(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 23 - November 2009

MICROSOFT'S SECURITY PATCHES YEAR IN REVIEW

WEB-BASED ATTACKS > SOCIAL ENGINEERING > MALICIOUS PDFs > MOBILE SPAM > PASSWORDS

REPORTS: RSA EUROPE / BRUCON / STORAGE EXPO

TABLE OF CONTENTS

Page 05 - Security world

Page 10 - Microsoft's security patches year in review: A malware researcher's perspective

Page 16 - A closer look at Red Condor Hosted Service

Page 20 - Report: RSA Conference Europe 2009, London

Page 25 - The U.S. Department of Homeland Security has a vision for stronger information security

Page 27 - Latest additions to our bookshelf

Page 29 - Q&A: Didier Stevens on malicious PDFs

Page 33 - Protecting browsers, endpoints and enterprises against new Web-based attacks

Page 38 - Twitter security spotlight

Page 40 - Mobile spam: An old challenge in a new guise

Page 43 - Report: BruCON security conference, Brussels

Page 46 - Are you putting your business at risk?

Page 50 - Events around the world

Page 51 - Why out-of-band transactions verification is critical to protecting online banking

Page 56 - Study uncovers alarming password usage behavior

Page 58 - Q&A: Noise vs. Subversive Computing with Pascal Cretain

Page 61 - Security software spotlight

Page 62 - Elevating email to an enterprise-class database application solution

Page 67 - Ask the social engineer: Practice

Page 70 - Report: Storage Expo 2009, London

Page 73 - Security videos

Page 74 - Jumping fences - the ever decreasing perimeter

Welcome to (IN)SECURE 23
the digital security magazine

The end of another year is near, and we're left reviewing a myriad of attacks and high-profile vulnerabilities that made headlines all through 2009. Predictions are grim as always, and we better brace ourselves for an ever worse 2010. All we can do is patch our machines, ensure our backups are scheduled and working, and wish for better security as a holiday gift.

We're getting ready for a busy 2010 with several events lined up. (IN)SECURE Magazine is going global like every year. Just in the first few months, we'll be with you at RSA Conference in San Francisco, InfosecWorld in Orlando and Infosecurity in London. If you'd like to meet, let me know.

On behalf of the entire team, I wish you safe holidays and some well-deserved downtime.

Mirko Zorz
Editor in Chief

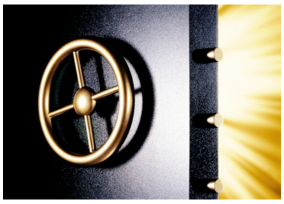
Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts
Feedback and contributions: Mirko Zorz, Editor in Chief - editor@insecuremag.com
News: Zeljka Zorz, News Editor - news.editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

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.

Security world

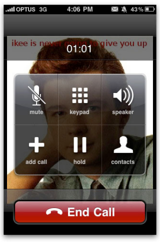
Major vulnerability in SSL authentication



Marsh Ray and Steve Dispensa of PhoneFactor discovered a serious vulnerability in SSL, the most common data security protocol on the Internet. The SSL Authentication Gap allows an attacker to mount a man-in-the-middle attack, and affects the majority of SSL-protected servers on the Internet. Specifically, the vulnerability allows the attacker to inject himself into the authenticated SSL communications path and execute commands. Furthermore, both the web server and the web browser generally have no idea their session has been hijacked. (www.net-security.org/secworld.php?id=8477)

First iPhone worm discovered

Apple iPhone owners in Australia have seen their smartphones get infected by a worm that has changed their wallpaper to an image of 1980s pop musician Rick Astley. The worm, which could have spread to other countries, is capable of breaking into jailbroken iPhones if their owners have not changed the default password after installing SSH. Once in place, the worm appears to attempt to find other iPhones on the mobile phone network that are similarly vulnerable, and installs itself again. (www.net-security.org/malware_news.php?id=1138)



Backdoor access for millions of Facebook and MySpace accounts

A Facebook application developer stumbled on a back door into any user account that accesses the application he's working on. He discovered the exploitable mistake while trying to get around a function limitation on his application, and realized he could modify the accounts and that his illegitimate interventions into the account couldn't even be traced. (www.net-security.org/secworld.php?id=8473)

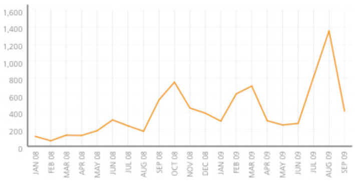
Battle of the anti-virus: What is the best software?

AV-Comparatives.org released the results of a malware removal test which evaluated 16 anti-virus software solutions. The main question was if the products are able to successfully remove malware from an already infected/compromised system. eScan, Symantec and Microsoft (MSE) were the only products to be good in removal of malware AND removal of leftovers. (www.net-security.org/malware_news.php?id=1137)

Google Dashboard: What does Google know about you?

You've been using Gmail for ages. Most searches you ever started online began at Google.com. You watch most videos at YouTube. Aren't you a little bit curious about what information Google collected about you? You can stop wondering and check out the new Google Dashboard, a privacy tool that will give you an overview of the things Google learned about you through your use of its products.(www.net-security.org/secworld.php?id=8474)

Record levels of spam, malware and Web-based threats



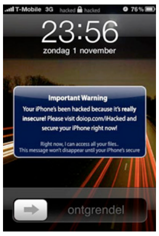
New illegal software and infringed copyright content, by number of sites.

The number of new file-sharing sites hosting unauthorized, copyrighted content skyrocketed over the last three months, according to McAfee's latest report. It also shows that spam, malware and Web-based threat creation has reached record levels in the last quarter, and that cybercriminals are extorting site-owners with threats of DDoS attacks. These botnets are capable of knocking even some of the most-protected sites offline. Cybercriminals will even offer a “demo” performance for a few minutes to prospective buyers. (www.net-security.org/malware_news.php?id=1131)

Windows 7 vulnerable to most viruses

The Sophos team installed a full release copy of the new OS on a previously cleaned computer, kept the default values for User Account Control and didn't install any anti-virus software. They then proceed to infect the machine with 10 unique samples of malware that SophosLabs received last. The result wasn't good for the users (although it technically is a good result for manufacturers of anti-malware software around the world): only 2 out of 10 failed to operate! (www.net-security.org/malware_news.php?id=1134)

Hacked iPhones held hostage



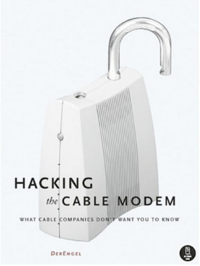
Important Warning

Your iPhone's been hacked because it's really insecure! Please visit doiop.com/iHacked and secure your iPhone right now!

Right now, I can access all your files..
This message won't disappear until your iPhone's secure

Dutch T-mobile customers that use jailbroken iPhones got a nasty surprise when a "message" popped up on their screen claiming that their iPhone's been hacked and instructs them to visit a site to secure their iPhones. When the scared users would visit the website, they were asked to send €5 to the hacker's PayPal account so he can send them instructions on how to secure their device. (www.net-security.org/secworld.php?id=8468)

Hardware hacker charged with aiding computer intrusion and wire fraud



Ryan Harris aka DerEngel, a hardware hacker/modder and author of a book on hacking cable modems has been charged with conspiracy, aiding and abetting computer intrusion and wire fraud. Harris has an online business that sells unlocked cable modems. The problem with this is that these appliances can be put to illegal use - stealing speed or obtaining free service from broadband providers, and he had the misfortune of selling a couple to an FBI agent. (www.net-security.org/secworld.php?id=8466)

What information security might look like in a decade

Esther Dyson, a former chair of the EFF and ICANN, gave a prediction of the future evolution of information technology. Microsoft and Apple will take more care to patch the vulnerabilities in their products, Google will alarm you more thoroughly if you search comes up with potentially dangerous links. ISPs will be held responsible for damages that result from their customers' computers and will start installing security software on their machines and hiring security experts. (www.net-security.org/secworld.php?id=8465)

Suspected European cyber pirates denied Internet access without court order

The verdict is in: Europeans can be cut off the Internet for persistent file-sharing, and it can be done without a court order. The decision comes as a surprise since on two previous occasions amendment 138 has been adopted by a majority of votes in the European Parliament, and it specifically states that restricting Internet access of an individual suspected of illegal downloading must be previously approved by a court of law. (www.net-security.org/secworld.php?id=8420)

Woman fired as a result of error in FBI criminal database

A senior accountant with Corporate Mailing Services was fired from her job because - due to an error in the FBI' criminal database - she was deemed "unsuitable" (no additional explanation given) to perform any job connected to the contract for which the employees had to pass a low-level security clearance. But, instead of just giving her other tasks to perform - assignments that have nothing to do with the contract in question - the CMS chose to eliminate her as an employee altogether. (www.net-security.org/secworld.php?id=8457)

Ubuntu 9.10 Karmic Koala released

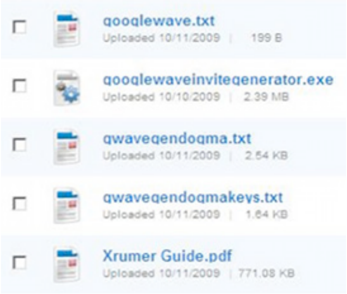
Ubuntu 9.10 Desktop Edition and Server Edition bring a host of new features and further position Ubuntu as a viable competitor to Windows 7. It features a redesigned, faster boot and login experience, a revamped audio framework, and improved 3G broadband connectivity. Developers interested in writing applications that run on Ubuntu now have a simplified toolset called 'Quickly' which makes it fun and easy by automating many of the mundane tasks involved in programming. (www.net-security.org/secworld.php?id=8450)

Facebook hit by phishing scam and banking Trojan combo

Facebook users should be on the lookout for an email threat that is posing as a message from Facebook administrators. The message contains both a phishing scam and a notorious "banking Trojan" virus. A link within the spam email takes users to a spoofed Facebook login page requesting the user's account information. After entering their credentials, users are then prompted to download "updatetool.exe" which is a Zbot Trojan variant. (www.net-security.org/malware_news.php?id=1130)

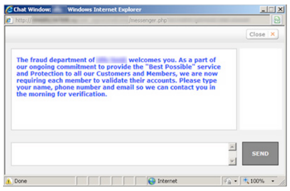
Careless spammer reveals tricks of the trade

Patrick Fitzgerald of Symantec has struck gold while investigating the latest malware campaigns he was alerted to. The campaign in question is simple enough: forum visitors and Twitter users are offered to download an application that supposedly generates invites for Google Wave. The application in question is, of course, malicious, but on the site there are also a few files you can download which the spammer hasn't probably planned to share - spamming how-to manuals. (www.net-security.org/secworld.php?id=8453)



□	googlewave.txt Uploaded 10/11/2009 | 199 B
□	googlewaveinvitegenerator.exe Uploaded 10/10/2009 | 2.39 MB
□	gwavegendogma.txt Uploaded 10/11/2009 | 2.54 KB
□	gwavegendogmakeys.txt Uploaded 10/11/2009 | 1.64 KB
□	Xrumer Guide.pdf Uploaded 10/11/2009 | 771.08 KB

"Chat-in-the-Middle" - new breed of phishing attack



Chat Window: [redacted] Windows Internet Explorer
http://[redacted]/messenger.php[redacted]
Close ✕
SEND
Done
Internet
100%

The fraud department of [redacted] welcomes you. As a part of our ongoing commitment to provide the "Best Possible" service and Protection to all our Customers and Members, we are now requiring each member to validate their accounts. Please type your name, phone number and email so we can contact you in the morning for verification.

According to RSA FraudAction Research Lab, there is a new type of phishing attack - "chat-in-the-middle", it's a variation of the standard phishing scam where a bank customer gets lured to a phished online banking site and is tricked into giving up his or hers username and password. The novelty is in the social engineering approach - when the victim enters the phished site, a live chat session with a "representative of the bank's fraud department" is launched. (www.net-security.org/malware_news.php?id=1111)

Serious cyber attacks on the horizon

A report by James A. Lewis, of the Center for Strategic and International Studies, used the recent cyber attacks that targeted the US and South Korea as a catalyst to raise a series of very important questions: Which nations possess the cyber capabilities to launch attacks against the US? What are the odds of that happening? (www.net-security.org/secworld.php?id=8439)

BlackBerry spy software

Mobile Spy for BlackBerry runs in total stealth mode and no mentions of the program are shown inside the device. After the software is set up on the phone, it silently records GPS locations every fifteen minutes. The entire text of all SMS text messages along with the associated phone number is also recorded. Additionally, inbound and outbound call information with duration of the call is recorded. Immediately after activities are logged, they are silently uploaded to the user's private online account. (www.net-security.org/secworld.php?id=8430)

Open source penetration testing framework Metasploit acquired by Rapid7

Metasploit, one of the top open source penetration testing frameworks, has been acquired by Rapid7. Metasploit will remain open source under the existing license. Initially, Rapid7 will be funding several developers, including HD, to work on Metasploit. In addition, Rapid7 will be donating vulnerability checks for some of the most popular Metasploit exploits to the Metasploit code base. (www.net-security.org/secworld.php?id=8402)

New patent for encryption key generation method

The newly issued US Patent No. 7,577,987 titled “Key generation method for communication session encryption and authentication system” describes a new encryption key management system integrated with a two-factor authentication protocol. This system provides for mutual authentication of the connected parties in a client-server architecture which results in a secure distribution of secret session-only random symmetric encryption keys that are generated at the server and distributed to clients. (www.net-security.org/secworld.php?id=8436)

Social media insight for the U.S. intelligence community

Visible Technologies announced a strategic partnership and technology development agreement with In-Q-Tel, the independent strategic investment firm that identifies innovative technology solutions to support the mission of the CIA and the broader U.S. Intelligence Community. Visible Technologies' end-to-end suite encompasses global features that enable real-time visibility into online social conversations regardless of where dialogue is occurring. (www.net-security.org/secworld.php?id=8395)

IBM's open-source alternative to Windows 7

IBM and Canonical are introducing a cloud- and Linux-based desktop package. It includes several open standards-based components: word processing, spreadsheets and presentations from IBM Lotus Symphony; cloud-based, social networking and collaboration tools from LotusLive.com; Ubuntu, an open platform for netbooks, laptops, desktops, and servers. (www.net-security.org/secworld.php?id=8400)

Cybercriminals use Trojans and money mules to loot online bank accounts

New research shows how a cybergang used a combination of Trojans and money mules to rake in hundreds of thousands of Euros and to minimize detection by the anti-fraud systems used by banks. The cybercriminals used compromised legitimate websites as well as fake websites. After infection a bank Trojan was installed on the victims’ machines and started communication with its Command & Control server for instructions. These instructions included the amount to be stolen from specific bank accounts and to which money mule accounts the stolen money should be transferred. (www.net-security.org/malware_news.php?id=1120)

Microsoft's security patches year in review: A malware researcher's perspective

by Josh Phillips

It's no secret that Microsoft has had the lion's share of security vulnerabilities. Its success as a company has made it the most obvious and profitable target for malware authors for nearly twenty years now.

While it is true that we are seeing malware authors begin to attack other pieces of software, to the tune of up to 84%, according to Microsoft's Security Intelligence Report v7, the fact remains that because of its ubiquity, the Windows operating system will continue to be the number one target for bad guys for a number of years to come (bit.ly/1b2Amu).

A Microsoft representative from the Netherlands has even gone on record saying Microsoft does not want malware on other operating systems, because that would then mean that the competitor is successful.

While it may seem no different than any other year, Microsoft has had a pretty hectic past 12 months on the security front. In one regard, they have made enormous strides in creating a more secure operating system starting with Windows Vista and culminating with the just released Windows 7. On the other hand, they've issued several out-of-band security patches and would of course love for everyone to forget about the Conficker (AKA Kido/Downadup) worm. Even pre-release versions of Internet Explorer 8 and Windows 7 were hit with critical security vulnerabilities.

In the past year, Microsoft has released four out-of-band patches addressing MS08-067, MS08-078 and they released MS09-034 and MS09-035 on the same day. In December '08, they addressed 28 vulnerabilities, in June '09 they addressed 31 vulnerabilities, a record at the time, and then in October '09, they beat two records; the most patches with 13, addressing the most vulnerabilities at 34. It has certainly been a busy twelve months in Redmond.

Security philosophies

There is a holy war in the security industry that has been going on for some time now. The one side says that security patches should be released as soon as humanly possible: a known vulnerability is a security risk no matter what. The other side though, says that if a vulnerability has been discovered internally by the company, or has been responsibly disclosed, that the simple act of issuing a security patch might be as risky as not issuing a patch. Both sides have their merits for sure which makes choosing sides fairly difficult.

The second camp says that whenever a company such as Adobe or Microsoft discovers a vulnerability, fixing it immediately is not always the best choice, especially in the case that the exploit is not publicly known, such as when Microsoft discovers the vulnerability itself, or when someone has disclosed their vulnerability responsibly. It frequently happens that malware is created to exploit vulnerabilities by reverse engineering the patches that Microsoft releases. In some cases, if Microsoft were to delay release of a security patch, they can also delay the release of malware that exploits that vulnerability.

The first camp however says that the second camp is relying on some potentially false assumptions. Just because it is thought that the vulnerability is not known by others, does not mean that it truly is not known by others.

Perfect examples of this is the SSL certificate spoofing vulnerability that both Moxie Marlinspike and Dan Kaminsky presented about at Blackhat this year and even more to the point, another SSL implementation flaw was stumbled upon just this week, November 4th to be exact (tinyurl.com/bty67m, tinyurl.com/l9yu77, tinyurl.com/yk83lla). This disclosure happened exactly as the second camp warns: a silent security fix was being planned by a group of people under the assumption that nobody else would find out until after the fact, and surprise, a third party came along and posted his findings without fully realizing the implications.

Microsoft has long had a history of prioritizing functionality and ease of use over security, however, this year marks two big strides at correctly prioritizing security.

Microsoft has long had a history of prioritizing functionality and ease of use over security, however, this year marks two big strides at correctly prioritizing security. Internet Explorer 8 has been made available on Windows XP, and along with it, the security improvements it brings, especially when compared with Internet Explorer 6.

Even more impressive however, is that Microsoft made available a patch for disabling the autorun feature on rewritable media such as USB drives or network shares. Security professionals have been screaming about this so called feature for years and we finally got it. This is a giant win for organizations still running Windows XP, and large majority still are, as removable media has regained its once prominent role as a prime infection vector in recent years due to the widespread usage of portable USB thumb drives.

