can also leverage "insider insight" to fight the insider threat - let users be part of the security solution. Information security should not just be IT's problem – it is everyone's responsibility. Give users the tools they need to practice security, and then reward them when they get it right. This will help you to reinforce the culture of information security across your entire organization.

# Events around the world



## **(ISC)2 Security Congress**

[congress.isc2.org](http://congress.isc2.org) - Anaheim, USA / 28 September - 1 October 2015

Now in its fifth year, (ISC)2 Security Congress 2015 will take place September 28 - October 1 in Anaheim, CA. This conference will offer more than 80 education sessions along with networking and career advancement opportunities.



## **McAfee FOCUS 15**

[focus.intelsecurity.com/Focus2015](http://focus.intelsecurity.com/Focus2015) - Las Vegas, USA / 26-28 October 2015

Attend Intel Security FOCUS 15 (their 8th annual security conference) and get the tools you need to leverage the features and functionalities of the products and solutions you have already invested in and gain valuable insights into other Intel Security technologies that you may not have currently implemented.



## **IP EXPO Europe 2015**

[www.ipexpo europe.com](http://www.ipexpo europe.com) - ExCeL London, UK / 7-8 October 2015

With six top enterprise IT events under one roof, IP EXPO Europe assists the IT Industry in future proofing their IT and embracing a digital future. The event showcases brand new exclusive content and senior level insights from across the industry, as well as unveiling the latest developments in IT.



## EMV's impact on increasing card-not-present fraud: Now what?

by Christiaan Brand

While card fraud has been around for decades, the advent of new technologies and the overwhelming reach of the Internet have only enhanced the methods and frequency of fraud attacks. With the success of wide-spread breaches like the recent Target and Home Depot attacks, data heists have become mainstream and are continuing to impact more and more consumers in the US and abroad.

As a result, the US is finally welcoming a new globally recognized framework for interoperable chip-based payment cards known as EMV. Already deployed across Europe, Africa, Latin America, Canada, the Caribbean and the Middle East, the EMV security standards—named for Europay, MasterCard and Visa—have proven successful in effectively eliminating in-person credit card fraud.

While these nations have seen significant declines in card-present fraud as a result of the introduction of EMV, they have also noted major increases in card-not-present (CNP) fraud as fraudsters focus on the vulnerabilities of this payment method.

In order to successfully conduct a card-not-present transaction, all a criminal needs are a

few basic pieces of information from a consumer's magnetic stripe or chip-based card. Once they've captured this information, fraudsters can conduct transactions by phone, by mail or, most commonly, over the Internet.

As the US prepares to begin its full-scale adoption of EMV, many are worried about the implications EMV may have on online transactions, especially as consumers continue to heavily rely on Internet and mobile technology, such as Apple Pay, to conduct every day transactions. Luckily, there are measures that can be taken in conjunction with EMV to ensure fraudsters are thwarted - in person and during attempted CNP transactions. The key lies in issuers providing better verification processes to ensure the person conducting the transaction is who they say they are.

## Option 1: 3-D Secure

Based on the wide-spread adoption of EMV abroad, many payment industry leaders were able to quickly identify EMV's impact on CNP fraud and determine a solution to the problem. Co-developed by Visa and Arcot (now CA), 3-D Secure is an XML-based protocol that acts as an added layer of security for online credit and debit card transactions and links financial authorization to a user authentication process.

During an online transaction, 3-D Secure momentarily redirects the cardholder initiating the transaction to the issuing bank who then verifies that the cardholder is legitimate through one of several potential user authentication mechanisms. When correctly deployed, 3-D Secure has proven successful in significantly decreasing CNP fraud and has also lowered issuers' operational costs, increased card usage and improved cardholder retention. While 3-D Secure has been met with overwhelming praise in a post-EMV world, it continues to encounter some resistance from online merchants.

Many online merchants worry that 3-D Secure may be too cumbersome for consumers as they are required to authenticate their identity for each online transaction, often times by entering a long password, which many consumers forget. One of the most widely used authentication methods to eliminate this issue is to have consumers authenticate themselves with a one-time password (OTP). OTPs are made up of a long string of digits and are delivered out-of-band, typically by text message or via a hardware token.

While OTPs have been used for decades to authenticate users and their transactions, text messages and hardware tokens are no match for today's advanced fraudsters. The issue with both SMS-based authentication and token-based authentication is that both methods continue to rely on browser-based communication with the bank, which can easily be infiltrated by hackers.

The key to leveraging 3-D Secure technology successfully lies in issuers providing their customers with multifactor, out-of-band authentication that does not rely on browsers for communication with the bank.

## Option 2: Tokenization

In addition to 3-D Secure, tokenization has been offered as the "end-all-be-all" solution for non-EMV transactions, specifically due to the introduction of digital payment platforms, such as Apple Pay. But how does it work?

As a new credit card is linked to Apple Pay via mobile device, the card number is sent off to the corresponding payment network and exchanged for a "token," which will be used in lieu of the card number for all transactions moving forward. However, before the exchange can take place, a real-time call is made to the bank that issued the card to request permission to do so. It's here that many card issuers either succeed or fail at protecting their customers.

Some issuers have created robust identity proofing techniques, which provide customers with a sign-up code via phone or email based on the information they have on file. This means that if someone steals a given customer's card and attempts to link it to their own phone, they will not be able to do so without the necessary code. On the other hand, some issuers have chosen to simply approve each token request blindly, which has resulted in Apple Pay incurring fraudulent charges up to 100 times greater than the industry standard.

Whether through 3-D Secure or tokenization, the main factor in the success or failure of these security techniques is the active participation of the issuer. If issuers can play their part in helping verify the identity of their customers for CNP transactions, it may finally be the end of CNP fraud as we know it.

Christiaan Brand is co-founder and CTO of Entersekt ([www.entersekt.com](http://www.entersekt.com)), an innovative pioneer in transaction authentication. He oversees Entersekt's information technology services, mobile processing platforms and enterprise applications, playing a key role in application development, infrastructure and operations. Additionally, he leads the delivery of Entersekt's cloud and mobile strategies, ensuring that the company is well positioned to address the introduction of new business models and payment types.