As somewhat of an expert it's always interesting to read about the various security vulnerabilities. Most people, including software developers, have no idea how much effort goes into creating truly secure software. Software development in general is a tough thing. There is a reason why the majority of projects are over budget and late, and that's just for core functionality, most software development teams completely excludes security concerns from their development cycles. Now add in security on top of the regular development cycle and it becomes easier to understand why even organizations such as Microsoft, who by all measures is an expert at delivering software, frequently find themselves at the butt end of a security vulnerability. When Java and .NET were released, people hailed them as the end of insecure software, gone are the days of buffer overflows. Well, the bad news is that security vulnerabilities are more than just buffer overflows and failures to correctly handle strings correctly.

MS08-067 - Conficker and friends

Without a doubt, the most publicized exploit of the year was due to the MS08-067 netapi32!NetpwPathCanonicalize. This is a prime example of the “security is hard” mantra. As it turns out, Microsoft had issued a patch addressing the same area of code two years prior with MS06-040. Nobody but Microsoft can tell you why they failed to catch the other errors, and good luck getting them to do so, as they would much rather forget the entire thing ever happened, but it goes to demonstrate exactly how hard security truly is.

The decision by Microsoft to release an out of bound patch for MS08-067 was triggered by the public availability of proof-of-concept code for the vulnerability followed by malware that was actively exploiting the vulnerability. The malware families in this case, according to Ziv Mador, speaking at CARO 2009, were Gimmiv, Arpoc and Wecorl among others (tinyurl.com/ykkr4tf).

Most people have heard of Conficker, however most industry outsiders probably have not heard of Gimmiv and the other lesser known malware exploiting MS08-067. The reason is obvious in the sense that in order to become well known, malware has to be widespread. The reason this was the case for Gimmiv, at least, was simple; it drops a batch script to delete itself after having executed its payload. This and the sole reliance on MS08-067 to spread had significant impact on its overall penetration.

For security professionals, November 21st will be remembered by many as a day of infamy, right alongside January 24th and August 12th 2003, the dates when Slammer and Blaster were discovered. For me, it was work as usual; stumble upon a pretty normal looking piece of malware, write a detection for it and move on. Little did I know at the time how truly remarkable both the malware and the name I chose, Conficker, would end up being. Conficker as we all know has been one of the most effectively propagating pieces of malware since the days of Sasser, Slammer and Blaster.

Most people have heard of Conficker, however most industry outsiders probably have not heard of Gimmiv and the other lesser known malware exploiting MS08-067.

Microsoft made an excellent decision to release the patch for MS08-067 almost a month prior to the appearance of Conficker and had Microsoft not released the patch, and had the Conficker Working Group not devoted so much effort, the story behind Conficker could have been much worse. The days when unpatched copies of any operating system were safe on the network have been over for at least a decade, but as the saying goes, you can lead a horse to water, but you can't force it to drink.

Conficker was so successful at infections due to a variety of reasons. First, Conficker patched the MS08-067 vulnerability so as to both prevent re-infection and to protect itself from other malware exploiting the same vulnerability such as the previously mentioned Gimmiv. Second, Conficker.B, started spreading via removable media such as USB sticks and via weak security controls in network shares and also attempts to brute force passwords on the infected machines to gain further access to network resources.

The C++ template nightmare

Most other security related events this past year pale in comparison to Conficker and MS08-067, but that still doesn't mean they are uninteresting. A highly interesting example from the point of remediation was the slew of vulnerabilities related to the ATL C++ template libraries. Talk about a nightmare to fix.

First off, there wasn't a simple binary that could be replaced, in order to actually fix the issue Microsoft had to provide an update to the ATL source code which means that in order to fix the vulnerability, developers need to recompile and reship their products, and, unless the developer is aware of that requirement, they will still have vulnerable products.

It took Microsoft, for example, a total of three months to completely address the issue in their own products. They issued the ActiveX kill bits only July 14th, with MS09-032, on July 28th they had the two out of band patches, one addressing Internet Explorer, and the other addressing the ATL C++ source code that is shipped with Visual Studio. Windows Live Messenger received an update on August 25th and on October 13th, Microsoft was finally able to address the vulnerability in Office.

The sad thing is that a large number of independent software developers will likely be unaware of the actions they need to take in order to protect their customers, and will thus be exposing their customers to the same vulnerability. Similarly, it is possible that Microsoft will be releasing more killbit updates for ActiveX controls as they become aware of them. Microsoft has provided a flow chart (tinyurl.com/ygdoytx).

MS09-059 was made famous at Blackhat Las Vegas 2009 by Moxie Marlinspike. Dan Kaminsky also discovered the vulnerability but I think Moxie stole the show with his energy and delivery.

Data formats are hard

There were several interesting vulnerabilities related to incorrect handling of various data formats. MS09-028 and MS09-059 were both related to the differences in formats between C strings and pascal strings. The core issue for both vulnerabilities is that dealing with structured data, especially when created by different groups of people, is extremely hard and error prone. For those interested, The Art of Assembly Language gives a fairly detailed description of the various string formats that are at issue here (tinyurl.com/5jm6rc).

MS09-059 was made famous at Blackhat Las Vegas 2009 by Moxie Marlinspike. Dan Kaminsky also discovered the vulnerability but I think Moxie stole the show with his energy and delivery. Briefly put, C strings use null sentinel characters to designate the end of a string whereas pascal strings use length prefixes to designate string content. Certificate authorities use the pascal convention while virtually every implementation using these certificates use the C convention, hence the vulnerability. It appears that exploitation of this vulnerability has been relatively limited, but due to the nature has received a widespread press.

MS09-028, however, was not so limited. Antivirus companies quickly discovered that malware authors were exploiting the vulnerability in order to infect victims with a password stealer that targets players of certain online games. This vulnerability, as with MS09-059, was again caused by the difference between C and pascal like string formats.

Following an ongoing trend in recent years, we saw MS09-006, which was a vulnerability in EMF/WMF image files. There were some poor design decisions here that increased the significance of the vulnerability because EMF and WMF images can have their extension changed to .jpg and still be recognized as valid EMT/WMF images. The especially alarming part here is that these images are handled by kernel mode code, a design decision that is potentially twenty years old, and it was this kernel mode code that was vulnerable.

Internet Explorer 8

Internet Explorer has had its share of battle wounds this year too. Besides security vulnerabilities, Betanews reports that the result of cumulative security patches has resulted in the once fast Internet Explorer 8 becoming only marginally faster than its predecessor. To borrow from Steve McConnell in Code Complete: sure your code may be fast, but mine would be faster if it didn't have to be secure.

Microsoft didn't catch a break in the last quarter of '08. Hot on the heels of Conficker, December brought another out-of-band patch addressing a data binding vulnerability that would result in drive by exploitation.

MS08-078 was released only 8 days after patch Tuesday fixed had already addressed 28 vulnerabilities. I during the last two months of 2008.

March of 2009 brought Internet Explorer 8, which brings fully enabled Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP or NX) to the browsing experience. The final release version, however, was beat to the punch by the Opera browser, which enabled the same features about two weeks prior to IE 8's final release date. It's significant to note the work of Mark Dowd and Alexander Sotirov on bypassing ASLR and DEP (tinyurl.com/yg2pw8x). Because of their work, a relative newcomer to the exploit field, who chose go by the name of Nils, was able to create quite a stir while participating in CanSecWest's pwn2own contest.

It was first thought that the exploit was achieved on the released version of IE 8, however, that turned out to not be the case. The final release of IE 8 included a fix to prevent the type of attack as outlined by Dowd and Sotirov and was therefore not vulnerable to the exploit. A patch was still required to resolve the vulnerability because, as we all know, ASLR is not available on Windows XP, and on 32 bit systems it is still possible to brute force. Lastly, it is still possible to disable DEP and ASLR and re-enable the feature at the heart of the ASLR+DEP bypass. I mention this because there was some confusion around why Microsoft would issue a patch for a vulnerability that its product was already protected against.

Conclusion

It's been an interesting year this year. A lot of things happened, Conficker, Internet Explorer 8, Windows 7, etc. The security story for Microsoft keeps improving, yet it seems to have no effect on the malware and exploit writers' ability to discover new ways to infect users systems.

As fast as security tools evolve to discover and fix new vulnerabilities, new ways are discovered to bypass them and this year has been no different in that regard. For the sanity of the world, here's hoping for a boring 2010!

Josh Phillips is a Senior Virus Researcher at Kaspersky Lab (www.kaspersky.com).

OWASP
The Open Web Application Security Project
JOIN US! OWASP is a free and open community dedicated to improving application security for everyone.
You'll find free tools, books, articles, best practices, mailing lists, conferences, and local chapters around the world to help you build secure code.
www.owasp.org

A closer look at Red Condor Hosted Service

by Zeljka Zorz

Over the years, email filters became a crucial factor in allowing us to open our inboxes without cringing. It doesn't matter how careful you are about giving out your email address, it will eventually find itself on spam lists and you'll be subjected to the barrage of worthless and malicious emails that you would rather do without.

Owners of private e-mail addresses hosted on web-based email services usually don't even have to think about filtering - the service probably thought of that. If you work at a big company that has its own IT department, you won't have to think about filtering, but if you own a small business or have a small IT budget and team, you might consider a Software-as-a-Service solution.

Red Condor's Hosted Service is a good choice. It's actually very simple to set up and extremely effective, and will prevent you becoming a target of spam, viruses, phishing schemes, offensive content, and other threats.

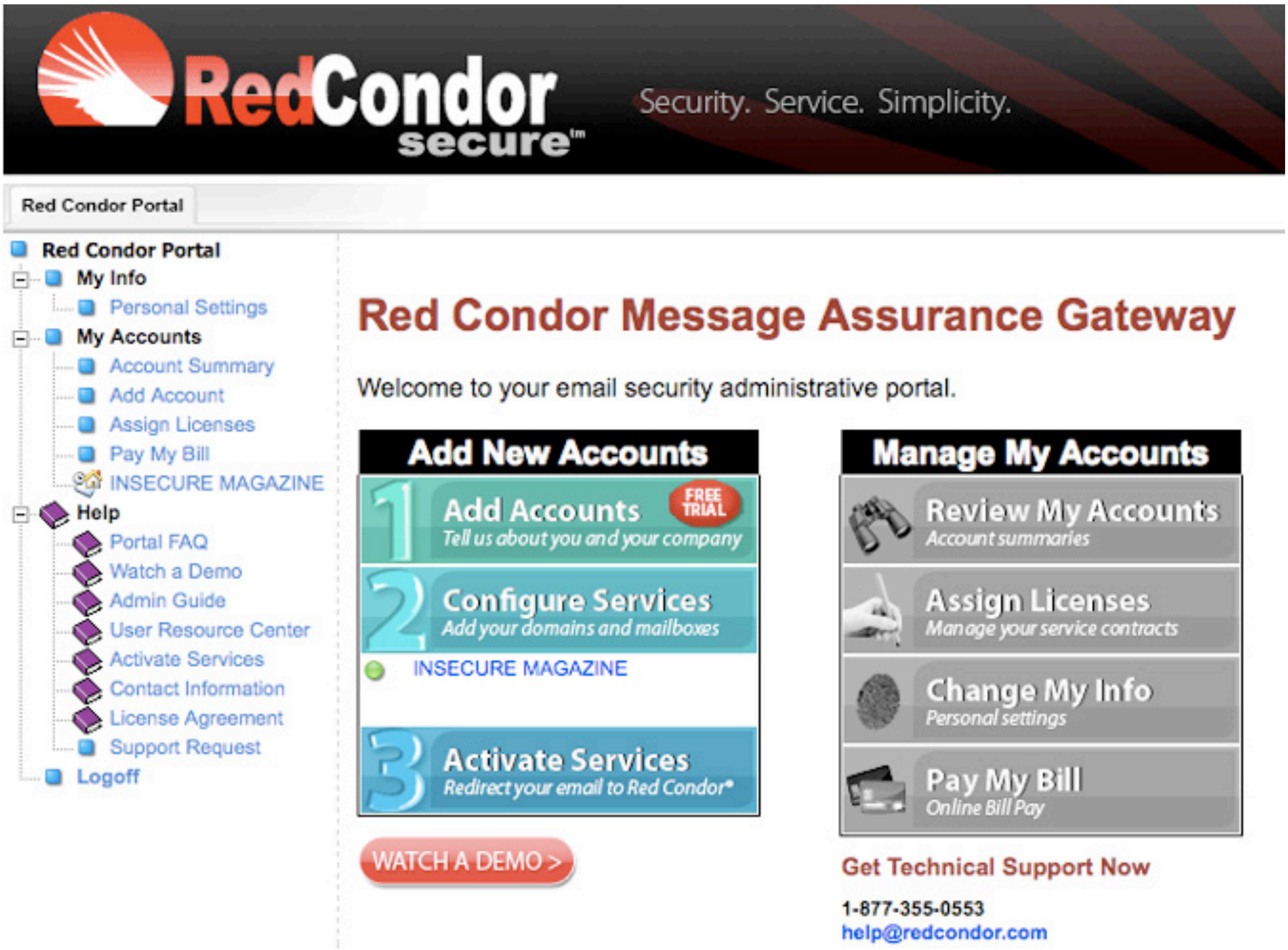
It works like this: you redirect your MX records to Red Condor's servers. There the emails are filtered and only the legitimate ones are passed on to your mail server. Real-time knowledge gathered from a worldwide sensor network is used to create heavy-duty filter rules.The filters analyze emails by content, keywords and behavior to separate the wheat from the chaff - so to speak.

You don't have to think about software or hardware installation, or even about filter tuning - and in case one of your email servers goes down, Red Condor stores your email for up to 96 hours until your server is brought back online.

Another great feature is outbound mail filtering, so if a PC in your network gets infected and turns into a "zombie", it will prevent the spam-sending activity and notify the administrator immediately.

After registering and logging in, you access your account through a simple and very user-friendly web interface/portal.

The first step is adding an account. You will be asked to input account information - name and address. Primary contact information is also required, but technical, admin and billing contact information is optional. The person that opens the account is automatically assigned administrator privileges.



RedCondor secure™ Security. Service. Simplicity.

Red Condor Portal

- Red Condor Portal
  - My Info
    - Personal Settings
  - My Accounts
    - Account Summary
    - Add Account
    - Assign Licenses
    - Pay My Bill
    - INSECURE MAGAZINE
  - Help
    - Portal FAQ
    - Watch a Demo
    - Admin Guide
    - User Resource Center
    - Activate Services
    - Contact Information
    - License Agreement
    - Support Request
  - Logoff

Red Condor Message Assurance Gateway

Welcome to your email security administrative portal.

Add New Accounts

1 Add Accounts FREE TRIAL – Tell us about you and your company

2 Configure Services – Add your domains and mailboxes

INSECURE MAGAZINE

3 Activate Services – Redirect your email to Red Condor®

WATCH A DEMO >

Manage My Accounts

Review My Accounts – Account summaries

Assign Licenses – Manage your service contracts

Change My Info – Personal settings

Pay My Bill – Online Bill Pay

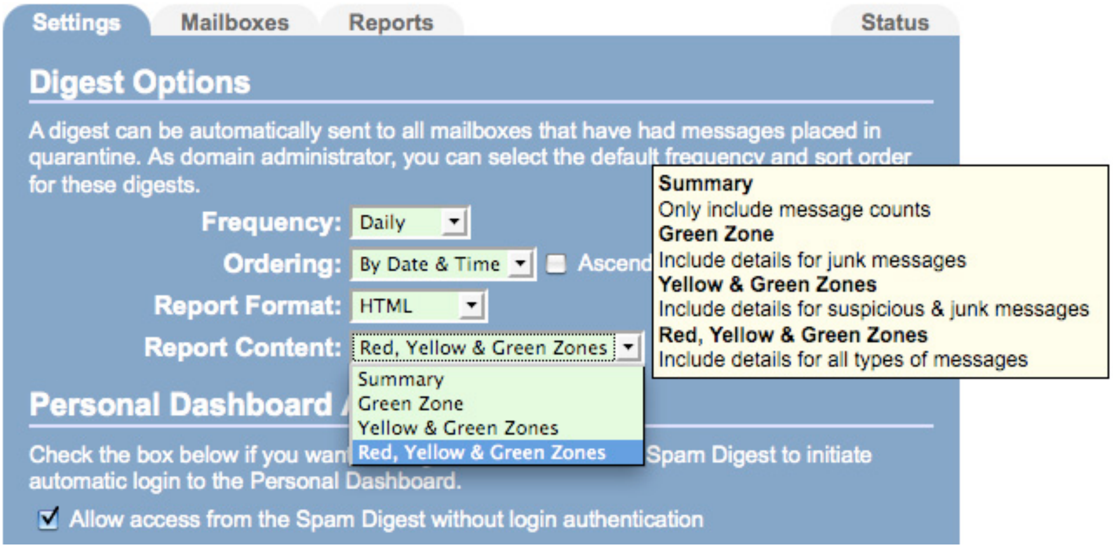
Get Technical Support Now

1-877-355-0553
help@redcondor.com

Red Condor's web portal

The second step is the configuring of services - after adding a domain, you can configure settings, mailboxes and reports. When adding a domain you can choose to add mailboxes and mail gateway manually or you can let Red Condor search for the gateway. Click on the Settings tab to choose among a myriad of options. Let me mention here that I found the fact that every option is explained via pop-up text boxes very helpful.

You can choose a digest to be sent to all mailboxes that have had messages placed in quarantine, so you can check if the filter caught some important and legitimate email by mistake.



Settings | Mailboxes | Reports | Status

Digest Options

A digest can be automatically sent to all mailboxes that have had messages placed in quarantine. As domain administrator, you can select the default frequency and sort order for these digests.

Frequency: Daily

Ordering: By Date & Time □ Ascend

Report Format: HTML

Report Content: Red, Yellow & Green Zones

- Summary
- Green Zone
- Yellow & Green Zones
- Red, Yellow & Green Zones

Summary
Only include message counts
Green Zone
Include details for junk messages
Yellow & Green Zones
Include details for suspicious & junk messages
Red, Yellow & Green Zones
Include details for all types of messages

Personal Dashboard

Check the box below if you want Spam Digest to initiate automatic login to the Personal Dashboard.

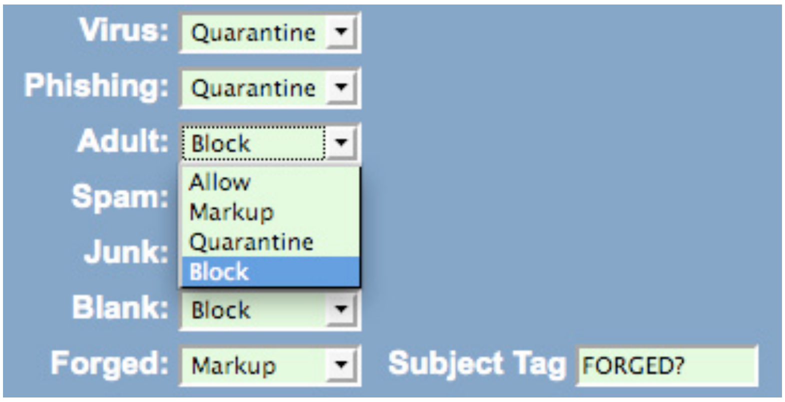
☑ Allow access from the Spam Digest without login authentication

Digest options

Filtering options are many - you can filter emails that contain viruses, adult material, spam, are phishing attempts, etc. Blocked messages are permanently discarded, whereas quarantined messages are stored for 35 days.

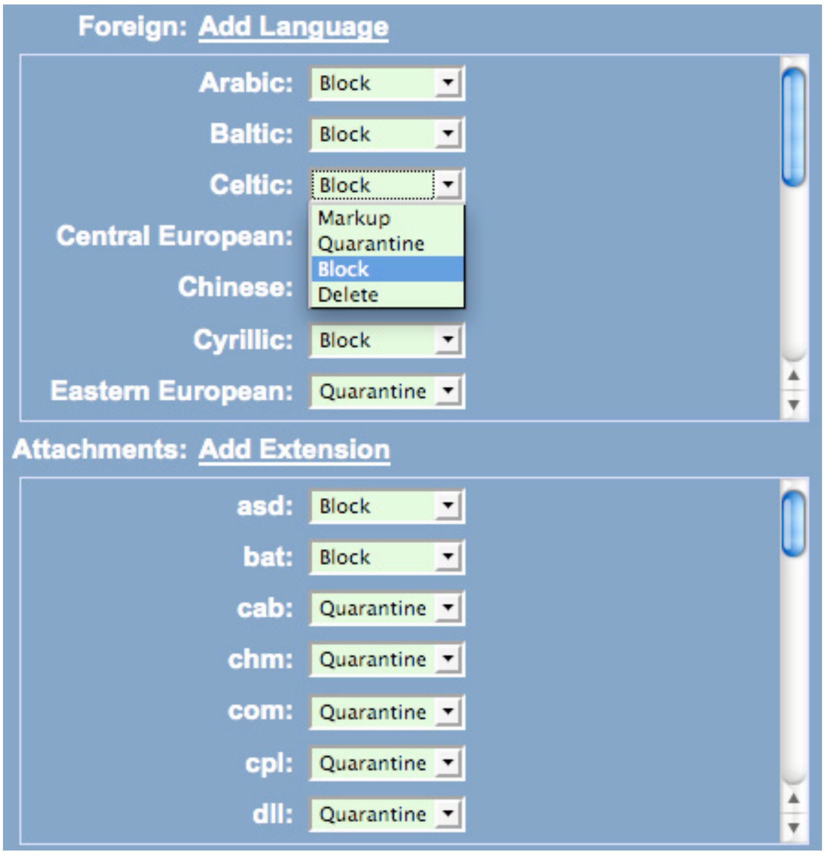
Personal mailbox settings cannot override the blocked policy.

You can also filter emails according to language and the type of extension of the file(s) in the attachment(s) - you can add some of your own.



Virus: Quarantine
Phishing: Quarantine
Adult: Block
Spam:
Junk:
Blank: Block
Forged: Markup
Subject Tag FORGED?

Filtering options according to content



Foreign: Add Language

Arabic: Block
Baltic: Block
Celtic: Block
Central European:
Chinese:
Cyrillic: Block
Eastern European: Quarantine

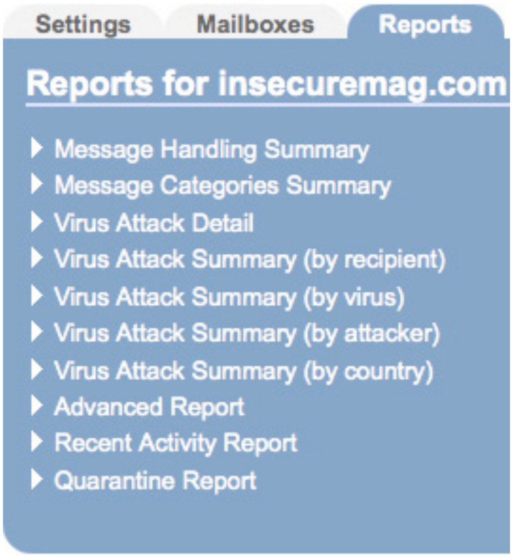
Attachments: Add Extension

asd: Block
bat: Block
cab: Quarantine
chm: Quarantine
com: Quarantine
cpl: Quarantine
dll: Quarantine

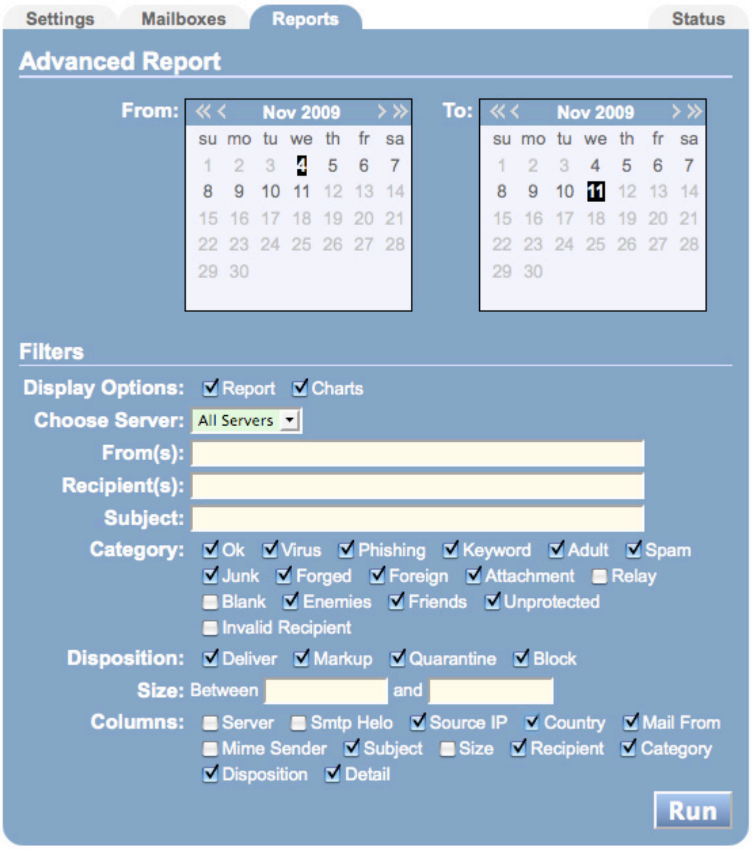
Filtering according to language and attachment extensions

You can make a whitelist and a blacklist, block messages that surpass the size you set, choose what will be the default action for messages that have an unrecognized recipient, the authentication procedure, etc. Existing mailboxes can be detected automatically and new mailboxes can be added manually. They are all configurable.

There are various types of reports you can choose from. I think that by far the most interesting are the various virus attack summaries and, of course, the advanced report, in which you can choose a variety of options.


Settings
Mailboxes
Reports
Reports for insecuremag.com
Message Handling Summary
Message Categories Summary
Virus Attack Detail
Virus Attack Summary (by recipient)
Virus Attack Summary (by virus)
Virus Attack Summary (by attacker)
Virus Attack Summary (by country)
Advanced Report
Recent Activity Report
Quarantine Report

Report list



Display Options: ☑ Report ☑ Charts

Choose Server: All Servers

From(s):

Recipient(s):

Subject:

Category: ☑ Ok ☑ Virus ☑ Phishing ☑ Keyword ☑ Adult ☑ Spam ☑ Junk ☑ Forged ☑ Foreign ☑ Attachment □ Relay □ Blank ☑ Enemies ☑ Friends ☑ Unprotected □ Invalid Recipient

Disposition: ☑ Deliver ☑ Markup ☑ Quarantine ☑ Block

Size: Between and

Columns: □ Server □ Smtp Helo ☑ Source IP ☑ Country ☑ Mail From □ Mime Sender ☑ Subject □ Size ☑ Recipient ☑ Category ☑ Disposition ☑ Detail

Advanced Report options

The hosted service runs on a couple of hundred of Red Condor Message Assurance Gateway appliances. All your data is at any given time stored at various locations around USA, so you can be sure that if disaster strikes at one of the locations, your data is still safe. Its Adaptive Threat Detection technology protects the perimeter layer from DoS and other email service attacks. Merit-based reputation and real-time analysis of evolving email threats stop the email attacks and block spam campaigns before they even enter the network.

All in all, I found Red Condor's Hosted Service to be extremely easy to set up and very effective. I can recommend it to anyone who wants a hassle-free, low-cost solution to the problem of unwanted email.

Zeljka Zorz is a News Editor for Help Net Security and (IN)SECURE Magazine.

The 10th annual RSA Conference Europe in London delivered its educational content through pre-Conference tutorials, keynotes and 70+ sessions across 10 tracks.

The future of information security is now

The information security industry is one of the very few that hasn't been severely impacted by the economic downturn. Many companies in this sector have thrived in the past 12 months. If you're in this line of work, you know why that is - the bad guys are working even harder and the enterprises can't afford to tighten the security budget without immediate consequences.

Art Coviello, President of RSA, opened with a keynote that put into the spotlight some of the issues we are going to face in the near future. As information security goes, good news are far and in between, and as new megatrends that are fueled by technology get into our lives, things are going to get even worse.

The scope of the problem we will face is easy illustrated with numbers. By 2015 there will be 15 billion devices communicating over the Internet and this will include rising fragmented workforces and a sea of mobile workers using social networking and collaborative technologies to do their work. With all the security troubles both organizations and end users are experiencing right now, you can only imagine how many threats will emerge in the next few years.

Executive Chris Young continued Mr. Coviello's discussion by emphasizing the problem at hand: How are we going to secure tomorrow's infrastructures if we're struggling with what we have at the moment? Trying to prevent the use of attractive technologies is a sure way to make security professionals irrelevant. Naturally, we also can't ignore the risks.

There are clear benefits to using new technologies and in order to achieve better and more effective security, it must be embedded into the infrastructure. No single vendor or product is going to solve a common set of problems but the message is that it's imperative to build an architecture that contains everything an organization needs in order to stay as secure as possible.

HERBERT 'HUGH' THOMPSON Ph.D
Programme Committee Chair
RSA Conferences
Chief Security Strategist
People Security
RSA CONFERENCE
EUROPE 2009

How social networking can hurt you

Let's put aside all the positive reasons to use social networking services and focus on the dark side. Most of the time, users don't even realize how much private information they're sharing over these services. There have already been stories about people Twittering or posting on Facebook that they're on holiday and getting robbed, but the problems don't end there.

At RSA Conference Europe 2009, Dr. Herbert Thompson talked about how attackers are launching innovative attacks against individuals and companies using the information shared over public social networking channels.

Dr. Thompson provided real-life examples where he was able to break into online accounts of several people (with their permission, of course). He didn't use complex tools or some esoteric hacking techniques, but rather focused on publicly available information.

The problem is even larger when you realize that you might not even be the one divulging the information. Maybe you're the kind of user that doesn't use Facebook, doesn't have a blog and avoids being photographed. At the same time, your e-mail password reset question may be: "What's my mother's maiden name?". This kind of data may be shared by other people you know and it could become a security problem.

The lesson to be learned here is that online hygiene doesn't necessarily depend only on the information you share, but it depends on everyone around you. If you don't have a Facebook page but a friend posts any personal information related to you, it can come back to haunt you.

We live in interesting times, in which we need to control not only what we do online, but also keep track of the information others are making available online.

Should we define a set of security policies for our friends? Surely, that would be a tough thing to implement.

Microsoft puts a spotlight on browser security

The Internet is growing. With the steady rise of the number of users from emerging markets getting computers and joining the online world, opportunities abound for the bad guys to launch worldwide attacks.

Some of these attacks target specifically these new markets and use password stealers and social engineering techniques. However, there is still a vast range of attacks that targets users through the Web browser.

In general, people tend to be confused when it comes to online security. They read security horror stories in the newspaper and they look to the operating system vendors and browser makers to make sure they are secure. At the RSA Conference 2009 Europe, Amy Barzdukas, General Manager, Internet Explorer and Consumer Security at Microsoft, discussed what Microsoft is doing to improve the security in Internet Explorer 8.

The talk didn't include technical details or upcoming defensie techniques, but focused on existing features and explored the logic behind Microsoft's choices when it comes to implementing certain new features.

While Microsoft's presentations are always top-notch, this one didn't manage to convince me. Don't get me wrong, what Ms. Barzdukas showcased does look advantageous, but the problem is that IE is still heavily plagued by security issues, and the features Microsoft talks about have a tendency not to work as advertised.

However, in recent years, Microsoft has made a notable effort and concentrated on secure development as well cooperating with law enforcement in order to prosecute cyber criminals. If this trend continues (and hopefully increases!), we might just have a product even security professionals will actually like to use.

The fact is that Internet Explorer is still dominating the browser market share so we can keep our fingers crossed that Microsoft continues to take security seriously and raises the bar for consumer protection. The desire to trust is a strong one and a company like Microsoft needs to give good advice and develop software that runs well without degrading the user experience.

Amy Barzdukas said: "We need to be relentless and focus on end users, we need to be transparent and provide them with clear choices." I'd like to add that what they need is to hire cutting edge code hackers to make sure new versions of Internet Explorer are not prone to so many security issues. This will certainly solve some crucial problems end users face every day.

Gathering data and its security implications

At the RSA Conference Europe Advisory Board roundtable in London, new board members and experts Dr. Herbert Thompson and John Madelin, Verizon Business, headed a stimulating discussion related to the role of the different types of data in the context of information security.

Although great efforts are made to secure structured data like social security or credit card numbers, little has been done to take control of the massive amount of unstructured online information.

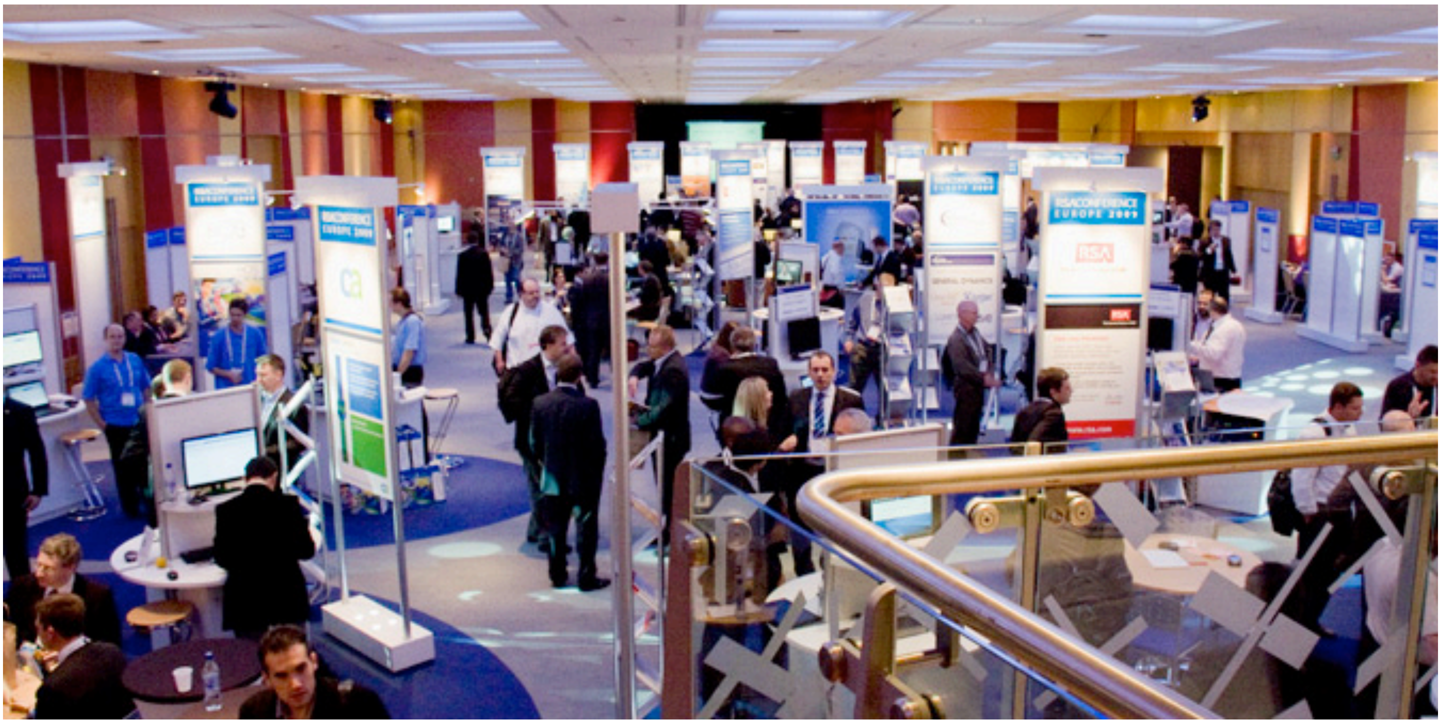
As new technologies proliferate, the line between private and public data is becoming very blurry. When you look at the volume of data that's being generated online on popular services such as Twitter, Facebook or LinkedIn, there's a ton of unclassified data, and some of it is of a sensitive nature. The real problem is that when it comes to new technologies, people are usually taught how to use them and how they can make their lives better, but at the same time, they are not warned about the dangers.

There's been a lot of talk about insider threats in the past year, and one of the aspects that it's usually left out of the conversation is the fact that the most significant problem is not the malicious employee - but the careless one. By not considering the way he treats the data and by constantly making non-intuitive and overall bad decisions, this person can misplace a USB stick on the subway or leave a laptop in a taxi. This kind of information loss doesn't have to be devastating if the data is encrypted, but some kind of data will still be exposed. By acquiring a large amount of scattered data, an attacker can draw some valuable conclusions about his target.