# Security Culture Toolkit

Industry Benchmark  
Personalized Actions  
Security Culture Assessment

<https://app.roer.com>



Security  
**CULTURE**  
Framework

*The free and open  
framework to build and  
maintain security culture.*

<https://scf.roer.com>

Security Culture

**SUMMER**  
**CAMP**  
2015

<http://learn.roer.com>



## Identity crisis? Honoring the IAM legacy while taking action and embracing the future

by Rob Faber

**The way we deal with identities is set to change rapidly and dramatically. We will see a strong growth in the use of different channels and devices, from different locations and with different identities, and this will hasten the need to redefine identity and access management. Dealing with identities the right way is essential for doing business safely. So, how do get to a solution?**

A rapidly changing landscape of cloud services, mobile services, apps, and social logins is precipitating changes in the world of identity and access management (IAM). These changes are multiplied by trends like Bring Your Own Device (BYOD) and/or Bring Your Own Identity (BYOI), which add more and more friction to the current situation.

In the past, we only had to worry about the efficiency and effectiveness of identity management in dealing with our own internal (back-end) systems and applications, with internal users located safely behind a firewall. The new reality is a completely different ball game.

It is turning our business into one of partnerships and external relationships, with integrated value chains, cloud- and mobile-based users, and precious data scattered everywhere. Furthermore, there are situations involving distributed ownership and control of resources by third parties (e.g. outsourcing). A closer relationship with business partners and suppliers is required in such cases. But how can we stay in control while giving them necessary access? This article is about the transformation of the identity management landscape, and the impact it will make on current implementations within our companies.

## Why the current situation is untenable

Many predictions have been made concerning the (near) future of IAM. While figures and percentages are sometimes divergent, we can come to some conclusions. Besides the business drivers and trends that will affect organizations, there will be a number of technological developments that will affect IT-intensive environments. It is important to understand this because these developments will lead to changes in configuration, business models, cost profiles and, without doubt, security-related issues.

A few of the most important drivers are:

### Consumerization

The employee-as-consumer will take more and more control. The consumerization of IT greatly affects corporate IT departments, which have set up policies, platforms and security measures to ensure the security of corporate data over a larger number of different types of devices. Still, most organizations have difficulties coping with these changes to security requirements.

### An increasing diversity of equipment

In the few years since the first smartphones and tablets came within reach of the consumer, the sale of these devices has boomed. There has also been a big change in the use of these devices (i.e., more devices, with different form factors), along with a growing overall trend toward being connected anytime, anywhere. We tend to use more devices during different periods of the day; each of them fulfills a different set of needs.

This kind of behavior drives innovation, meaning that the separation between consumers and employees will eventually disappear (if it has not already). There will be a shift from a traditional IT-managed support scenario to a situation where services are more customized and adaptable: a shift from the one-size-fits-all towards the tailor-made.

### Ever-increasing cyber threats

Reports by big vendors and analysts say that potential threats continue to increase, and point out the need for a comprehensive cyber security approach. Both criminal organizations and states have been mounting targeted cyber

attacks. But users are becoming less interested in protection and aware of privacy issues. Add to this the growing ubiquity of smartphones and tablets, and the ever-increasing connectivity, and you can see how the risks organizations face are rising dramatically.

### Always connected

The use of public wireless networks and mobile networks with large coverage areas (3G, 4G, Wi-Fi hotspots) is still increasing. In addition, local wireless services (WLAN, Wi-Fi) are increasingly offered by service companies (e.g. trains, hotels, airports, conference centers) to consumers and thus to our employees. Entry-points will increasingly shift from the trusted office LAN towards untrusted environments and unfamiliar places.

### Cloud computing

Functionalities that were previously offered “on the premises,” within our trusted data center, will increasingly be offered as a service (e.g., mail, telephony, video, basic office functionality, knowledge sharing, collaboration) on the internet, via cloud services or apps. It is also possible to install and provide our own applications to our audience, through an IaaS (Infrastructure as a Service) model. This will drive a shift from “ownership” towards “management” and “governance.” It would be a huge mistake not to have the requisite technological knowledge, or to decide to blindly trust the external supplier concerning security-related measures.

### Fast, cheap hardware, and large storage capacity and memory computing

We have seen an increase in storage and processing capacity, which will soon be available to consumers. IT is also becoming an integral part of all products, with embedded sensors, smart metering, and connectivity. All this is combined with increasingly clever ways to analyze the massive amounts of data produced by these products.

The ability to analyze this data using fast, powerful hardware offers various advantages in the field of business intelligence, along with new business models. For \$2,500, you can have your own “supercomputer” using only Raspberry Pi’s. (You actually can! <http://tinyurl.com/l6cpu62>)

But the downside is that, in many cases, embedded systems are not secure at all (this is sometimes not even considered; ease and comfort are usually the number-one concerns) and big data is poorly protected. Yet this could be the core business of the organization, earning a large amount of money.

### **Commodity service**

The notion that "the workplace has become a commodity" is often heard. The use of devices to do our daily work will increasingly become like having gas, water and light. It is necessary, but it's certainly not a differentiator anymore. However, a significant portion of the IT budget is currently spent on the management of devices, and little of it is left for supporting innovation. This results in a workplace environment that does not meet the requirements of the end user.

In addition to these general trends, there is increasingly more cooperation, co-development and integration between supply chain partners. An evolution in open networks, and making (internet-facing) services available, will encourage extensive interoperability in the value chain. When large systems are opened as services, issues will arise concerning organizational control, governance and security. To conclude, in all the described scenarios, the handling of identities and authentication will be a crucial ingredient.

### **IAM in a changing landscape: The identity of things**

After taking all the aforementioned changes into account, we start to see that IAM is not only about managing the identities of people, but also includes the identities of "things." As a result of these changes, adaptive IAM will enter the market to replace current enterprise IAM solutions. Scalability, deployment ability, and mobility needs are all driving the redesign of most enterprise IAM implementations. Enterprises must be able to view and manage all users (whether enterprise or consumer), but also all "things."

The Internet of Things (IoT) will redefine the concept of IAM in terms of what people own (digital IDs, smartphones), share (profile data, location, authenticators) and use, as well as the relationship between these at any given

moment in time. The artificial borders that exist between internal and external identities (employees vs. customers, partners, and suppliers) will start to vanish. The same services or applications will be used by different target groups; therefore, why have multiple IAM components active that, in the end, control the same application (whether intranet- or internet-facing)? This makes no sense at all. A traditional IDM or IAM solution will no longer be sufficient to manage these scenarios.

Employees are starting to act like consumers. Their wish is to decide for themselves how best to do the job, and to pick and choose the right device for that purpose. As we know, consumers also like to have comfort and ease when using services to do business. Memorizing multiple IDs and their associated passwords isn't the answer to this demanding question. When I look at my own situation, I am faced with dozens of different IDs and passwords, which is certainly not convenient. At the same time, more and more people have started using social logins. According to some analysts, about 90% of people have come across a social login on a website they frequently visit, and more than half of these people use it. More than 80% of these logins are being filled in by Facebook and Google. What if all of these people want to use their Bring Your Own Identity to interact with our business application?