Details about you (available on the Internet) can be used to influence various parts of your life. HR managers routinely check social networking profiles and use search engines to perform in-depth queries about people they consider hiring. This means that while you may be a well-adjusted person and qualified for the job, you might still be judged by what you do in your private life. The problem with data of this type is that it's easily taken out of context.

In a business to business context, data leakages are another towering problem that can be used by your competitor. It's definitely not company policy, but employees could basically "stalk" the workforce of the rival company for broadcasted data. Would they get an advantage? Definitely, it just depends on how much data they're able to acquire.

The questions you have to ask yourself is: "How do you share valuable data that's not going to be useful to the bad guys?"



The U.S. Department of Homeland Security has a vision for stronger information security

by Mirko Zorz

It was not all corporate talk at the RSA Conference Europe 2009 in London. Attending one of the roundtables was Philip Reitinger, U.S. Department of Homeland Security (DHS) Deputy Under Secretary for the National Protection and Programs Directorate. He is the DHS lead on all cyber operations, policy and coordination with interagency, international and private sector partners.

The reality is that with the proliferation of dangerous online threats, the average citizen can ultimately have an effect on homeland security and the US government is making an effort to build a better defensive system. The DHS started with the announcement that they are hiring information security professionals, but they didn't stop there. They are also trying to raise awareness and raise the bar when it comes to understanding the perils of Internet use, and as Reitinger's visit to London shows, they are serious about spreading the message worldwide. I must say, a serious approach like this was long overdue.

As Reitinger pointed out, their goal is to hire 1,000 people over the course of three years. The emphasis is on recruiting highly ethical people that pass a long clearance process. The specific standards are naturally not disclosed, but Reitinger noted that these good guys should be able to put on the "black hat" while still keeping the interest of the public in mind. In other words, the US government is looking for an army of honorable infosecurity professionals that will be able to simulate attackers' mindset and consequently implement successful defenses.

When addressing the issue of the number of experts that the DHS plans to hire, Reitinger emphasized that, in the end, it's not about bulk but about capability. Although, the more top-quality people the government has working for them, the more we can expect them to be able to do.

When it comes to raising awareness of the dangers lurking in the virtual world, a huge drawback is the fact that the age of the Internet inverted the traditional teacher-student roles. Most of the time kids are far more knowledgeable about computers than their parents.

But, at the same time, they're ignorant about most of the risks.

Therefore it's crucial for parents to educate themselves on new technologies so that they can offer better guidance to their children. This is especially important since the misuse of certain aspects of the Internet (such as social networking sites) can lead to the dissemination of sensitive data than can harm not only the child, but the entire family.

Prioritizing between the government, the enterprise and the end users is impossible. All are crucial elements that construct an exceedingly co-dependent ecosystem and all have to be brought to a higher level of security at the same time in order to make any progress. Companies have to mitigate the risks involving their intellectual property. End users should be taking care of their sensitive data. The government must think about a multitude of serious points.

Reitinger said that right now security is too hard. I agree, but I also wonder if it will ever become easier.

At the moment, the government is taking the individual operational centers that have cyber responsibilities and co-locating them so that they can work together as effectively as possible. In the near future, they also plan on co-locating US CERT, the National Coordinating Center and the National Cyber Security Center. The difference this time around is that the government is not doing this entire shift on its own - the private sector will be invited from day one. The idea is to build communication channels that will create, given the type of issues at hand, an underlying benefit for everyone involved.

A sentence stuck with me after the briefing. Reitinger said that we must treat cyber security as a science and make sure we have the correct data and the proper amount of data in order to make the right decisions. Indeed, too many people tend to approach security like religion and base their actions on what they believe it's true, instead of what's really happening.

Sadly, we don't have a rigorous, up-to-date statistical analysis about the current state of network security, online crime, application security, and so on. A variety of vendors release surveys and provide research papers, but these can differ greatly from one another and tend to emphasize significant problems in the area that specific company is invested in. There's nothing wrong with trying to drive sales but this kind of research doesn't really assist in the formation of a clear global threat overview since it's based on experience and it's not exact statistical information.

REITINGER SAID THAT RIGHT NOW SECURITY IS TOO HARD. I AGREE, BUT I ALSO WONDER IF IT WILL EVER BECOME EASIER.

The main problem with obtaining rigorous data is the fact that no one wants to admit to compromises as well as other failures. This is where breach notification laws come in, and help everyone to see the big picture - even if it's an ugly one. This is definitely a start, but unfortunately still miles away from Reitinger's vision. I wonder if we'll ever be able to build a system that provides us with this kind of information and what the costs of such an endeavor may be.

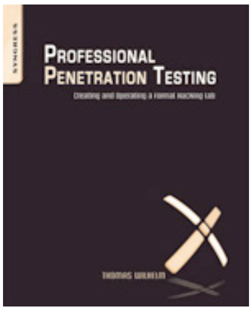
Dangers lurking in the digital world have changed during the years as reputation-fueled attacks were replaced by greed and turned into full-scale organized cyber crime. The risk and threat profiles have increased regardless of the state of the economy. Since the value has moved online, the criminal activity has moved online, too. The key thing here is to focus on what's most important right now: regular patching of vulnerabilities, updating software, moving beyond the username/password to two-factor authentication, and so on.

Both the private sector and the public at large may be hesitant to cooperate with the government for a number of reasons. However, the question remains - can anyone achieve proper security on their own?

Professional Penetration Testing

By Thomas Wilhelm

Syngress, ISBN: 1597494259



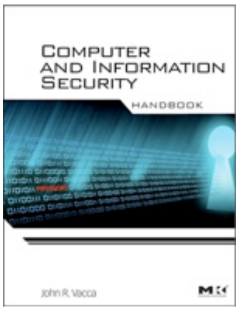
Thomas Wilhelm has delivered pen testing training to countless security professionals. After reading this book you will be able to create a personal penetration test lab that can deal with real-world vulnerability scenarios.

Find out how to turn hacking and pen testing skills into a professional career, understand how to conduct controlled attacks on a network through real-world examples of vulnerable and exploitable servers, master project management skills for setting up a professional ethical hacking business, and more.

Computer and Information Security Handbook

Edited by John R. Vacca

Morgan Kaufmann, ISBN: 0123743540



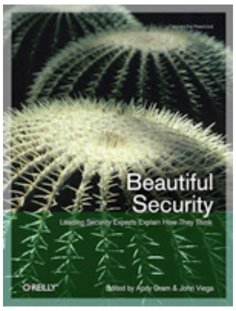
This book presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats.

It also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures.

Beautiful Security

Edited by Andy Oram and John Viega

O'Reilly Media, ISBN: 0596527489

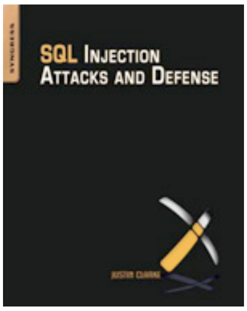


In this thought-provoking anthology, today's security experts describe bold and extraordinary methods used to secure computer systems in the face of ever-increasing threats. Beautiful Security features a collection of essays and insightful analyses by leaders such as Ben Edelman, Grant Geyer, John McManus, and a dozen others who have found unusual solutions for writing secure code, designing secure applications, addressing modern challenges such as wireless security and Internet vulnerabilities, and much more.

SQL Injection Attacks and Defense

By Justin Clarke

Syngress, ISBN: 1597494240



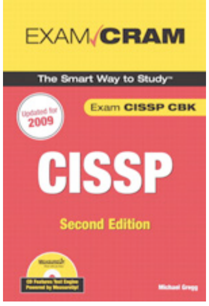
SQL injection represents one of the most dangerous and well-known, yet misunderstood, security vulnerabilities on the Internet, largely because there is no central repository of information to turn to for help.

This is the only book devoted exclusively to this long-established but recently growing threat. It includes all the currently known information about these attacks and significant insight from its contributing team of SQL injection experts.

CISSP Exam Cram (2nd Edition)

By Michael Gregg

Que, ISBN: 0789738066

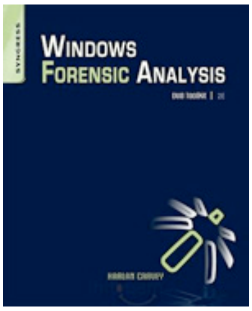


This book covers the critical information you’ll need to know to score higher on your CISSP exam. You'll learn how to: build and manage an effective, integrated security architecture; systematically protect your physical facilities and the IT resources they contain; implement and administer access control; use cryptography to help guarantee data integrity, confidentiality, and authenticity; secure networks, Internet connections, and communications; master the basics of security forensics, and more. The CD features a test engine to help you review your knowledge.

Windows Forensic Analysis DVD Toolkit, Second Edition

By Harlan Carvey

Syngress, ISBN: 1597494224



This book covers both live and post-mortem response collection and analysis methodologies, addressing material that is applicable to law enforcement, the federal government, students, and consultants. The title is also accessible to system administrators, who are often the frontline when an incident occurs, but due to staffing and budget constraints do not have the necessary knowledge to respond effectively. The companion DVD contains significant new and updated materials (movies, spreadsheet, code, etc.) not available any place else, because they are created and maintained by the author.

Q&A: Didier Stevens on malicious PDFs

by Mirko Zorz

Didier Stevens is an IT security consultant well-known for his interest in malicious PDF filed. He's currently working at a large Belgian financial corporation and is employed by Contraste Europe NV, an IT consulting services company. You can find his open source security tools on his IT security related blog at blog.DidierStevens.com.

What drove you to analyze PDFs to the point of becoming THE name associated with malicious PDF analysis? How much time do you spend with malicious PDFs?

Eric Filiol's talk about PDF security at Black Hat Europe 2007 inspired me to analyze the PDF language. I peeked at the inside of PDF files before Eric's talk, and noticed some kind of structure, but never took the time to analyze it further.

As I started to read the PDF Reference document that you can find on Adobe's site, I noticed 2 things. First, although the basic structure of a PDF document is relatively simple, the language itself is very rich. This means that the same information can be expressed in many ways (and thus be used to obfuscate meaning and bypass detection). This complexity implies complex and vast amounts of code to parse the PDF language, which implies more bugs to be exploited. The more code you need, the more bugs you'll have. And complex code is more likely to have more bugs than simple code.

Second, although the PDF language supports scripting (JavaScript and ActionScript), the designers have gone to great length to restrict the misuse of JavaScript in PDF documents. JavaScript in PDF is even more sandboxed than JavaScript in HTML. For example, JavaScript in HTML can emit HTML code (via document.write), but this feature is not present in PDF. JavaScript in PDF cannot emit PDF code. Since the latest versions of Adobe Reader, even benign JavaScript functions like switching full-screen generate an alert asking the user for approval before moving on.

When I started analyzing the PDF language, it took almost all of my spare time. But now, it takes me couple of hours per week at most, depending on what interesting malicious PDF documents I obtain. I'm not a PDF bug-hunter, I'm not actively searching for vulnerabilities in PDF software, although I found a couple, more or less by accident.

What types of malicious PDF files are there? What kind of trouble can they cause?

Actually, there are malicious PDF files that exploit vulnerabilities and PDF files that just contain spam or try to social engineer trusting users to divulge information (like phishing). Most PDF malware exploiting vulnerabilities falls into one of 2 main categories: those exploiting a PDF bug and those exploiting a scripting bug (mostly JavaScript).

PDF exploits are more insidious, because they can't be mitigated by disabling JavaScript. You've probably read advisories where you're encouraged to turn off JavaScript to prevent exploitation of the bug, but sometimes it comes with the warning that disabling JavaScript is not a fool-proof method? To exploit a PDF bug, you don't need JavaScript.

However, the thing is, that many malicious PDF authors don't have the skills to achieve full EIP control. They know how to trigger the bug and to make the flow of control jump to a random/fixed place in memory to continue execution, but they lack the skills to jump to an arbitrary place in memory (e.g. full EIP control) where they've prepared the shellcode to be executed.

How do they make up for their lack of skills (or resources)? They resort to a heap spray in JavaScript. It will store a huge amount of copies of the shellcode in memory, so that the probability that the flow of control jumps to a place in memory where shellcode is located increases significantly. If you've opened a malicious PDF document and noticed a long delay where Adobe Reader is unresponsive, you've noticed a heap spray in action. The long delay is caused by the JavaScript filling the memory with shellcode. Disabling JavaScript for PDF bugs will mitigate exploit code that uses a heap spray. But if the attacker is skilled enough (this is more likely with targeted attacks), the PDF bug will be exploited without resorting to JavaScript and disabling JavaScript won't help you. Then there are the JavaScript bugs, where vulnerable JavaScript functions are exploited. Disabling JavaScript is an effective way to deal with these.

The kind of trouble PDF files can cause is actually determined by the payload and the environment they execute in. Malicious PDF documents are opened by users, and thus the exploits run under the user account. In short, PDF files can cause the same trouble as most viruses. Because this is what most malicious PDF document do: the exploit cause the shellcode to execute, which in turn downloads and executes a malicious executable from the Internet (a Trojan). If you're a local admin and you open a malicious PDF document that downloads a botnet Trojan, it will take full control of your machine, and you won't notice it.

What tools do you use during your research?

I started by using a hex editor and PDF software (Adobe Reader, Foxit Reader, Sumatra PDF), but later on I developed my own tools in Python to generate PDF documents and tools to analyze PDF documents. My PDF generation Python module comes in handy when I'm researching a new feature or vulnerability and I try to make my own proof-of-concept samples.

PDFiD and pdf-parser are my 2 analyzers. PDFiD is a type of string scanner and it helps you identify malicious PDF documents. One of the things it will tell you is if a PDF document contains JavaScript. If you're suspicious about a PDF document and PDFiD tells you it contains JavaScript and is only one page long, then you're probably right about your suspicion and you shouldn't open it. PDFiD is also hosted on VirusTotal. When you send a PDF file to VirusTotal, it will also be analyzed by PDFiD (the reports comes after the AV detections).

If you want to further analyze the PDF file to know exactly which harmful actions it will perform, you can use my pdf-parser to extract the payload. To analyze the embedded JavaScript, I often use Spidermonkey (the Mozilla JavaScript interpreter) I patched. For the shellcode, I use sctest from the libemu software, OLLYDebug and IDA Pro. On occasion, I also use pdftk and PDF Origami.

If you could sit down with the core PDF team at Adobe, what questions would you ask them? What recommendations would you give them for the development of future versions of Adobe Acrobat?

I would like to know what they plan to do in order to restrict the damage caused by a buggy Adobe Reader. I'm not talking about what they plan to do to limit the number of bugs, but how they architecture their products to limit the exploitation range of the bugs. I would tell them to be more defensive. Adobe Reader is exploited, but how can I limit the damage the exploit can cause?

I do understand that they can't disable JavaScript by default because that would alienate too many of their “security-unconscious” customers, but they could fork their products: a restricted version and a full version. The restricted version would contain less features and thus have a limited attack surface. They could even go further in the security design: for example, the restricted version would not be able to create new processes (and thus not be able to execute downloaded Trojans). Also, I don't believe they use ASLR in Adobe Reader or run with a low integrity level (both are Vista features).

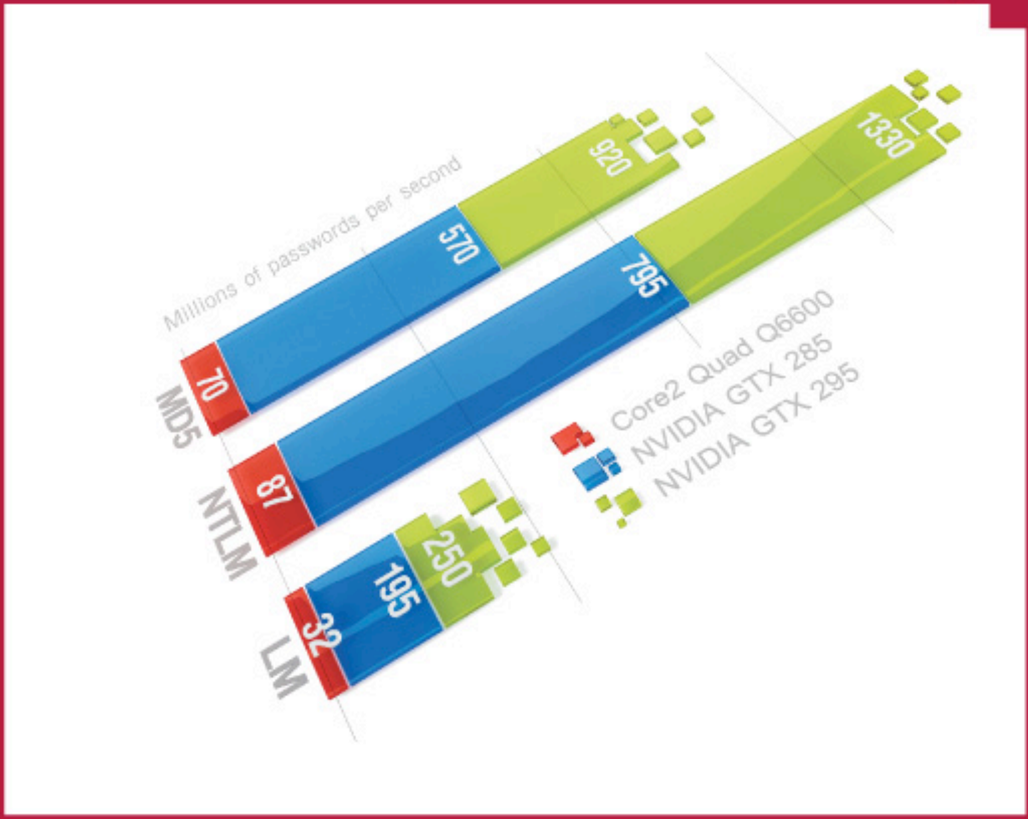
The average user is generally not aware of the dangers that malicious PDFs can pose. What advice would you give to someone that would like to protect themselves against this problem?

The best advice I can give is to run with a limited user account. This will not only protect you from malicious PDF documents, but also from other malicious files and documents, like Microsoft Office documents (PowerPoint anyone?). The reason why this helps with malware found in-the-wild is because most malware does the following: the exploit executes shellcode, which in turn downloads a trojan, writes it to SYSTEM32 and executes it. The shellcode used in these exploits is very simple: if it fails to write to SYSTEM32, it fails to execute the trojan. Limited user accounts can't write to SYSTEM32. Trojans are also very limited in their action if they can't run with admin or system rights. I've written an article for issue 21 of (IN)SECURE magazine where I explain how malicious PDF documents can exploit a vulnerability even if the user doesn't open the PDF documents, but it's extremely rare to find such exploits in-the-wild and there are ways to mitigate this. If you use Windows Vista or later, and haven't disabled UAC, then Adobe Reader will run with a restricted user account. If you're stuck with Windows XP, switch to a non-admin account. If that's not possible to you, use DropMyRights or StripMyRights to run Acrobat Reader with a restricted token.