### **IAM and role-based access (RBAC): RIP**

Most of the IDM/IAM solutions today are based on RBAC. However, RBAC and its current implementations have many limitations in a highly connected world and in the scenarios described above. Why? Because the methodology involves linking a set of permissions within information systems or applications to a specific role and connecting an identity to that same role. The problem is that we have to know the identities if we want to grant them a role.

What if we don't have a user ID at the time of contacting the web application? Or if the identity provided is not yet trusted, and must first be enrolled? Or if partners or chain suppliers want to log on to our application using their own credentials? How do we deal with a plethora of customer identities?

And what if they want to provide ID of choice? We would then have to manage all these IDs locally. This is no longer feasible.

Another problem is that RBAC doesn't take into account other contextual factors, like geolocation, time, and device type and behavior. These factors are really important in order to obtain greater assurance (I'll return to this later). RBAC works well with roles but it can't handle context in effective authorization scenarios. RBAC will fail because it is unable to take the contextual information into account when making access decisions.

How can we add the factor of geolocation into the example of Joe using a tablet in a certain location? And more importantly, how can we add this context-based information about the location of the device on the fly, in a real-time authentication scenario, to make a well-informed decision about whether to provide access or deny it? This cannot be done with RBAC.

The third problem concerns scalability. Traditional IAM platforms are good for supporting 10k, 20k, 40k and maybe even 100k users "behind the firewall." Most of us will have (and use) at least three or four devices every day, on average.

The total number of devices and applications that are used to access data will increase dramatically in the near future. Suddenly, we will be facing 1,000 times, 10,000 times, or even 100,000 times the previous figures, both intranet- and internet-facing, in a highly connected world.

Social media will bring in more users from a wider variety of different places. There will be more information generated about users. As the number of possible interactions between users, devices, services, data, and the external environment increases, so does the volume of contextual information needed to describe these interactions through a set of attributes.

This is data that can be used within security scenarios for analysis, which will enable the detection of abnormal behavior and thus enable timely interventions.

## **The development of attribute-based access control**

Role-based access control (RBAC) will be replaced by attribute-based access control (ABAC). Within ABAC, roles will be just one of the various attributes that form the context. In this approach, rules based on attributes will lead to decisions based on the total context, including roles.

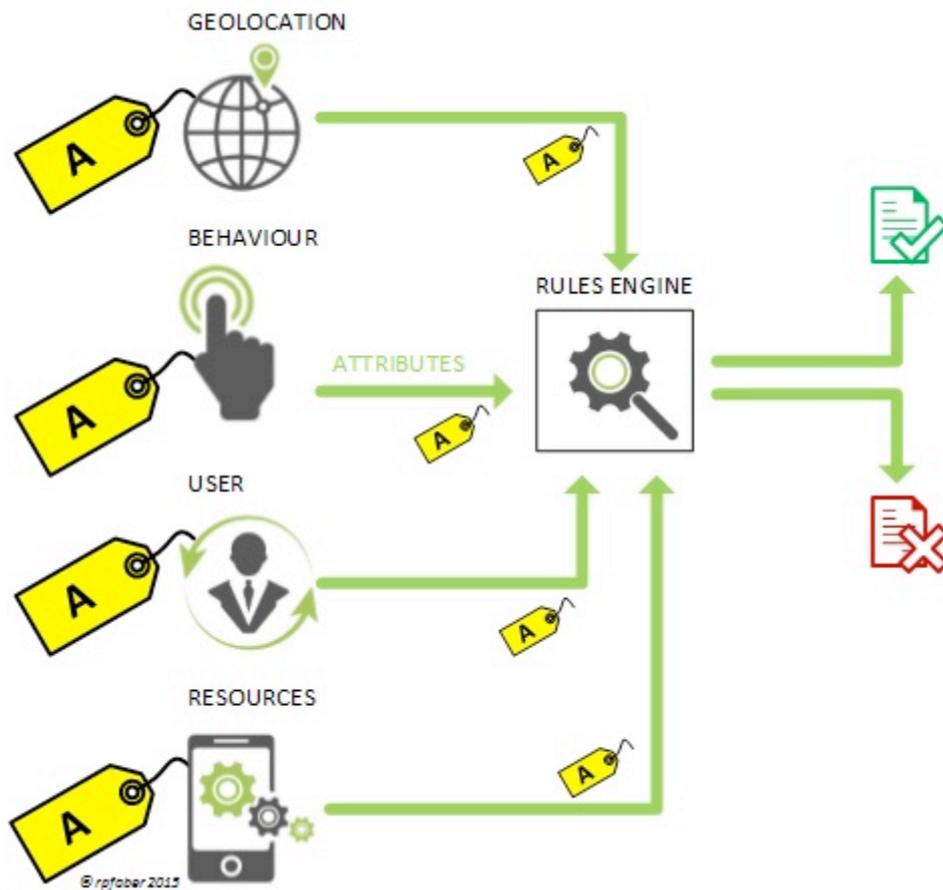
These attributes might include the organization you're working for, the specific unit, the location from which you're trying to gain access, the brand of the customer portal, and so on. NIST has already published a guide to ABAC (<http://tinyurl.com/nbkeftu>).

Systems will increasingly support ABAC in the near future. This trend is supported by examples in the product strategies of popular software vendors. Microsoft introduced dynamic access control (DAC) within their server product and Azure cloud services. After a couple of years, claims-based authentication arrived, in the form of the claims-based architecture in Windows Identity Foundation.

Claims-based authentication is, in essence, ABAC. Application owners are provided with authentication services that are platform- and application-independent, so that no silos or separate identity stores within organizations are needed. The authentication aspect is separate from the actual application. On top of this, identities from other third parties can be used and accepted.

After verification, the provider (issuer) of the requested digital identity creates and returns a token. A token is nothing more than a signed statement by an issuer about a subject. The token includes one or more claims or attributes. They can contain very specific or more generic pieces of information about the subject, like an address, birth date, gender, and so on. This information can then be presented in an authentication process. If the issuer is trusted, they will be provided access.

Systems that don't support ABAC will rapidly become legacy, and it will be increasingly difficult to support them.