This advice will help you a lot when we're talking about malicious PDF documents found in-the-wild. This is malware that's targeted to all Windows users and distributed by criminals via e-mails, websites, illegal software, etc. Unfortunately, all bets are of for targeted attacks. Malware written for targeted attacks, unlike malware found in-the-wild, is designed to work around the security measures of its target. In this case, the malware author knows his target (you) and designs his malware to operate in your environment. For example, if they know you run with a limited user account and they want to steal your confidential documents, they'll write malware that does this without needing admin rights.

Based on your experience, what kind of PDF security issues do you think we can expect in the near future?

I believe there are still many bugs to be exploited in Adobe Reader. Malware authors will also start to target Foxit reader, because its market share is increasing significantly and because it lacks many features of the PDF language and thus its attack surface is reduced. Flash (ActionScript) exploits will increase, caused by the increasing market share of Adobe 9 (prior versions don't support embedded Flash). For the longer term, I expect malware authors to develop LUA malware (in general, not only PDF). Due to the increasing market share of Windows Vista and Windows 7, more users will use restricted accounts and ultimately, malware authors will have to take this into account for the design of their malware.


Millions of passwords per second
MD5
70
570
920
NTLM
87
795
1330
LM
32
195
250
Core2 Quad Q6600
NVIDIA GTX 285
NVIDIA GTX 295

Protecting browsers, endpoints and enterprises against new Web-based attacks

by Nick Lowe

Security technology has come a long way in the last 850 years, but we can still learn a thing or two from our medieval ancestors. After the Norman conquest of Britain, the new administrative centers and power bases of the country were quickly strengthened against attack.

Hilltop fortifications were remade as imposing stone castles, with multiple layers of security built in. These protected the newly centralized trade and business operations against theft and external attacks, and controlled third-party access – rather like the perimeter defenses, intrusion protection systems and VPNs of a typical company's network.

And if important figures left the protection of the castle, they would not only wear body armor, but also carry a shield for additional, mobile defense against all types of weapons. But do corporate endpoints – laptop computers and smartphones – have the same level of protection?

Unfortunately, it seems that unlike their medieval counterparts, modern mobile workers are no longer adequately prepared for attacks when they are away from the relative safety of the corporate 'castle'.

Why is this? Well, attack methods are changing, and the dominant threat to endpoint security now combines historically effective attacks with newer, more elusive methods of delivery and infection. As a result, attacks are extremely difficult to stop, and carry more serious consequences than previous exploits.

New web-based attacks have emerged and are becoming more common. And while traditional endpoint security controls are still important, they are unable to fully cope with these new attacks, because they focus on the wrong things.

New controls are needed: web security must extend to users' behaviors as well as to the PC software and configuration. Signature-based methods alone won't stop new attacks, and neither will simply removing malicious software.

What new approaches are needed? Let's look in detail at how enterprise attack vectors are changing and evolving, at the motivations behind them, and how they get around traditional endpoint security. Following this, I will look at a new approach to protecting endpoints against these attacks, both reactively and preemptively.

The new attack front: Web usage

One of the key malware developments over the last 5 years is the move from email-borne to web-borne attacks. Exposure can occur if a business PC is used for business or personal use on the web.

The issue is, organizations often have a false sense of security, because traditional controls for protecting enterprise endpoints do not secure against web-based threats. Here's a small sample of recent incidents in which criminal hackers have used the Internet as a platform to distribute their wares:

In July 2009 web services provider Network Solutions disclosed that hackers broke into its servers and stole details of over 573,000 credit card accounts from its customers. The company discovered in early June that its servers had been hacked into by unknown parties. The servers provide e-commerce services such as Web site hosting and payment processing to nearly 4,500 small to mid-size online stores. The hackers left behind malicious code, which allowed them to intercept financial information from people who made purchases at the online stores hosted on those servers from March to June '09.

ORGANIZATIONS OFTEN HAVE A FALSE SENSE OF SECURITY, BECAUSE TRADITIONAL CONTROLS FOR PROTECTING ENTERPRISE ENDPOINTS DO NOT SECURE AGAINST WEB-BASED THREATS

Also, in June 2009, more than 40,000 web sites were hit by a mass-compromise attack dubbed Nine Ball that injected malware into pages and redirected victims to a site that attempted to download further malware. In September 2008, malware was planted on the Business Week web site through an SQL injection attack. According to statistics from Google, 10% of the pages on the Business Week web site were serving malware to visitors.

These new web-based attacks have three key properties:

- Threats are much less noticeable because they are designed to be silent on the victim PC. Only a loss of PC performance or stability might be apparent.

- Threats are targeted and sent in small batches to avoid detection. It's now rare to see major headlines accompanying a threat - the exception being this year's Conficker outbreak, which still has AV researchers puzzled as to motive.

- Consequences are serious and may include personal data loss/identity theft, as well as the silent takeover of individual PCs to create botnets - thousands of computers that can be controlled at once to launch large-scale attacks.

Web-based attacks include "drive-by" downloads, PHP and AJAX exploits -all retaining the worst characteristics of the recent past. They remain financially motivated, extremely damaging, and relatively silent and unnoticeable. Like earlier threats, they are once again viral and widely distributed.

Many enterprises assume they already have sufficient Internet security to prevent these web-based attacks - but remain unprotected. Unfortunately, most providers of endpoint security software do not yet offer the appropriate controls to prevent exploits by today's web-based threats. Let's take a look at why is that.

Where traditional controls fall short

PC-based security software - whether a single-user suite or a corporate endpoint solution – is still critically important, but is no longer enough to combat these new web-based attacks. Each type of solution arguably falls short in at least one important way.

Signature solutions

This category of solution includes PC-based forms of security such as antivirus, anti-spyware and signature-based IPS. Signature solutions had difficulty keeping up with attacks a decade ago, and this was before modern automated, morphing and small-batch custom attacks were available.

In the face of modern attackware, it is no wonder that experts and analysts have written hundreds of articles predicting the decline and death of antivirus. After all, antivirus software reacted too late for "Melissa" in 1999, and for "I Love You" in 2000—all of which were mass-mailed, relatively low-tech (slowly morphing) viruses. How can antivirus (and its cousins anti-spyware, IDS and similar) keep up with today's that are blended, and more advanced?

The simple truth is - they can't. Recently, threats have appeared in small batches (thousands, not millions of infections) that constantly morph, change their signature on every PC they hit, and stay hidden.

While antivirus, anti-spyware and similar security solutions are useful for "clean-up duty" in the aftermath of an attack, they are ineffective as a defense for some zero-hour web-based attacks.

Firewalls

Desktop firewalls are effective against zero-hour, morphing, and targeted network attacks. They follow a simple and elegant rule: do not allow any traffic onto the PC unless the user and/or administrator specifically allow it.

This "reject all unless known good" rule is in direct opposition to the signature rule of "allow all except known bad." However, there are a couple of downsides to desktop firewalls. First, they generally allow user-solicited traffic on TCP port 80, the standard port used for HTTP traffic.

When the user initiates an HTTP connection, the firewall acts as a wide-open highway that brings traffic straight onto the PC. Most studies show that spyware and other malware exists on over 80% of PCs running firewalls.

Also, firewalls are focused on protecting users' computers, not users' behavior. Similarly, they do little to prevent direct online contact with malware.

Desktop firewalls continue to be critical components of endpoint security because they provide network-based protection in a way that nothing else can. When it comes to web-based attacks, however, they are not fully effective.

Different transactions need different security controls

In the face of modern web attacks, new signature-based security solutions have emerged that try to protect users online. These new transaction security products use signatures of known bad web sites, including phishing sites and spyware distribution sites. Some also contain signatures of malicious web site behaviors. This information allows them to identify and prevent users from visiting web sites at a more general level, and keep a more secure environment.

These signature solutions are the first response to the new attack types, but they are not the most effective. They work as partial solutions but are no match for the threat environment described earlier, in which hackers design dynamic, morphing threats that get past signature systems. Just as today's viruses can bypass antivirus systems, modern web attacks evade these signature-based web transaction security products.

This means supplementing the traditional security 'armor' for endpoints (firewalls, antivirus, antispyware, etc.) with additional protection specifically for the web browser application. Just as medieval noblemen would carry a shield to stop attacks before they hit the body, so the web browser needs a shield to absorb attacks, and protect identities and data against both high profile and stealthy infiltration attempts.

Making a virtual shield

There are several technologies that have emerged to fight web-based attacks without the use of signatures. These can be classified into two broad categories:

Manual virtualization systems: These systems virtualize all or a part of the host computer, and require that all changes from the Internet to the PC take place in the virtualized system itself. This way, nothing harmful can transfer from the Internet to the PC.

While this seems like an elegant solution, it requires the maintenance of both a virtual machine/file system and an actual one. It also requires making ongoing decisions about both systems - something that the average enterprise user is unwilling or unable to do.

Method-blocking systems: This technology focuses on one or more known browser vulnerabilities that allow hackers to target users with malicious code. For example, cross-site scripting presents a vulnerability that enables a hacker to inject malicious code into other people's web pages.

A method-blocking system actually interferes with this feature, thus removing the method by which these attacks can be carried out. While these systems are important and necessary, their shortcoming is that they block only some methods of attack (usually just one), and therefore cannot stand on their own against the sheer breadth of tactics that web-based attacks employ.

How are these combined to give the best protection against newer attacks?

Stopping the full range of web-based attacks

The first step is taking the correct approach to virtualization – that is, choosing the right elements of the OS and relevant applications to virtualize.

The aim of virtualization is to protect the user's web session by enclosing it in a "bubble of security" as they browse – while keeping the process simple and transparent for the user. It's a process that can be called precision emulation.

With this approach, only those parts of the operating system that the web browser is able to access need to be virtualized. This means that there is no large installation, much less system memory use and associated performance degradation, and no need for the user to keep track of multiple operating systems or file systems. The virtualization engine should also automatically maintain the virtual system it creates.

For example, each time a user browses the web, a number of changes -most of them innocuous - are made to their computer system. A specific case is the processing of an online form to become a registered user of a web site - often the site's server creates a cookie that is placed onto the user's computer.

Under precision emulation, the virtualization engine should follow a very simple, firewall-like rule. All user-solicited downloads from the Internet write to the computer just like they usually do. But unsolicited downloads such as drive-bys write to the emulation layer, never touching the computer.

The result is that users can browse to any web site and click on any link without worry because all unknown or unwanted changes (from browser exploits and drive-by downloads, spyware, and viruses) are made to a virtualized file system. So only the items the user purposely downloads are placed on the endpoint PC.

Precision emulation: Under the hood

Precision emulation works by intercepting Microsoft Windows interfaces to directly access files and registry keys. In doing so, the process creates two major components:

- A virtualization engine to create a duplicate Windows file and registry system
- A hooking engine to selectively redirect NT kernel calls for virtualization.

The purpose of the hooking engine is to intercept indiscriminate NT kernel calls. At this point, it decides if a kernel call was solicited by the user or was automatic, as in a drive-by download. The engine determines this based upon whether or not expected UI calls were made (user initiated) or not (automated, drive-by).

User-solicited calls are made to the native system component as always, so as not to interrupt the user's normal workflow.

Unsolicited calls, however, get applied to the virtualization engine and virtual file and registry system, and therefore never reach the actual computer. At the end of each browsing session, the virtual layer can be reset and scrubbed to a clean state.

Without this approach, user accounts often run with administrative privileges, giving applications freedom to read and write to the operating system and kernel. This allows malicious code to directly access and harm the operating system.

The benefits of web shielding

To conclude, placing a virtual shield around the browser has three core security benefits.

It is signature independent - it's a zero-hour system that employs a simple firewall-like rule: reject all changes to the user's PC unless the user specifically solicits them.

It protects the user's PC from the moment of connection - as web-based attacks can occur the moment the user encounters a web site, the shield approach does not passively wait for malware to transfer from the Internet to the PC. The virtualization layer shields the user immediately and through the whole session.

It's unobtrusive - no special setup or maintenance on the part of the enterprise administrator is needed, and all virtualization activity is invisible to the user and requires zero maintenance.

The latest generation of web-based attacks requires a solution that supplements and goes beyond the best of traditional endpoint defenses, including signature-based security, updates to virus and spyware eradication mechanisms, and firewalls. It needs to shield the browser - the user's point of contact with the Internet - from the endpoint's operating system and file system, to stop unauthorized changes.

After all, if you're going to put armor on your endpoints, why not do what our medieval ancestors did, and use a shield as well?

Nick Lowe is the Check Point Regional Director for Northern Europe (www.checkpoint.com).

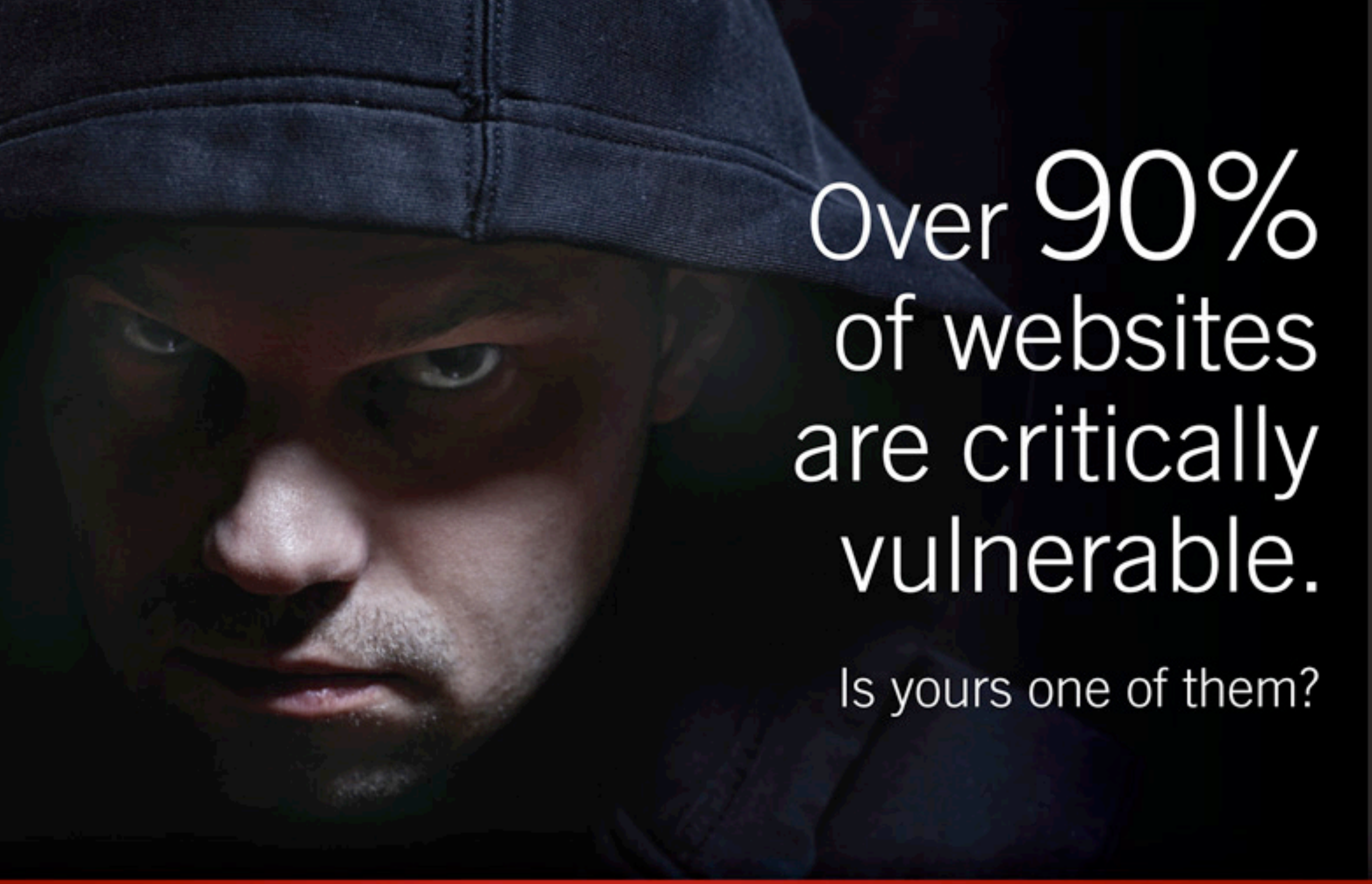
Here are some of the Twitter feeds we follow closely and can recommend to anyone interested in learning more about security, as well as engaging in interesting conversations on the subject. If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter.

Our favorites for this issue are:

@MorrMac
Sean Morrissey - Forensic analyst, Mac and iPhone author, speaker.
http://twitter.com/Z3r0Point

@intel_chris
Christopher Clark - Intel HW/SW architect.
http://twitter.com/intel_chris

@iia_security
Maintains the Internet Industry Association's security portal.
http://twitter.com/iia_security



SECURE YOUR WEBSITE

Hacker-Proof Your Website with Cenzic's SaaS offering

Cenzic provides Web security assessments as a service through the cloud. No installation of hardware or software is needed. Get your Web applications assessed remotely from Cenzic experts and stay ahead of the Hacker curve. It's that simple.

Request a Web Security HealthCheck for your Website today, visit:

www.cenzic.com/gethealthcheck
1-866-4-CENZIC

CENZIC CLOUD COMPUTING

EASY AS 1-2-3

AFFORDABLE.

RELIABLE.

FAST.

CENZIC

Mobile spam: An old challenge in a new guise

by Hugh McCartney

In markets worldwide the mobile phone has become ubiquitous. As the revenue opportunity moves from voice to data, operators must work harder than ever to ensure their customers continue leveraging their mobiles for services beyond voice. According to a recent consumer research Cloudmark conducted, nearly two thirds of users can't manage a week without their mobile phone. While this reliance on mobile phones bodes well for the industry, the adoption of mobile services such as mobile banking, mobile commerce and mobile marketing is by no means assured.

With the explosion of SMS usage and the increasing use of mobile Internet and diverse mobile applications, mobile users and operators alike are finding themselves faced with a range of new security threats targeting mobile devices. What was once confined to email has now reached mobile devices, and spammers and hackers are realizing that mobile networks often have inadequate protection against mobile spam and fraud.

This lack of protection makes mobile networks prime targets for unsanctioned activity. Unlike with email, where users are educated about spam and malware, mobile users have an inherent trust in their device, making them more susceptible to falling victim to mobile attacks – so it's easy to see why mobile spam is on the rise.

The scale of the problem

In Asia, up to 50 per cent of all SMS traffic is spam, the highest percentage in the world. This can be attributed to the fact that 'all-you-can-eat' texting plans are standard there, meaning the cost of sending a message can be negligible – sometimes less than $0.001 per message. In addition, operators are struggling to identify sources of spam as many spammers are leveraging SIM cards they simply dispose after their effective use.

In North America, SMS volumes are beginning to reach network capacity and there is a significant risk of threats causing service outages. While the figures are lower in the UK and Europe, they are still significant.

A recent research that Cloudmark carried out among consumers found that two thirds (66%) have received unwanted or unsolicited messages on their mobile phone, and while the majority of spam messages could simply be seen as nuisance (e.g. SMS marketing), an alarming 29 per cent had received malicious spam such as phishing messages, fraud messages or messages containing inappropriate content.

The most common threats

Mobile threats are increasing rapidly in sophistication and frequency. Some of the most common mobile spam types – malicious and otherwise – are listed below:

Premium-rate number scams: One of the most common types of spam, and it can be quite pernicious. Users are sent a message that tricks them into calling back or replying via SMS. The number the user responds to is actually registered as "Premium-Rate" number, and is charged at a significantly higher fee on the bill. Some of these scams also sign users up for ongoing subscription services when they respond, which end up being added to their mobile phone bill each month. Most countries have a code of practice regulating these services, and most providers of these services are legitimate. However, users should watch out for messages (always unsolicited) that ask them to reply to a premium-rate "shortcode" using vague messages.

Mobile threats are increasing rapidly in sophistication and frequency.

Phishing: Phishing is a well-known term when applied to email, and is now becoming common on mobile phones as well, often referred to as SMishing. It can be quite hard to detect on a mobile, because many users don't question the trustworthiness of the SMS messages they receive that claim to be from their bank, mobile phone operator or credit card company. Mobile phishing spam messages lure users to websites which look like official bank web sites, and proceed to steal login information. This can lead to identity theft, or using personal details to add premium services to the user's phone bill. Some phishers have taken this one step further and even set up automated voice response systems that sound like the user's bank. Since most people simply don't expect to be scammed in this manner on their mobile devices, these new fraudulent schemes are often very successful.

Viral hoaxes: Viral hoax messages, while not typically harmful, are often sent around and can be very annoying. These hoaxes attempt to get users to forward a message to all of their friends, in return for some reward (financial or even to bring "good luck".) As these types of message normally come from the user's friends they appear trustworthy, and this alone is often enough to encourage people to follow the instructions in the message.

Mobile viruses: Viruses do exist in the mobile world and are growing in sophistication and penetration capability, particularly with the rise of smartphones. Transmitting viruses in an SMS message is a complex operation, but is already being done. SMS viruses are typically unsolicited SMS messages containing a web URL that look very enticing (e.g. "Britney's bare-faced cheek!" or "Video of WWII bomber found on moon!"). This URL takes users to a website that downloads a virus to their mobile phone, and in the future could even be used to turn mobile phones into spam-sending bots of the type commonly found among PCs, which would have serious implications for users' phone bills.

The ROI of mobile spam

Mobile threats will continue to increase as spammers have much to gain. Not only do spammers make money from users purchasing products or falling victim to scams, but they do so at very little cost since the price of sending a message has dropped so dramatically in recent years. Criminals that have traditionally used email as the most effective way of targeting victims have found themselves thwarted by advances in technology and have quickly moved on to a more lucrative, and at present less defended territory.

The problem for operators

Our research shows that these mobile threats are not only intrusive and annoying, but they also put consumers at risk of fraud and identity theft and are subsequently eroding consumer confidence in the security of their mobile phone and the services they access on it. Half the consumers Cloudmark surveyed don’t think the information they send on their phone is secure and more than two thirds said they wouldn’t use value-added services such as mobile banking, while a further 37 per cent wouldn’t shop online due to mobile security concerns. In addition, it is clear that the consequence of letting spam proliferate can be hugely damaging to brands’ reputations, as well as contributing to customer churn and a rise in customer complaint calls. The increase in spam is also putting pressure on operators’ networks and negatively impacting customers’ quality of service.

These combined factors are threatening the future growth of operators’ revenue from mobile data services. Mobile operators must ensure they take the necessary steps to prevent this increase in mobile messaging abuse and fraud, before mobile spam becomes as ubiquitous as the mobile phone itself.

The need for network protection

The importance of network level protection for the mobile network was highlighted by the recently announced SMS vulnerability that affected Apple iPhone, Palm Pre, Windows Mobile and Google Android devices. The vulnerability enables an attacker to gain full access of a device by sending specially coded SMS messages to the device.

Once a patch was available, the process of getting millions of subscribers on the network to update their devices to the latest patch level, across multiple smartphone operating systems, was an immense task. Some of these devices, including the Apple iPhone did not support over the air provisioning for a patch – meaning that users had to manually upgrade their devices themselves. Waiting for users to do this on their own can take months – all the while leaving users vulnerable to these serious attacks.

Conversely, solutions that provide messaging abuse protection in the network infrastructure could prevent this type of attack from infecting devices immediately. Network level solutions are able to block malicious SMS messages before they are sent to the device, preventing the messages from ever arriving to the device in the first place. This has several benefits.

Network level solutions can:

1. Protect multiple device types
2. Provide protection without user involvement or awareness
3. Provide protection without device manufacturer or operating system vendor involvement
4. Immediately protect all subscribers upon deployment.

This type of protection requires a relatively advanced solution to be in place in the mobile network infrastructure. I believe that we will see this become more and more common as a means to protect against attacks of this nature in the coming months and years.

Conclusion

There are many lessons to be learned from the fight against email spam, but perhaps the most important is that only by investing in the necessary technology to safeguard operator networks will customers feel confident using their mobile phones, and take full advantage of additional revenue-generating services. Scammers will always prey on the weakest and most lucrative targets, so the quicker the European mobile phone industry clamps down on spam, the more effectively it will be able to prevent spam levels from reaching the extremes already experienced in Asia.

Hugh McCartney is the CEO of Cloudmark (www.cloudmark.com). Formerly an independent director of Cloudmark's board, Hugh also served as chairman of UK-based Scapa Technologies, an innovator in security testing solutions; as an executive and chairman of Neverfail, a global provider of fail-safe technologies; and as chairman of Centennial Software, a developer of network discovery tools.

Report by Mirko Zorz

After visiting several computer security events and being impressed by the energy and the open exchange of knowledge, a small group of people dreamed of creating a hacker conference of their own. After much hard work, BruCON was born.

Benny K., one of the organizers, comments that an event like this was absent from the "land of beer". With all other Belgian information security gatherings having a strong commercial undertone and, according to some, missing balanced research, the BruCON announcement was met with enthusiasm both online and offline. Soon volunteers began gathering in Brussels and organizing the minutiae of what was to become an important event for the European hacker and security research community.

It's worth noting that this conference is made by the community, for the community and everyone's input is taken into consideration. Some may think that this approach can alienate sponsors and make sure that the presented is not up to scratch with other security conferences that have rich corporate backing, but as I've witnessed first hand, this couldn't be farther from the truth.

Months of hard work and coordination came to an end last week, when BruCON opened with two days of workshops followed by two days of lectures, lightning speeches, classes and informal gatherings of like-minded individuals interested in the intricate details of the world of information security.

Unlike other events that are largely shaped by commercial sponsors that even have the power to prevent certain presentations, BruCON intends to welcome technical speeches that may be turned down at some events. In a conversation with Eric Filiol, who presented on cyber attacks, I realized how much some speakers welcomed this sort of gathering. With their studies being rejected at other events where organizers brim with fear that sponsors are not going to like them, BruCON has the unique possibility of bringing together cutting edge hackers that may not even want to submit to events that are enshrouded in a corporate veil or predictable talks.

The event was held at the Surf House in Brussels, a monumental concrete dwelling that evocates images of Orwell's grim 1984. On the inside, it is one of the most comfortable and visually pleasing conference venues I've visited in the past decade. Since BruCON had one track this year, all of the talks took place in the main auditorium. This was definitely an international conference, with 300 attendees from all over the world. The talks covered a lot of different ground and topics, including cryptography, social engineering, SQL injection, cyber warfare, botnets, hackerspaces, kiosk hacking, and a lot more. Some of the material has been prepared exclusively for this event and won't be available elsewhere which is definitely another good reason to attend next year.

Between talks, attendees gathered in the Hacklounge, a one-of-a-kind area that looks like like a set for a movie about hackers. Those of the old school certainly appreciated the retro feel of the space where you could play arcade games. The same space hosted our meals, the EFF charity auction, and served as an all-around meeting place where attendees met many of the faces they only knew in the virtual world.

What would a hacker conference be without a challenge? PDF analyst extraordinaire Didier Stevens was one of the designers of the Hex challenge, where the first prize was an Asus netbook. The quiz was intended for all levels of expertise and included topics such as the history and culture of hacking, penetration testing and reverse engineering.

BruCON is a gathering of security aficionados that shows towering promise. For those who attended, the air in the halls was filled with curiosity. Finally, a European event that delivers well-crafted information security knowledge in an informal atmosphere where the only important things are knowlege and networking, no commercial strings attached. Don't you dare miss BruCON next year!

Are you putting your business at risk?

by Marc Hocking and Kathleen Porter

Data loss is a serious issue that affects countless businesses daily, yet data breaches continue unabated. According to the Ponemon Institute, compromised data cost U.S. companies an average of $202 per customer record in 2008, an increase of nearly 40 percent since 2005. The average cost of a data breach in 2008 was $6.65 million. These figures are staggering, so why are businesses still falling victim? Are they being careless? Should there be more government intervention?

The impact data loss has had and continues to have on U.S. citizens and businesses has already resulted in a wide variety of data security-related legislation at both the federal and state level.

A number of federal laws have been adopted requiring companies to take measures to protect and secure the most sensitive information, while state legislation has focused more on providing notice to consumers in the event of a breach. To date, 44 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted laws requiring companies to notify individuals if their personal information has been compromised.

Data loss risks

As embarrassing as it is to publicly admit that your business has suffered a data breach, the possibility of loss of customers, revenue and share values is even worse.

Data breaches cause also devastating monetary losses. In addition to the figures discussed previously, another recent Ponemon study estimated that every lost laptop can cost companies up to $200,000, with an average cost of $49,246. Often people hear an amount that high and think that’s not possible, but when you think about all of the additional costs involved in a breach - such as internal investigations, forensic experts, consumer notification, crisis management, call centers, credit monitoring, attorney fees, payment card industry fines, creating and disseminating software patches, litigation expenses, subpoenas or other government action by state Attorneys General or the Federal Trade Commission - it adds up quickly.

One of the reasons why breaches continue unabated is that there are countless ways to lose data. Whether it's malicious or inadvertent, some of the most common ways in which data is lost include network hacking, insecure wireless networks, lost or stolen laptops and portable devices, media lost in transit, unredacted online records, breaches in physical security, phishing or pretexting scams, botched software upgrades/updates, insecure disposal of print and electronic media, human error, rogue or disgruntled employees, misdirected mail and faxes, malicious software, and/or failings by vendors and service providers.

Surprisingly, a recent study by Verizon found that 74 percent of data breaches investigated were caused by external sources, 32 percent were linked to business partners and only 20 percent were caused by insiders - a finding that may be contrary to certain widely-held beliefs.

Real world examples

Whether a breach involves unauthorized access into a company's systems by an employee or remote intruder, or occurs because of a loss or theft of physical property, it almost always makes news headlines and affects the company negatively. Some recent examples include:

• Continental Airlines reported in January 2009 that a laptop containing records used for security background checks was stolen. The laptop, which had been in a locked office in New Jersey at the time of the theft, contained the individual names, addresses, Social Security numbers and fingerprints of more than 200 individuals. The reports do not indicate that the laptop or the records were encrypted.

• Also in January 2009, Heartland Payment Systems, one of the nation's largest credit card payment processors, announced one of the largest data breach in U.S. history. The company learned of the breach after Visa and MasterCard notified it of suspicious activity surrounding processed card transactions. The company determined that intruders had hacked into Heartland's computer system and accessed data that was not properly encrypted. The exact number of victims remains unknown, but the potential is exceedingly high – Heartland processes 100 million payment card transactions per month for more than 175,000 merchants. Heartland has since been sued for damages and relief stemming from the delay in notifying its customers.

• In 2007, TJX, the parent of leading off-price home and apparel retail stores such as TJ Maxx and Marshalls, reported that on multiple occasions dating back to 2005, hackers had gained access to approximately 45.7 million unencrypted credit and debit card numbers. The investigation revealed that a financial fraud ring exploited the company's outdated encryption systems to access financial data being transmitted between hand-held price-checking devices, cash registers and the store's computers. Officials have made more than 11 arrests globally in connection with this breach, with at least one conviction. To date, company and external estimates on the cost of the breach range from $256 million to $1 billion. Some 20 class actions brought by individuals, card issuing banks, state banking associations and shareholders were eventually settled out of court. The retailer is still defending claims brought by two financial institutions. There were also investigations by federal and several state enforcement agencies.

• In October 2008, an Ohio medical insurer reported the loss of 11 disks containing personal information of 36,000 employees and retirees. The disks were mailed from the insurer's office to the plan office, both in Columbus. Apparently, because the disks were mailed without sufficient postage on the envelopes, they did not arrive at their destination and remain missing, perhaps within the postal system.

Not only is a company at risk of data loss relating to its customers' sensitive personal information, but also its employees' confidential information. For example, in July 2008, the Washington Metropolitan Area Transit

Authority accidentally published its employees' Social Security numbers on its Web site. While a company may not suffer the same level of embarrassment or scrutiny it would upon losing customer data, the employees' trust in the organization may be lost, and worse yet, the company may be held financially liable to the employee.

Company carelessness can also lead to avoidable data loss. In 2005, a disgruntled former Kaiser Permanente employee posted links on her personal blog to a Kaiser document posted on a public Web site, claiming to expose the company's breach of HIPAA. The document included database names, IP addresses, computer codes and screen shots, potentially affecting some 140 insured Kaiser customers. The company later sued the former employee and obtained an order to destroy any company information in her possession and enjoining her from using or sharing the information. However, as a result of the company's failure to protect this information from disclosure, Kaiser Permanente was eventually ordered to pay a fine in the amount of $200,000 by the California Department of Managed Healthcare.

AUDIT, TEST, AND VERIFY.

Best practices and guidance

While complete data security seems at best a moving target, there are several measures that a company can and should take to minimize the occurrence of data loss. The following practices are suggested to help companies avoid data breaches, and in the event one occurs, to be able to respond quickly:

1. Conduct a security risk assessment and develop a security plan and policy. The policy should include statements addressing the points below. Once the policy is developed, training should occur for all members of the organization.

2. Use password protection. Use passwords for log-in and access to sensitive data. Only unique passwords should be used as identifiers and for accounts. Avoid using information that can be easily checked, such as names, birth dates, social security numbers, or phone numbers. Restrict access to email, screen savers and the like with passwords.

3. Use encryption to further protect sensitive information. Make sure all sensitive information is encrypted, especially when physically or electronically transferring files with personal information, and when storing files on laptops, portable devices, DVDs, or CDs.

4. Physically secure sensitive information, equipment and files, and restrict access. Sensitive data should be physically restricted in a secure location. Maintain records of who must have access to the electronic files and how the information is distributed.

5. Manage files and systems, including archiving and updating. Periodically review system capacity and files for updating, deletion, or storage in secure locations. Wipe portable devices before disposing of them or transferring them to a new user. Have a routine for review and disposal of paper information that is no longer essential. Adopt and follow a retention policy.

6. Employ and update software to guard against viruses, spam and malware. Use a firewall for the network. Use only secure servers. Apply patches as they become available.

7. Adopt and follow terms of company privacy policy.

8. Audit, test, and verify. Periodically conduct audits of the system.

9. Monitor system use and information access. Use application logs.

10. Terminate access for former employees. Coordinate with human resources to disable passwords and access upon termination and to collect any portable devices and laptops.

Conclusion

It's clear that data loss can cripple an organization – not only through financial losses associated with it, but also through loss of reputation. The massive TJX breach in Massachusetts is a prime example of just how detrimental a data breach can be. Not only has the company already spent four years dealing with the repercussions of the breach, but it has also lost millions (possibly a billion) of dollars as a result. For many companies, such costs could put them out of business.

Despite more stringent breach notification laws, businesses have to remember that such initiatives are designed to protect the individual. It is up to businesses to protect themselves, which they can easily do by implementing a comprehensive security plan as outlined above.

This byline contains a general overview and statement of the law and is not a substitute for obtaining detailed legal advice. You should seek specific advice on a particular issue.

Marc Hocking is the CTO of Becrypt (www.becrypt.com). He is a leading proponent of Information Assurance, with extensive government and global cross-border data security experience. Before joining Becrypt, Marc worked for the UK Government Cabinet Office where he developed solutions for a number of cross-government projects. He also spent 10 years in a variety of roles within global financial institutions working on systems that included PKI, authentication, authorization, and privilege management infrastructure.

Kathleen Porter is a partner in the Business Group and chair of the firm's Intellectual Property and Technology Practice Group. Kathleen counsels clients on the development, protection, and commercialization of intellectual property and technology. She has extensive experience in structuring and negotiating sophisticated domestic and international license agreements, acquisitions, partnering arrangements, strategic alliances and other technology-driven businesses.

Infosecurity Europe 2010

Earls Court, London. 27 April-29 April 2010
www.infosec.co.uk

RSA Conference 2010

Moscone Center, San Francisco. 1 March-5 March 2010
www.bit.ly/rsac2010

IBWAS09

Universidad Politécnica de Madrid, Spain. 10 December-11 December 2009
www.ibwas.com

ASIACRYPT 2009

National Center of Sciences Building, Tokyo, Japan. 6 December-10 December 2009
asiacrypt2009.cipher.risk.tsukuba.ac.jp

2009 Annual Computer Security Applications Conference

Sheraton Waikiki Hotel, Honolulu, Hawaii. 7 December-11 December 2009
www.acsac.org/2009

Financial Cryptography and Data Security '10

Dream Hotel Gran Tacande, Tenerife, Canary Islands, Spain. 25 January-28 January 2010
fc10.ifca.ai

HITBSecConf2010 - Dubai

Sheraton Dubai Creek, Dubai, UAE. 19 April-22 April 2010
conference.hackinthebox.org/hitbsecconf2010dxb

Why out-of-band transaction verification is critical to protecting online banking

by Steve Dispensa

There's a new breed of bank robber out there, and this time, the bad guys are carrying laptops instead of guns and ski masks.