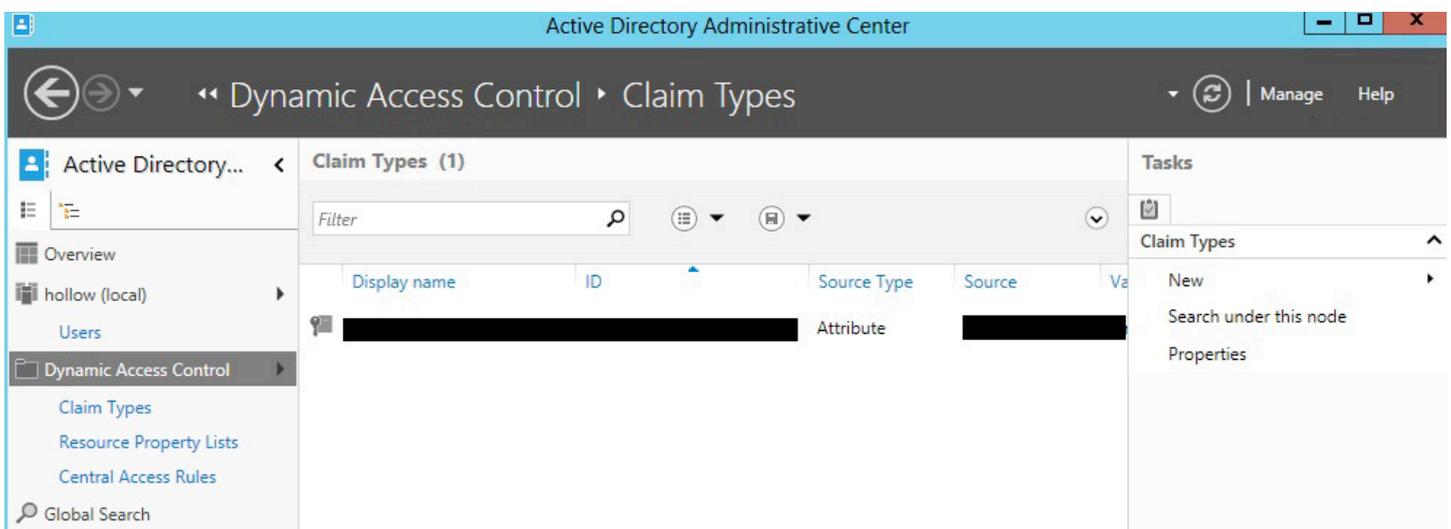


Working with attributes

## Dynamic access control

Introduced by Microsoft with the Windows 2012 File Server, dynamic access control (DAC) allows companies to control access using dynamic access control rules, which use information classification, user claims and device claims to authorize access. Using DAC, companies can take their first steps towards attribute-based access control and introducing information classification. In this way, a greater control over sensitive data is achieved.

Microsoft's dynamic access control is a first step toward the deployment of a new type of access rules. However, it is only a first step. There are still a lot of problems to resolve, and it does not provide a complete solution to all the issues discussed. Token size and management are some of these concerns. What is required is a dynamic attribute container or an attribute space that can be filled in on the fly, for different purposes. Nevertheless, it will be interesting to continue to monitor developments over the coming period.

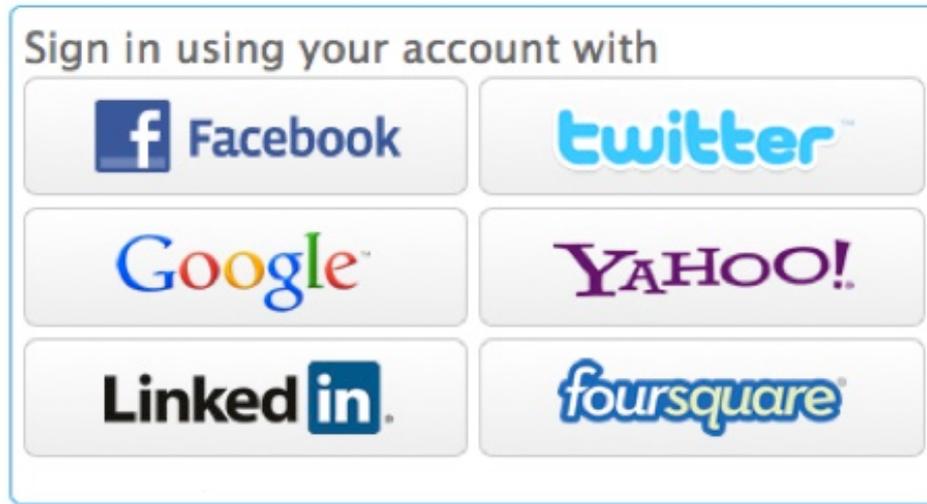


Dynamic access control

## Identity assurance

The use of externally provided identities to access applications has already taken off. Social identities are being used in a number of applications - retail, banking, and media services are used through Google ID, Facebook iden-

tity, PayPal ID, and so forth. Consumers use these identities for convenience, and enterprises support this since the outcome is a desirable digital business scenario. But how can we trust these identities, or add extra information to achieve a higher trust level?



Using social logins

The quality aspects of identity validation should be kept in mind in order to achieve the desired assurance. A combination of sources and aspects (i.e., adding more attributes) is important to receive the overall picture. There are five main quality aspects of digital identities:

- The quality of the identification of a natural person when registering during the process of applying for ID credentials
- The quality of the procedure by which the credentials are issued to the user
- The quality requirements for the organization issuing the credentials and facilitating the registration process
- The technical type and robustness of the credentials
- The security features of the authentication mechanism.

The overall assurance level is equal to the lowest score for any of these five aspects: a high score for one aspect is pointless if there is a weak link elsewhere.

One route into accepting social IDs would be to start with non-critical actions. In the case of a user wanting to perform a more critical action, like changing essential profile data or carrying out a transaction within a banking portal,

we could then step up the authentication process. This authentication solution would have to be under strict control from within the organization. This pattern can already be found within a lot of banking applications. You can enter your bank account and access some basic services, like checking the balance of the account. However, when you want to transfer money, extra steps are needed in order to complete the transaction.

There have been various initiatives to provide identity assurance services to organizations that rely on them. One good example is the Pan-Canadian Identity Management and Authentication Initiative. The Pan-Canadian assurance model involves a three-step assessment process, which allows jurisdiction over the management of risks relating to identity and credential assurance, and to determine what their impact within a federation would be.

According to the roadmaps provided, there are plans for an ID Messaging Hub, which would mean Canadians would only need to make a single update following important life events, and which would enable the secure confirmation of (personal) identity information. More information about this initiative can be found at <http://tinyurl.com/kn2bjhz>.

Another interesting example of this is the digital identities that Estonia provides. The provision of digital ID cards is still a struggle in most countries, but they've been part of everyday life in Estonia for years now. Until recently, you would have to have lived in the country to take advantage of these cards. However, for those who frequently do business in the country, this can be cumbersome.

To solve this, Estonia has been handing out identification services to non-residents since the end of 2014, making it the first country to have a globally relevant digital ID.

Estonia wants to provide citizens of the EU with digital ID cards, making us “e-residents” and allowing us to obtain a digital identification card issued by the Estonian government. Estonian ID cards use open-source public-key-private-key encryption, which allows government agencies to perform various secure functions online in connection with this identity. These functions include, among other things, financial transactions, public transportation tickets, and student university admission records.

The great thing about this scheme is that this is a qualified digital identity. Providing this identity makes it possible for individuals to launch or participate in business, to be authenticated on many (local) web services, and even to send encrypted email. Estonia is counting on a lot of interest in its technology. More information can be found at <http://tinyurl.com/pel6nyc>.

My conclusion is that, since Dick Hardt’s stunning Identity 2.0 presentation at OSCON 2005, there is still no overall answer for how to deal with identities in a digitalized world, and that was 10 years ago! This is very strange if we consider that 10 years is a really long time in IT (more like light-years), and yet we are still struggling with this topic. It’s beginning to seem like it might be too hard to handle.

## **Operational intelligence**

People will increasingly attempt to access our applications and services from many different types of devices, sequentially and even at the same time. Thus, the questions arise: do we trust these devices? Where is the device? Is

the device already known to us? Is the relationship between the person and the device known to us? Are there further factors involved that could help prove the ID?

It is not just the identity itself that counts anymore; adding the right context is highly important in order to receive greater assurance about the identity itself and its reliability in that respect. To gain an insight into what is happening to our infrastructure and applications, it is very important to focus on multiple identities and the relationships between them.

It is crucial to realize not only that people’s identities matter most, but that identities are equal.

Here is an example: Joe wants to log into our web application. He tries to connect from his tablet and smartphone. Within the enrollment procedure, we can connect these identities to each other. Now we know that, time and time again, Joe has been using his tablet or smartphone to gain access. So far so good.

Suddenly, one day late at night, this turns out no longer to be the case. Joe is now using a laptop and is situated elsewhere, a long way from his normal geolocation. Alarm bells start to go off, and we ask Joe to provide some more information that only he (and we) would know, to prove his identity.

This example is essential, in terms of adding more contextual information about the identity itself on the fly, and having intelligence in place to perform real-time analytics. If we know that Joe is connected to the tablet or smartphone, we have a greater assurance.

Another example: it has been known for some time that banks and telecom providers cooperate by passing on information about the use of mobile devices/smartphones. If, for example, I change my SIM card, or the smartphone itself, a notification from the telecom provider will be sent to the bank to let them know about this change.

The telecom provider won’t let the bank know all the details, just the telephone number and certain other characteristics to ensure that they comply with applicable privacy laws.

If there is a “hit,” a bank can have its own measures in place to block me for a while, before sending me a notification or letting me enroll my smartphone again via their portal. Such collaborations across the supply chain concerning identities will become increasingly important; in fact, the brokering of functions and services will be developed in near future.

Information about the device being used and how exactly the user is interacting with it—as well as the behavior of the person, their location at the time of access, and so on—will become very important for obtaining the right assurance.

This is the so-called “context-based authentication” to which further context-based attributes will be added. Suppose we add so much information concerning the identity of the person involved that we know for sure that it is Joe who is interacting with us.

At this point in time, there would be no real need for any further “step up” in authentication scenarios. This would be a potential cost saver, reducing complexity and providing greater convenience for the end user!

Therefore, there is now a clear need for new answers and attributes that can deliver this, and enrich both IDs and the level of confidence. Attributes can be generated and held internally, but they can also be provided by external parties or arise from the user’s context.

Relationships are most important, and not only in terms of people: other identities are equally important. The context of identities is key. The old way of thinking, within a lot of organizations, involved employees accessing applications that protected resources (data). However, traditional IAM cannot solve the problems arising in a highly connected world and in a (hybrid) cloud scenario.

Just as globalization makes a country’s borders more open, so the adoption of cloud and other external services by enterprises opens those enterprises’ “identity borders,” and demands simpler, more consumer-oriented approaches to access while staying in control.

The commoditization of certain identity functions, open standards and ID providers, which can afford a much higher rate of confidence, will be the next gap to be filled in. There are exciting things to come for IAM solutions!

Rob P. Faber, CISSP, CEH, CFI, MCTS, MCSE, is an enterprise security architect and consultant. He is currently working for the largest insurance company in The Netherlands. His information security experience covers a broad range of areas. In addition, Rob has presented many classes and courses concerning IT security. In his spare time, he also blogs at [www.icranium.com](http://www.icranium.com).



# bitglass



## Secure Cloud & Mobile in Minutes

BYOD and Cloud Apps are unstoppable trends. The benefits are huge but you lose control of your data.

Regain control with Bitglass.

IT can enable cloud & mobile, securely.

Employees can enjoy privacy and unencumbered mobility.



### Secure Cloud

- SaaS Firewall for access control
- Full visibility and alerting
- Track data anywhere on the Internet
- Supports any cloud or internal app



### Secure BYOD

- Secure corporate data without MDM or agents
- DLP for sensitive data
- Track data anywhere on the Internet
- Supports Exchange, Office 365, Google Apps etc.

Bitglass deploys in the time it took you to read this.

Sign-up for a free trial at [www.bitglass.com](http://www.bitglass.com)



# Report: Infosecurity Europe 2015

by Mirko Zorz



**Infosecurity Europe is Europe's largest information security conference and exhibition. Over 300 exhibitors showcase the most diverse range of products and services to 13,000 visitors. Here's an overview of the most important news and product releases from the event.**

## Endpoint Protector gets integration with cloud storage apps

**CoSoSys** announced the development of Endpoint Protector 4 to include new integrations with Dropbox for Business and Box to strengthen data security policies and prevent data losses and theft through employee's data transfers made to cloud-based storage applications.

Endpoint Protector 4 integration with Dropbox and Box offers Scanning Data in the Cloud, which is an important addition to existing features. Being able to scan content already saved in the cloud creates an additional layer of protection and remediation in case sensitive data gets on cloud storage.

Dropbox for Business differentiates from the consumer product through additional features like sharing audit logs, remote wipe, possibility to quarantine certain files just for work computers and other security features. For enterprise customers using the Endpoint Protector platform, administrators will gain better visibility for users' actions related to data transfers and, in consequence, optimize the DLP policies. The integration with Dropbox will allow for data in transit to the cloud to be monitored from source to destination, providing even information about the owner of the Dropbox ac-

count. With the same purpose of mitigating threats that come from the cloud storage and file sharing apps, businesses will be able to monitor data transfers to Box through Content Aware-Data Loss Prevention from Endpoint Protector.