Just ask Henry Slack of Slack Auto Parts in Gainsville, Georgia. Over the July 4 weekend, crooks broke into his bank account and cleaned him out of nearly $75,000 over a four-day period.

The scary part is that the crooks pulled off the robbery using nothing but commonly available malware. They likely never met (or even heard of) Slack, they probably never got near one of his computers, and – worst of all – the bank had no idea it had been robbed until Slack noticed what had happened.

How did they do it? Was the bank lax about security policies and procedures? Was a new server software bug discovered and exploited? The answer to this last question is no. Instead, crooks used a new kind of attack, called an inline or real-time man-in-the-middle attack, to bypass existing defenses and carry out crimes. Indeed, these attacks have been known for years, and the problem doesn't result from a specific vulnerability in any one piece of software or hardware.

Online banking attacks are evolving

Before we analyze these new attacks, let's take a brief look at how we got to this point. With the advent of online banking, the crooks realized that the only thing standing between them and unfettered access to a fresh source of funds was a simple username and password. Initially, the bad guys simply started asking users for their passwords. These techniques evolved into today's sophisticated phishing attacks.

The banks went on the defensive, rolling out anti-phishing site identification technologies. Browser vendors added sophisticated anti-phishing tools to their products. Anti-malware vendors added anti-phishing technologies, and even network operators started rolling out sanitized DNS services, aimed at quickly recognizing and shutting down phishing domains.

Even with all of these safeguards, banks were still suffering a significant number of attacks. Eventually, the root cause had to be addressed: passwords are simply not good enough. FFIEC recognized the issue with user authentication and began requiring banks to strongly authenticate users for high risk transactions. This led to the deployment of tools, such as secret questions and device identification. Some banks took it a step farther by deploying two-factor authentication in the form of security tokens, requiring the user to enter a password plus a code from the token in order to gain access to the website.

As threats become more sophisticated, accounts protected with two-factor authentication are becoming increasingly common.

Inline attacks

With all these defenses, what's a crook to do? As it has always been the case, necessity is the mother of invention. Unfortunately for the rest of us, the bad guys are well paid by organized crime rings to invent. And invent they did!

When you can't steal credentials, the next best thing is to just let the user log in and then steal the logged-in session. The means is a new breed of malware, installed on unsuspecting users' computers, that lays in wait while users surf the web. When the victim surfs to a website that the malware recognizes, it wakes up and springs into action.

The attack is simple, and it's over in the blink of an eye. The malware lets the user log into the website in question, and then simply assumes control of the authenticated session. From there, it does whatever it pleases with the user's account. A broken webpage or perhaps a slightly friendlier "Please try your request again later" message is displayed to the end user.

Meanwhile, the bank sees a request from the user's computer – a legitimate-looking request from a legitimately logged-in user. In fact, the irony of the situation is that, with all of the new strong authentication technology that has been put in place, banks have more reason than ever to trust the inbound request: "We just authenticated the user with two factors, so we KNOW it must be a legitimate user. Let's go ahead and complete this request."

The attack is simple, and it's over in the blink of an eye.

Once the malware has taken control of the connection, it's free to do whatever it pleases. Often, that means transferring money out of the account using a wire transfer or an ACH transfer. Sometimes, this happens repeatedly over the space of a few days in order to bypass transaction limits. And because the entire thing can be automated, the crooks may not have to lift a finger – they can just sit back and wait for money to start showing up in "mule" accounts.

The technique isn't actually new. While variations on this theme have been used for decades, this exact mechanism has been in the wild since at least 2007, when the Silentbanker trojan was first discovered and described. Silentbanker had built-in support for about 400 banks (as of January 2008), and in at least one case, it used exactly this attack to do its dirty work.

More recently, newer malware tools like Clampi and ZeuS have been in the news, and unlike Silentbanker, the damage this time has been significant and widespread. Clampi infections have been on the rise, with over 500,000 newly infected computers since March. It is a versatile program, letting the attacker adapt its code and targets over time. One analyst puts the number of sites that Clampi supports at 4,600. And while it's commonly referred to as a Trojan horse, it is self-propagating like a worm and uses techniques commonly used by rootkits to hide its presence.

These attacks have been responsible for a variety of actual thefts. Generally targeting business bank accounts (where the account values tend to be higher), crooks have made away with hundreds of thousands of dollars in documented thefts in the last few months, including the Slack Auto Parts incident.

The Washington Post reports that Bullitt County, Kentucky, lost $415,000 in June due to malware present on the county treasurer's computer. In another case, the Western Beaver School District is suing ESB Bank over malware that drained $700,000 from its account this summer. Some estimates put total losses in the millions of dollars this year alone.

Mitigating inline attacks

The fundamental problem is that banks and financial institutions are paying a lot of attention to authenticating users' logins but relatively little attention to authenticating the transactions themselves. Because malware can simply wait for a user to log in legitimately, defending only against fraudulent logins misses a major attack vector. In fact, these inline attacks are exactly what prompted Bruce Schneier, a prominent data security researcher, to declare in 2005 that two-factor authentication "won't secure online accounts from fraudulent transactions."

Login authentication, even two-factor authentication, does not stop inline attacks. The malware simply waits for the user to complete authentication and then takes over. Once the authenticated session has been hijacked, the malware can transfer funds, change account information, etc.

The good news is that there is a straightforward solution using out-of-band technology. Generally referred to as out-of-band or out-of-channel transaction verification, these systems acknowledge that the identity of the user may change the instant after a successful login, so they force re-authentication any time a risky transaction is requested. Because the transaction is verified out-of-band, the attacker's malware never gets a chance to alter the verification message before it gets to the customer.

Let's look at an example using phone-based authentication and transaction verification. Say the user logs into a bank account to download statements or check on balances. The malware notices the login and surreptitiously submits a bogus transaction. At this point, the bank places a phone call to the user for verification. On answering, the user hears exactly what transaction has been requested: "Hi, this is First Bank of Main Street, please confirm that you want to transfer $1,000 to the Bank of Nigeria account ending in 1234." The user is then asked to confirm the transaction. The user, of course, did not initiate the transaction, and so does not confirm the request. Furthermore, the bank's fraud department can be notified in real time, the user's account locked down to prevent further damage, and forensics data captured for follow-up.

Out-of-band transaction verification can also defend against a more subtle and insidious form of this attack. Imagine that the user legitimately tries to transfer money from one account to another, but this time, the malware simply alters the destination account. Even if the malware is kind enough to display the transaction details to the user, it would be easy to miss such a subtle change. Even worse, the user wouldn't notice the missing funds, since the funds were being transferred anyway.

With transaction verification, though, the user is presented with the transaction details. As an added degree of safety, the issuing bank can require the user to re-enter the destination account number over the phone to make sure there's no chance of misdirecting the funds.

Using transaction verification

There are a number of usage scenarios that banks are implementing. To begin with, wire transfers tend to be high-value, high-risk transactions. It's difficult for a bank to know what a normal wire transfer pattern is, since they tend to be relatively rare events. Adding explicit transaction verification to all wire transfer requests effectively prevents inline attacks.

Automated Clearing House (ACH) transfers are another obvious usage scenario. Because these transactions tend to be more common and to display a clearer pattern, banks can be somewhat more intelligent in deciding where to apply transaction verification. For example, a bank could apply out-of-band transaction verification to any ACH transfer into an account that hasn't had a transfer in the last year. This strikes a nice balance between security and convenience.

Most banks have implemented fraud scoring or risk scoring systems. Out-of-band transaction verification is a natural complement here as well: whenever the risk score is anything other than “low risk,” the bank can simply initiate an out-of-band request to confirm the transaction. Because risk scoring systems generally flag only about 5% of transactions as potentially fraud, legitimate users will rarely be prompted for a verification. On the other hand, because users will easily be able to confirm transactions, banks can actually increase the sensitivity of fraud detection systems, making it even harder for bad guys to carry out fraudulent transactions, without having to worry about angering end users with high transaction denial rates. It’s a win-win situation.

One of the highest-risk transactions in online banking is the creation of a new online bill pay recipient. Because this is a relatively rare event, the imposition on the end user is slight, but the security benefit to both the bank and the end user is significant.

Finally, the first thing that most phishers do after gaining access to a new account is to change the password and contact information. Adding phone-based verification of any of these changes is easy to do and has a good cost/benefit ratio for both the bank and the end user.

Looking ahead

To quote Bruce Schneier again, attacks always get better, they never get worse. The threat landscape is evolving, and experts agree that inline attacks are the way of the future. It’s not hard to see why, either: banks have deployed increasingly effective defenses against the stealing of access credentials, so the bad guys have to find another attack vector.

At the moment, very few banks have any way to defend against inline attacks. Fortunately, there is a solution, in the form of out-of-band transaction verification.

Steve Dispensa is co-founder and CTO of PhoneFactor (www.phonefactor.com), a provider of out-of-band two-factor authentication services. Steve has several patents pending in the fields of computer science and telecommunications, is a Microsoft Certified Systems Engineer and a Cisco Certified Internetworking Expert. He has been recognized three years in a row by Microsoft as a Most Valuable Professional for his contributions to the Windows kernel mode development community.

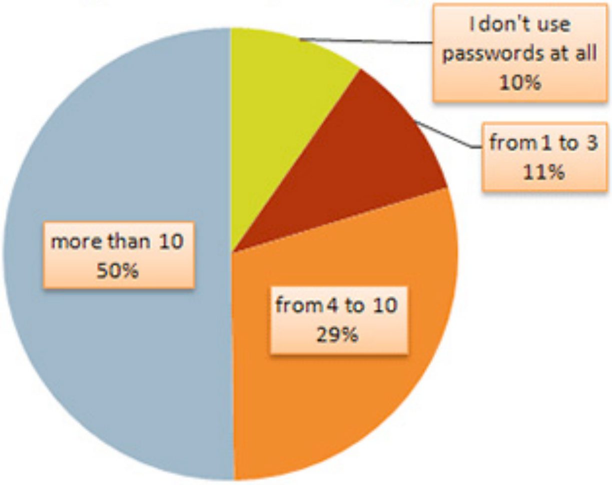
Study uncovers alarming password usage behavior

by Frank J. Harris

ElcomSoft has conducted a survey on its customers, and discovered a major security hole in the choice of passwords among respondents.

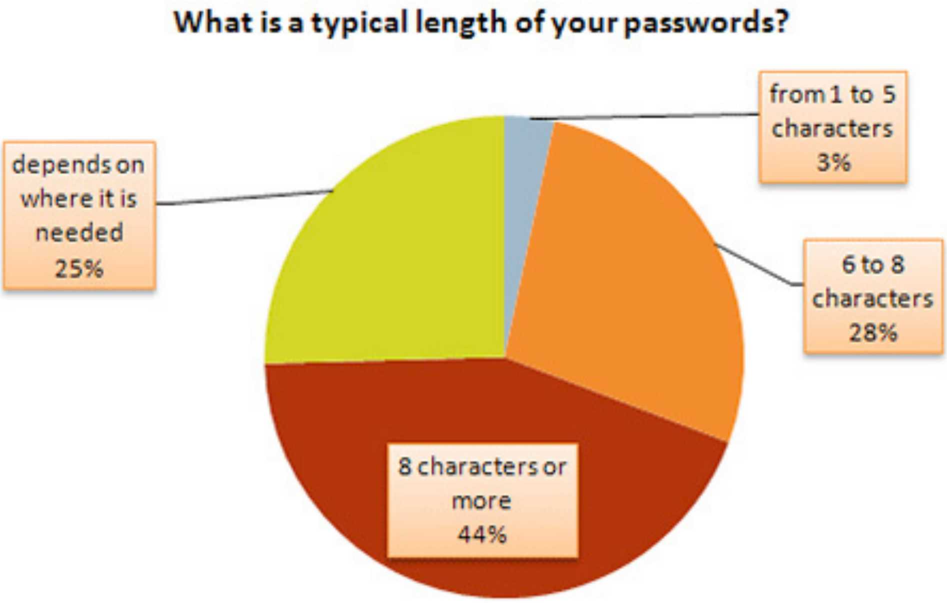
According to the survey, as many as 77% of respondents use or have used the same passwords for different applications, documents and websites. This fact per se does not help an outside attacker to quickly unlock a single document protected with a strong password and an adequate encryption algorithm. However, if one gets access to the entire hard drive, extracting passwords protecting certain types of information (e.g. email accounts, Web forms, instant messenger accounts and so on) is near instant. By using passwords extracted from the weaker link, it becomes possible to unlock other types of information protected with much stronger encryption algorithms if the same or similar passwords are used.

How many passwords do you use in your real life/work?

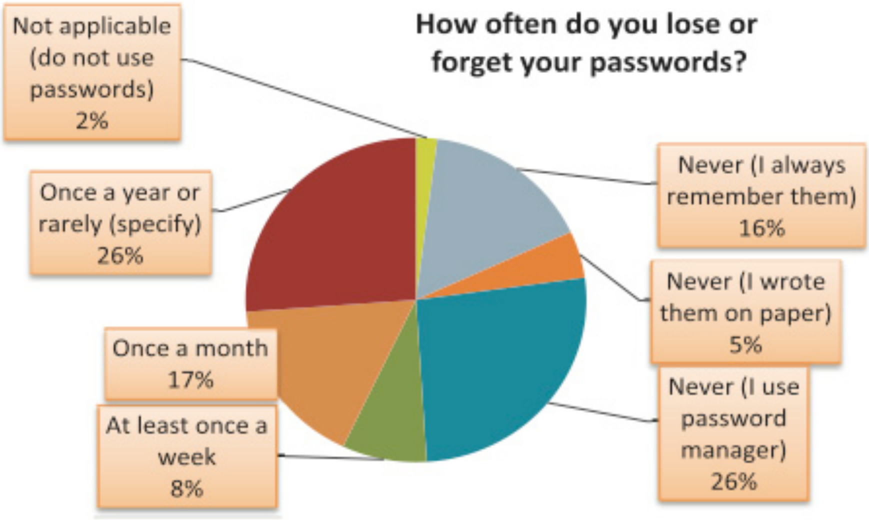


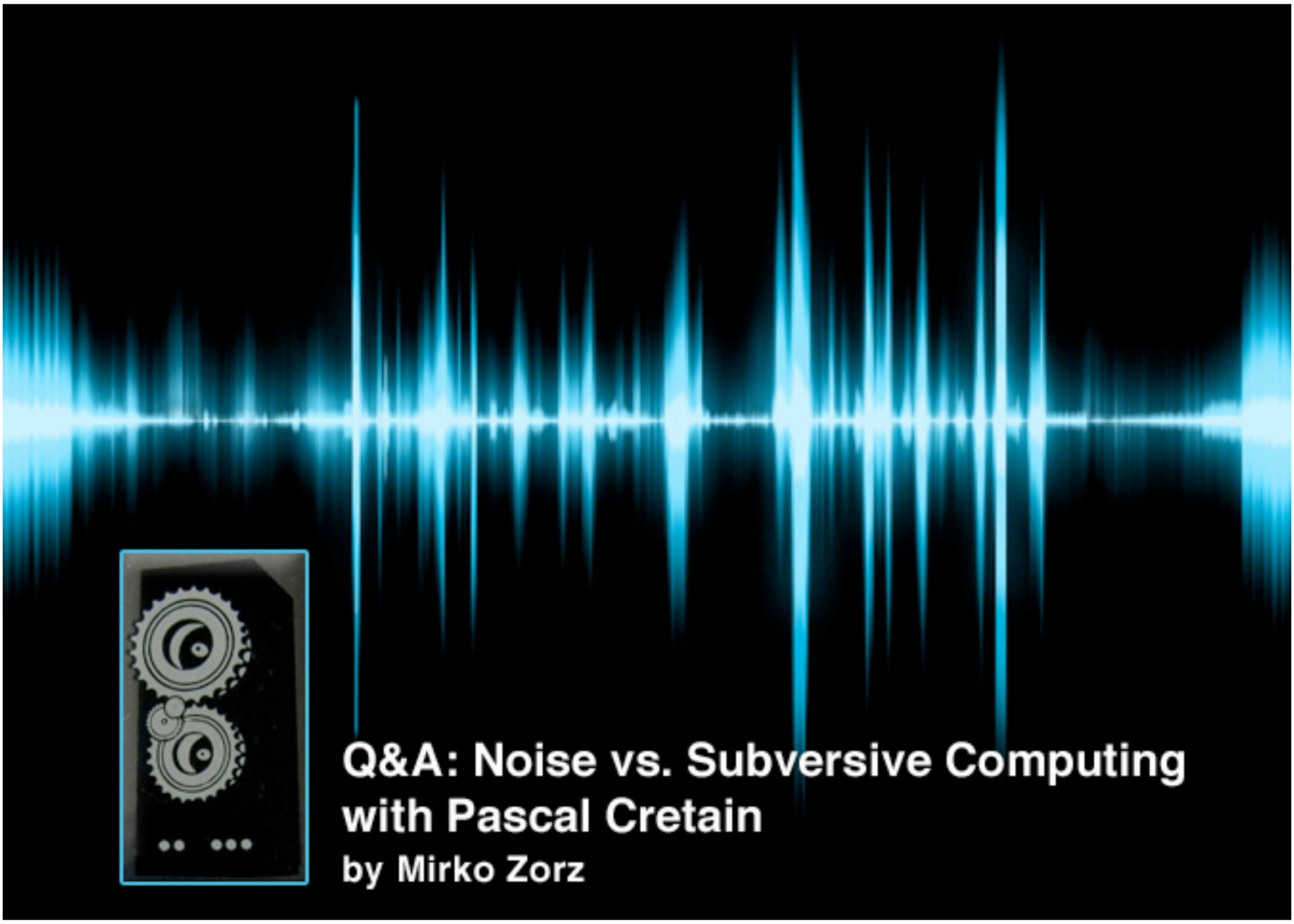
While using the same password on multiple types of information is usually against corporate security policies, other researches suggest that such users can avoid automatic enforcement of a security policy by adding numbers or suffixes to such passwords. Password recovery tools with advanced dictionary attacks allowing permutations of dictionary words can easily handle the slight differences in password prefixes and suffixes.