IT administrators will have the ability of tracking and stopping data transfers through various criteria like File Type, Predefined Content (PII, Credit Card Numbers, etc.), Regular Expressions or Custom Content (keywords). The integration with Box API will provide additional features, like reporting and deleting of files that do not comply with the data security policy from the cloud storage.

"Data loss and data theft which happens through the cloud, especially through Dropbox, Box and other file sharing apps, will be addressed by Endpoint Protector at a more advanced level," said Roman Foeckl, CEO of CoSoSys." The recent moves by Dropbox underscore the growing concern by both large and small organizations alike regarding the use of cloud storage apps by their employees and the risk of losing enterprise customers if these risks could not be seriously addressed."

The updates will be available in Q3 2015 through download from [endpointprotector.com](http://endpointprotector.com) or through Live Update for existing customers.



## Malvertising infected millions of users in 2015

New research from Malwarebytes has found that malvertising is one of the primary infection vectors used to reach millions of consumers this year. The analysis looked at the three large scale zero-day attacks affecting Flash Player, and the results have been presented at the conference.

Analysis of one particular zero-day attack investigated using the HanJuan Exploit Kit showed that cybercriminals paid an average of 49p for every 1,000 infected adverts impressions on major websites at highly trafficked times of day. This amount could even drop as low as 4p per infected ad impression on lesser-known websites and during quieter times of day.

Malicious adverts placed on popular websites including The Huffington Post, Answers.com and Daily Motion, which all boast monthly unique users in the millions, are responsible for exposing vast numbers of consumers to zero-day attacks.

Even consumers and businesses running the latest versions of Internet Explorer, Firefox and Flash Player are susceptible to becoming immediately infected when exposed to this type of threat which makes it particularly lucrative for the criminal community. Further, with one zero-day remaining active for almost two months of the analysis period there is scope

for exploits to have especially wide-reaching effects.

The nefarious use of the online ad industry is facilitated by real-time bidding as this allows advertisers to bid in real-time for specific targets and weed out non-genuine users or those that should not be targeted by exploits.

“Exploit kit authors leverage the most popular software vulnerabilities to build the most effective tools they can and in the past year, we have seen new vulnerabilities being found and weaponized at a much faster rate. This is a game changer because there is a lack of awareness on zero-day threats and most businesses and consumers aren’t properly equipped to deal with them,” Jerome Segura, senior security researcher, Malwarebytes, explains.

“While one could have foreseen Flash zero-days increasing in frequency in 2015, witnessing three major zero-days happening so close to one another is unique. To face this new reality, businesses and consumers must adapt by adopting new tools to safeguard their assets.”

This is especially important with the kind of malware that is dropped by exploit kits, and in particular ransomware. Companies can literally be crippled by such malware, lose customers and, in some cases, put their whole business in jeopardy.



## Intel and VMware team up to provide advanced threat protection

Intel Security and VMware announced an integrated solution that leverages a Software-Defined Data Centre approach and the VMware NSX network virtualization platform to automate the distribution and enforcement of Intel Security's McAfee Network Security Platform (NSP), providing Intelligent Intrusion Prevention services (IPS) for the protection of east-west traffic within the data centre.

The new integrated solution includes the McAfee NSP IPS-VM100-VSS (a new IPS-VM Series model designed for interoperability with VMware NSX), McAfee Network Security Manager, Intel Security Controller and VMWare NSX network virtualization platform.

The Intel Security Controller transparently runs as a broker between the VMware NSX infrastructure and the Intel Security's McAfee NSP.

Working in conjunction with the VMware NSX Manager, it enables network IPS protection to be dynamically and automatically provisioned to help protect intra-VM traffic based on the defined policies and requirements allowing administrators to experience a "plug-in" like environment that enables support for micro-segmentation, security profiles, workflows, policies, and groups.

## Cloud-based solutions that protect against zero day attacks

BAE Systems Applied Intelligence announced that it is bringing cloud-based cyber security to commercial organizations in Europe for the first time.

The company is introducing a suite of security products designed to defend against targeted attacks, including so-called zero day attacks.

Most cyber attacks start with an email message; the first set of cloud-based products to be introduced by BAE Systems will comprise BAE Systems' Email Protection Services (EPS) which provides comprehensive protection against even the most advanced threats.

In the face of an ever evolving cyber threat and increasing budget pressures, companies are increasingly seeking better protection through advanced security platforms while requiring that costs be significantly reduced. The new services offered by BAE Systems meet this demand.

## Enhanced security for corporate information on mobile devices

Enterprise organizations are continually looking for ways to effectively secure sensitive corporate information on mobile devices. At the conference, TITUS announced the availability of the latest version of TITUS Classification for Mobile, which features a secure corporate email app.

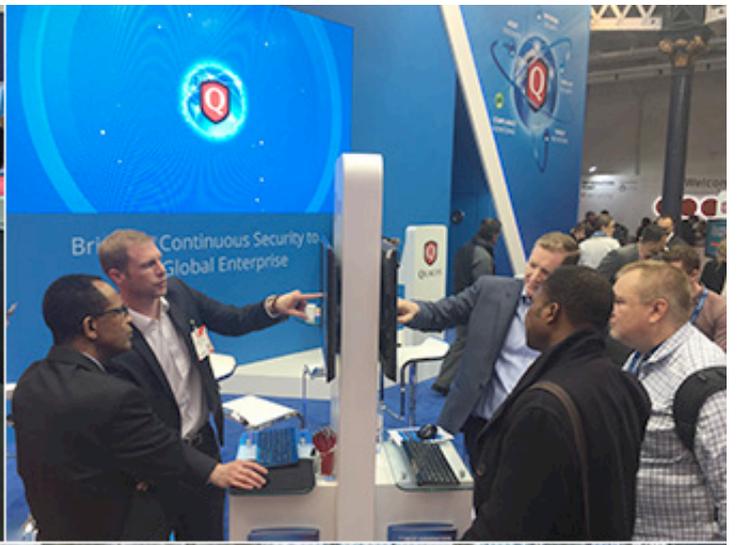
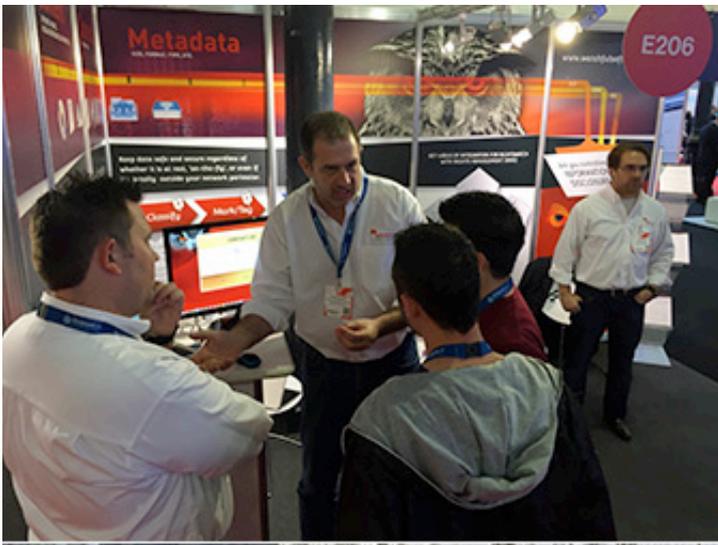
TITUS Classification for Mobile provides a secure and separate container for business email and documents. The intuitive interface provides direct access to corporate email, SharePoint libraries and common file sharing services, ensuring that sensitive files are managed according to corporate policy.

Administrators are able to leverage classifications to enable fine-grained control over a user's ability to email, print, copy, upload, and open files into third party apps. Additional data protection is provided by extending Microsoft Active Directory and Azure Rights Management Services (RMS) to mobile devices, allowing users to access or protect data using Microsoft RMS.

## Akamai and Trustwave unite to protect businesses from online threats

Akamai Technologies, provider of content delivery network services, and managed security services firm Trustwave announced a new strategic alliance designed to help businesses more effectively fight a wide range of malicious online activities through vulnerability assessment, denial of service prevention and incident response.

Through this partnership, Akamai and Trustwave plan to make available to their respective customers select technology solutions and security services from each company's portfolio.



## Employee credentials of half of European top 500 firms exposed online

Cyber attacks and data breaches very often start with phishing or spear-phishing. Access to good credentials is key - whether it's for straight emailing or direct access to target email systems, etc.

Web intelligence firm Recorded Future has recently scoured the Web's underbelly, including paste sites and forums, for exposed corporate credentials (emails and passwords), and found that 49 percent of Europe's largest companies have had credentials belonging to their employees exposed online.

"These 244 companies account for 57% of top banks, 50% of oil and gas producers, and 64% of mobile telecommunications companies in the FT 500 Europe (a Financial Times listing of Europe's top companies)," the company's Special Intelligence Desk noted in the report released during the conference.

In addition to this, many critical infrastructure companies - utilities, healthcare providers, defense contractors - have had their network credentials exposed on the open Web in just the last six months.

## 3-in-1 solution for enterprise management of privileged accounts and info

ManageEngine announced the Enterprise Edition of Password Manager Pro, its privileged access management software. Designed for large enterprises, the new edition combines enterprise-class scalability, security, performance and affordability, facilitating highly secure and easy management of shared sensitive information such as passwords, documents and digital identities.

Privileged accounts, which offer unlimited access privileges, are omnipresent and all pervasive in organizations of all sizes. While the number and mix of privileged accounts in IT enterprises keep growing constantly, cyber-criminals are increasingly targeting login credentials of employees and privileged accounts to gain access to IT assets.

Identity theft often lies at the root of modern cyberattacks. To effectively combat those attacks, IT enterprises require a reliable and scalable solution that can automate the entire life cycle of privileged password management with a policy-driven approach.

## CSA releases tool for personal data legal protection

The Cloud Security Alliance (CSA) Privacy Level Agreement (PLA) Working Group released the Privacy Level Agreement (PLA) v2, a tool that provides cloud customers and potential customers, of any size, with a mechanism to identify a baseline of mandatory personal data protection legal requirements across the EU.

It also allows cloud customers the ability to evaluate the level of personal data protection offered by different cloud service providers (CSPs). PLA v2 also addresses the needs of CSPs by providing a guidance to achieve compliance with mandatory privacy legislations across the EU and a simple way to disclose, in a structured way, the level of personal data protection that they offer to customers.

## Firewalls for SMBs that chew through encrypted streams

WatchGuard Technologies announced a new series of enterprise-strength firewalls engineered specifically to protect small- and medium-sized businesses (SMBs).

SMBs are increasingly the focus of cyber attacks that are no less sophisticated than those targeting large enterprises. WatchGuard's new Firebox M200 and M300 Next-Generation Firewalls (NGFW) and Unified Threat Management (UTM) appliances are up to 218 percent faster than competitors with all the layers of the company's award-winning defense-in-depth solutions turned on.

Plus, the new firewalls are up to 385 percent faster performing HTTPS inspection, which is increasingly critical given encrypted traffic is expected to make up 75 percent of the total Internet traffic by 2016.

# IoT, interoperability, and identity

by Paul Madsen



**It's easy enough to get systems working together and achieve interoperability when the different systems are all within the same domain, or between different implementations of a single software vendor's stack. In such closed communities, proprietary protocols can provide effective and efficient exchange between different computer systems. There are many instances of this sort of interoperability in the current version of the Internet of Things.**

Wearables like Fitbit report step and activity data back to their own cloud. Similarly, Home Automation systems like SmartThings report data on lights and temperature back to its cloud. New IoT devices are hitting the market every single day. Since most connect only to their own backend cloud services, they can use their own proprietary mechanisms for both the communication and the means of securing those messages.

There are many use cases where silos are sufficient and even appropriate. A jet engine should not be expected to support arbitrary API clients -- rather the engine will push its data to a dedicated and trusted client, from there to be proxied further. But of course, the vision for the Internet of Things is grander than multiple siloed "Intranets of Things." To

achieve the anticipated scale, and so the desired efficiencies and optimizations, (and to allow my thermostat to select a TV show about penguins on a hot day) we will need these current silos to be broken down, or at least connected together. And that demands standards.

As nature also seems to abhor a vacuum of standards, we have no shortage to choose from at every level of the stack, from radio to application protocols. Take your pick from the alphabet soup - Zigbee, Thread, Wifi, BLE, CoAP, MQTT, XMPP, etc. - and hope for the best when trying to connect to devices from different manufacturers.

Even if you are able to find an intersection in the protocol support between two unrelated

devices and enable them to talk to each other to share data or control operations, there remains a different type of interoperability that, while seldom discussed, will likely be critical for IoT adoption amongst consumers: identity interoperability.

Identity interoperability refers to one IoT provider being able to accept, rely on and trust an identity created and managed by another, whether that be another IoT provider or a social network like Facebook. We've become used to this sort of convenience when using web applications. Employees can access SaaS applications like Concur using their enterprise identities, and consumers can use their Facebook identities to login to social applications.

The current default for identities in IoT requires users to create a new identity (username and password) for every IoT provider with whom they interact. As a personal example, I have a Fitbit Flex, a Misfit Flash and a Samsung Gear watch, all of which count my steps. For each device, I have created a unique identity with each corresponding provider. While users go through the effort of creating and managing their individual identities, silos of identity are created, inhibiting any sort of cross-provider integration for big picture analysis -- such as comparing the accuracy of my step counters.

Another example is the "Works with Nest" developer program from the Google-owned company. The program aims to position the Nest thermostat as the central hub for a variety of other devices that will be in or near the home -- wearables, washing machines, lights, cars, etc. While the program will allow, for instance, August or Kevo smart locks to inform Nest who is in the house to personalize heating (and thereby achieve a functional interoperability), the presumption remains that the homeowner would have had to create different accounts with Nest and the lock providers. But if I have already bought into the premise of basing my home automation around the Nest, why must I create additional identities at each and every device provider I purchase? As an example, could not August, when I was

first setting up the lock, allow me to use my existing Nest relationship instead of prompting me to create a new one?

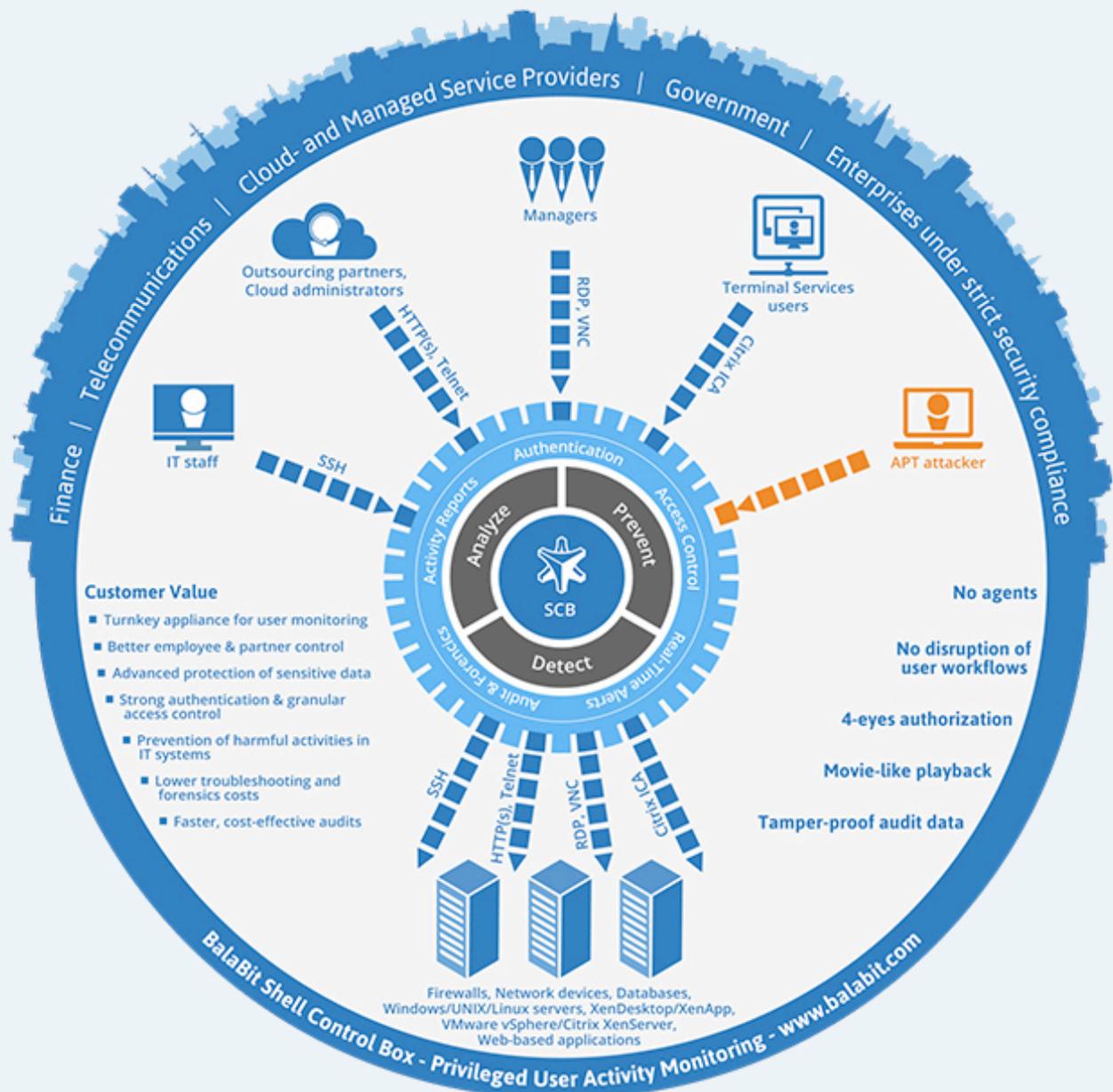
Consider the following scenario. When installing a new device into my home, as in the current practice, I'd install the corresponding native application onto my phone. When I first attempted to login to that application, I'd be given the chance to "Login with Nest" rather than create a new account with that device provider. I'd be redirected to Nest, either the Nest application also on the device or perhaps the Nest site, where I'd be able to login and give my consent to my Nest identity being used by that new device/provider. The two devices are able to work together as I desire, but I have one less identity to manage.

Identity interoperability will also be critical for social scenarios. For instance, once I've set up a smart lock to work with Nest, how do I grant access to my friends and family to the front door (which smart lock providers seem to think I am desperate to do)? How do I invite somebody to assign them authorizations to open my front door? What is the burden on them; must they download a particular app? And critically, by what identity do I refer to them? What if I don't know them as individuals and can't send them an email, but need to grant access to a group, such as "Couriers between 9 and 5"?

The valuable corners of the IoT will necessarily cross the boundaries between the various device manufacturers and application providers. If not, it will be an "Intranet of Things" -- the same acronym but a very different value proposition. But how do you cross such boundaries without a consistent way to refer to the devices, users and applications in question? How do you cross such borders without something equivalent to a passport for things (though hopefully without the horrible pictures? As important for IoT interoperability as standards at the radio and application layer, will be standards at the identity layer. Fortunately, such standards exist -- OAuth 2.0, OpenID Connect 1.0. However, work remains to profile these existing standards for the more constrained environments of the IoT.

Presented at #RSAC:

# TOP 10 Best Practices regarding Privileged Activity Monitoring by BalaBit



Download the "The Essential Guide to Privileged Activity Monitoring" study for free at <https://balabit.com/rsa>.