"People tend to re-use passwords among different accounts, and to protect different types of information", says ElcomSoft CEO Vladimir Katalov. "We just haven't realized how large the extent of the issue is." Sharing passwords among different accounts and types of information gives those equipped with appropriate password recovery tools a good chance to gain access to everything protected with said password in almost no time.



The "Password Usage Behavior" survey was conducted online from June 3, 2009 through September 1, 2009. ElcomSoft has invited its clients - CIOs, IT administrators, security experts from governmental and military sectors as well as ordinary users - from around the globe. The results of this survey are based on responses from more than 1000 security and IT professionals from more than 70 countries. Thirty-nine percent of respondents were from Europe, followed by North America (36%), Asia (12%), the Middle East (6%), Australia (4%), South America and Africa (3%). According to the poll findings, 50 percent of respondents use more than 10 different passwords. While 29 percent have from 4 to 10 passwords, 11 percent claimed to use only from 1 to 3 passwords to get access to websites and applications. This news is disturbing as 3 passwords used everywhere cannot guarantee proper security, especially when these passwords are used to access both personal and work accounts.





Q&A: Noise vs. Subversive Computing with Pascal Cretain

by Mirko Zorz

The "Noise vs. Subversive Computing" project is a collaborative release split between noise/experimental artists and subversive technologists/computer hackers. Ten representatives from each camp were asked to contribute a piece of work which could be anything at all: an audio track, a drawing, a written passage, software, video, combination of all that, or anything else that can be converted to binary.

The Noisicians had "Subversive Computing" as their central theme, and the Technologists worked with "Noise". We've spoken with the main voice behind the project, Pascal Cretain.

What was the motivation behind the "Noise vs. Subversive Computing" project? How did it all start?

The main motivation is to connect the (archetypal) hacker types with the noise and experimental music and art community. To explore the creative potential of technology, stir things up and stay interested.

I have been involved in both worlds for some quite some time now - that's how the whole idea came about - and have met some truly bright people with very diverse interests and surprisingly similar, "out of the box" thinking mindsets. In my eyes, the two communities just happen to use different instruments.
The same people who build custom hardware and compile obscure OS kernels, would, under the right circumstances, set up custom performances passing on blindfolds to the audience in order to explore different perceptions of a live show.

I can see an explosive potential here waiting to be explored.

How many individuals contributed to the project and how did you choose who to feature?

A total of 21 individuals (including the graphics designer) worked on the project. I know quite a few people in both scenes, and tried to pick as diverse a sample of individuals from both scenes as possible, while at the same time maintaining a healthy DIY attitude.

Featured in the project are many different countries and tendencies of both the hacker and the noise scenes.

What are the inspiration forces behind the project and how do you see it evolving in the future?

The inspiration forces in this instance have to be precisely these two fascinating spaces: The music underground and the spectacular neighborhood that is the Internet.

The music underground is a fascinating place to be in, with its own aesthetic rules and a general anti-attitude. It is a genuine, inclusive community with strong bonds and literally no geographic limits. I think that that the stubborn, non-pretentious, music subgenres that collectively make up the underground have plenty to share. Even when they don’t have much to say, you can be sure that they will never lie to you.

Regarding the Internet, I'll quote Richard Thieme: "Now if it's all right with you, I just want a few minutes with my friends. I just want to go where we don't need to be always explaining everything, where everybody understands. Okay? And would you mind closing the door, please, as you leave?"

There surely will be continuation. A team of 10 is already working on a follow up project to "Noise vs. Subversive Computing". This one's called "Mutant Rhetorics", will constitute the second release for my label - Computationally Infeasible Records - and is a collaborative authoring project utilizing the concept of "reusable resources" from object-oriented programming. You could say we are working on an object-oriented noise novel. Aimed for release in 2010.

To learn more about the “Noise vs. Subversive Computing” project visit Pascal Cretain’s MySpace page (www.myspace.com/pascalcretain) and Computationally Infeasible Records (computationallyinfeasiblerecords.blogspot.com), an experimental null-profit label from Denmark.

The project is available for order on a limited release of 256 numbered copies in USB stick format.

InfoWorld
2009
TECHNOLOGY
OF THE YEAR
AWARDS

DeviceLock (www.net-security.org/software.php?id=121)

DeviceLock gives network administrators control over which users can access what devices (floppies, serial and parallel ports, Magneto-Optical disks, CD-ROMs, ZIPs, etc.) on a local computer.

Espionage (www.net-security.org/software.php?id=760)

No longer is it necessary to encrypt your entire home folder just to protect your email or your chat history. Espionage can protect individual folders, allowing you to easily secure sensitive data. Espionage is designed to integrate with Apple's Finder, so that you can protect only the data that you want protected, without having to resort to any special "vaults".

Ratemask (www.net-security.org/software.php?id=309)

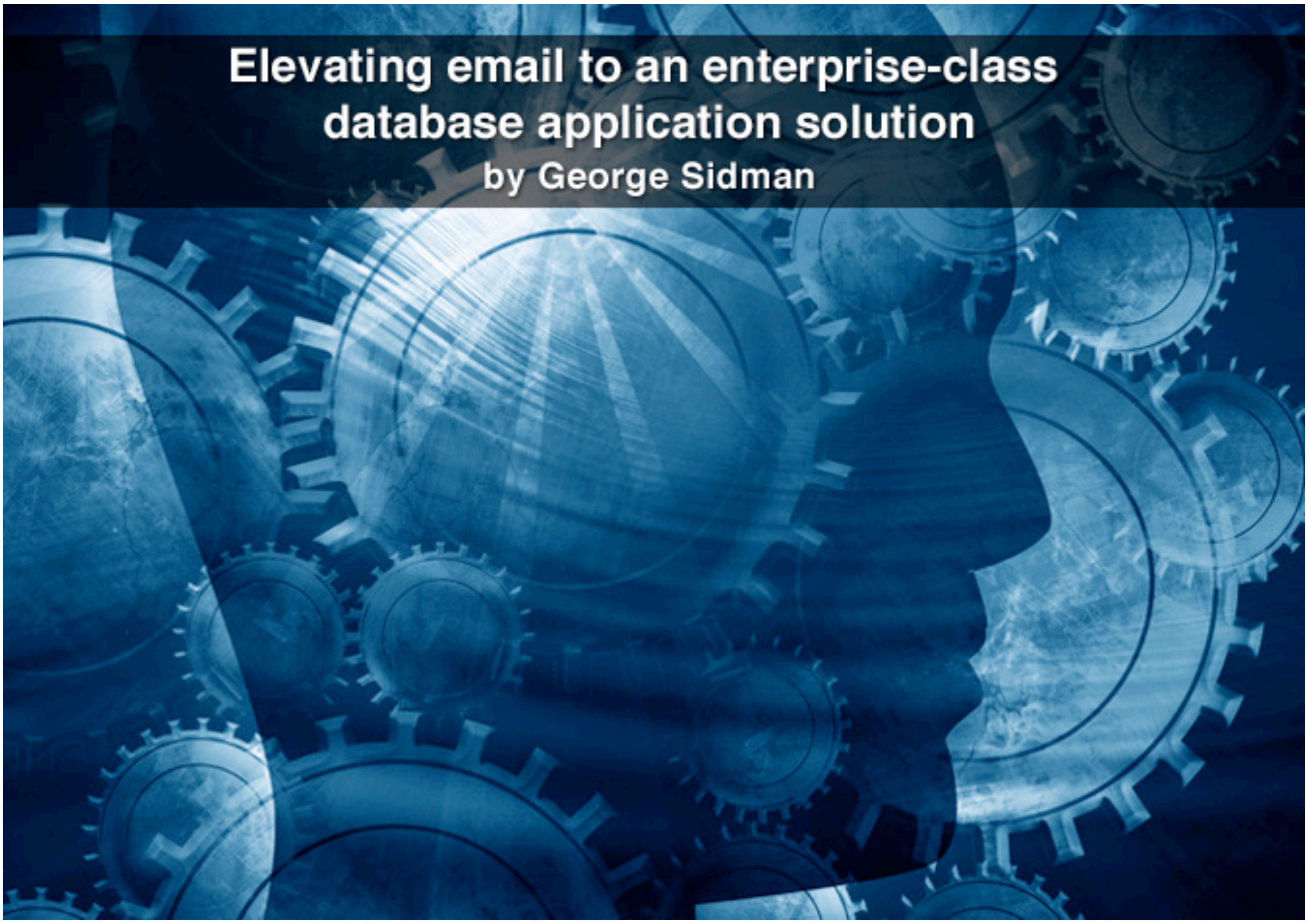
Ratemask is a small program that will make it easier to create ICMP type masks, as used in the icmp_ratemask sysctl, viewable through the /proc filesystem.

Trojan Killer (www.net-security.org/software.php?id=749)

Trojan Killer application is a malicious computer software (malware) removal tool. Samples of malware include various types of adware (displays unwanted advertising); spyware (may keep and send logs of your keyboard and mouse activity, such as credit card or personal identity information); hidden dialers (may initiate unsolicited phone call which then shows on your bill), and more.

Elevating email to an enterprise-class database application solution

by George Sidman



When compared to the growth and maturity of other technologies, the Internet appears to be struggling with adolescence. It was born and nurtured on networks presumed to be private, exploded worldwide in the late nineties, and never had a chance to develop on sound engineering principals equal to its present importance and requirements.

Web applications and the cloud are now rapidly morphing towards true database solutions, while email is still stuck in the protocol layer of the OSI model (tinyurl.com/5bvu8). Emails are sent out to traverse the Internet totally un-chaperoned and un-encrypted.

As fast and convenient as email is, it exacts a tremendous price as it forces us to protect ourselves against abuse, loss of privacy, financial fraud and fight other malicious behavior. Dollar losses to online fraud are already in the billions and show no signs of abating. We all pay for more than 90% of Internet traffic that is dangerous and unwanted, and no one is immune as this problem is the same for the individual and the corporation.

More and more observers and commentators suggest that the Internet is fundamentally broken - the security industry is no better than 90% effective against the one billion spam and fraud messages sent every day (tinyurl.com/5q8vys) - and we all wonder why the new protocols (IPv6, DNSSEC, IPsec, Domain Keys, etc.) have been so ineffective.

Current solutions get limited results

The DNS, critical to the routing mechanisms of the Internet, is also openly visible and also under constant attack. As a result, an email address presents itself as an open invitation to pillage and plunder. Malware blockers and filters are fighting a band-aid war they can never win.

Continuing to fight against a growing and increasingly innovative enemy will continue to be an expensive rear-guard action and a losing proposition.

Pursuing privacy and security through encrypting content or the transport wrapper (TLS, VPNs, etc.) has proven nearly worthless, as the exposure of the routing is the basis of the abuse. An email sent from a laptop over a VPN to a corporate server is safe until it must traverse the open Internet to reach a customer, partner or supplier (about 80% of commercial traffic.) It then leaves the DMZ to route in the clear, undoing the efficacy of the VPN. Legacy encryption solutions have failed to gain wide adoption, mostly because the technical challenges are beyond the average user. The market perceives that the true dangers of the Internet are really general abuse and fraud. Users are much less aware – and therefore concerned - that their email content might have value to someone other than the intended recipient.

Enter federal and state privacy laws

Federal and state agencies have began enacting new privacy laws because there are industries, such as healthcare and finance where the protection of personally identifiable information is critical (tinyurl.com/oyt9j).

The upturn of interest in electronic medical records includes compliance for HIPAA and SOX which is today driving an increased interest in private email. Web-based portals have emerged, under HTTPS, to deal with this requirement, but are only a partial solution. Adoption of portals is minimal, as doctors dislike clicking into a portal when their regular work habits include using email programs, such as Microsoft Outlook.

Portals are also only accessible to a small and select group of direct subscribers. But the larger issues are that only the transport layer is encrypted, leaving the central data storage in clear, usually in third-party hands, and not likely to pass a security audit. (See the EPIC complaint to the FTC regarding Google privacy claims - http://tinyurl.com/yk8cnf5).

Federal and state agencies have began enacting new privacy laws because there are industries, such as healthcare and finance where the protection of personally identifiable information is critical.

This growing problem needs a new solution

There are hundreds of companies selling firewalls, VPNs, encryption solutions, malware blockers, and other security technologies and consulting services. The industry presumes that nothing can be done about the underlying problem, which is simply that the openly disclosed routing of email addresses, domain names and web addresses invites and supports abuse and fraud.

The next logical conclusion is that if the routing could be made private and the content hidden from view, the fraudsters would be thwarted and the abuse and fraud would be dramatically reduced, if not eliminated.

There is fundamentally nothing wrong with the basic engineering that underlies the Internet. Its protocols do a remarkable job of delivering connectivity and maintaining a high degree of integrity across billions of operations every day. The problem is that the protocols (as described in the OSI model) are inadequate for the tasks at hand. They should be put to work in service of a broader software model. That model requires a true database application layer that wraps the protocols, providing an overlay of control facilities, bundling in encryption, key management, authentication, and certificates, as well as delivering on the new compliance requirements.

Email will most likely remain an adolescent technology until it acquires an application layer that lets it act like a true enterprise-class solution.

Ease-of-use is the holy grail of successful software. This has been achieved in a number of industries and solutions such as financial accounting software, CRM programs, online shopping and other day-to-day solutions which achieve that through the application layer.

It seems logical that we could achieve a new and much more powerful email capability simply by adding an application layer to the email protocols. The complexities of the components can be easily managed with database and applications code, removing the end-user from the technical challenges and masking the operations and content from prying eyes through private routing mechanisms and end-to-end encryption.

The dangers of the DNS

No standard email could route without the DNS and all web activity needs the DNS to translate names to IP addresses. Many view the DNS as sacrosanct, and so deeply imbedded in Internet operations that even questioning its use is heresy. However, this is one Emperor who is indeed wearing no clothes. All DNS operations - from address lookups and resolver activity, to the Whois (beloved by fraudsters), and on to the many domain registrars (whose focus is revenues), across the (politically embattled) ICANN TLD – every aspect of the DNS is exposed on the open Internet.

That blatant visibility is the root cause of almost all malware - it fuels all fraud and cyber attacks and is the primary reason that no individual, enterprise or government is safe on the Internet.

Nobody is going to fix the security flaws of the Internet. It is here to stay as it is.

Towards a new privacy model

Nobody is going to fix the security flaws of the Internet. It is here to stay as it is. Even with all its warts and problems it has driven new levels of information speed and freedom that the world has never before seen. We can use the Internet as it is, employing industry standards and open source code to create and deliver new levels of privacy, security and legal compliance.

The DNS can be left as it is. We don't necessarily need to use the name conversion facility to find a server. (In the private email space server IP addresses are few and easily managed – not by end-users, but safe within the application layer.) If we drop the DNS, we can then modify the email address so that it thwarts malware, simply because an email address without a TLD won't route publicly. We can render the addresses invisible through packet header encryption, along with the subject heading and other clues that might otherwise attract the wrong crowd.

These concepts are the first glimmers of privacy. By exploring this direction we could well create a new model that takes email away from its "Wild West' reputation and empowers it as a robust, safe and private means of communicating.

The components of the new architecture

To build a standard database application solution, we need central servers and a connectivity model, cloud or otherwise, that achieves layers of managed services. Today, the standard email server is James from Apache (james.apache.org). It is a protocol layer utility that utilizes flat files to route email to and from senders and recipients. The problem is that James and its cousins, SMTP/POP3/iMAP and others, all operate "in clear". They will accommodate encrypted content but the header must remain visible for routing under the DNS. Across all these protocols there is simply not enough information to deal with the additional needs now emerging for end-to-end privacy, compliance and reporting. Components that could be added to create a new architecture include:

- Adding a database to manage subscribers, policies, transaction logging, etc., James could take on a new life. Suddenly a whole new range of information is available to manage encryption, keys, authentication, user account services, etc.

- Adding a central key store within the database, PKI becomes easy to manage. Key distribution gets automated within the application layer and is no longer a burden to end-users.

- Encryption processes for both the content and the transport layer get handled within the application layer, eliminating the need for end-user involvement and much of the potential for errors. This enables the accuracy, efficiency and safety of large machine generated keys.

- Adding some dedicated server code we can resolve encrypted traffic before it gets to James and also manage connectivity to find addresses of remote services.

- Authentication and certificates also get embedded into the application layer, becoming more durable and reliable, free of user involvement and totally controlled by system administrators.

- Then, to extend the application layer to the desktop, we need a small piece of code that is downloaded and easily installed on desktops, laptops and other devices. It handles end-user side encryption and decryption, and other housekeeping functions through tight integration with the server-side code. By self installing, it handshakes standard email clients through standard ports and protocols. By utilizing standard email clients, end-user training is minimal and no substantial changes are required to existing business processes.

Under this new model, email becomes a complete ecosystem for privacy, security and compliance. It is a unified space into which all the scattered bits and pieces of our previous 'security toolkits' get integrated under a single application solution. This model operates in the OSI stack from the session layer up to the application layer. (VPNs operate from the session layer down.) As a result, such a solution is highly portable and independent of transport and connectivity.

Other major benefits

With a central database to log all transactions, the system can report on all email traffic on-demand. For the first time, the life cycle of an email can be tracked, through replies and forwards, delivering on emerging compliance and eDiscovery requirements with ease. Reports can be rendered in various output formats for business intelligence purposes, and managers will have an enforcement mechanism to track end-user compliance to privacy policies.

With a network neutral application in place, plug-ins can be created for the various enterprise email services, such as Exchange, GroupWise, Domino and Citrix. This means that minimal disruption will occur in implementing a private email network and that private traffic will be easily managed alongside standard email services.

Freedom from malware is one of the major benefits of such a model. The standard Internet model of anonymity and non-accountability is inverted. In this new 'Gated Community' all users are known and fully accountable. A rogue subscriber can simply be shut down.

If the two ends, the client-side and the server-side, are indeed closely coupled through application code and encryption - and all routing is protected through non-DNS addressing and other controls are in place - then privacy is truly achieved. After all, do you have privacy if publicly visible routing exposes who you are, and you cannot control who sends you email?

The Internet has been mostly under the control of network engineers. Email would most likely benefit hugely if application and security software engineers took a stronger hand. Bringing the email protocols together in a database application is the next logical step and until that happens we be subject to the risks and dangers of abusive and costly email problems.

George Sidman is the Chairman and Chief Technology Architect at WebLOQ (www.webloq.com). His technology experience spans large-scale library and information automation, commercial ISP services, and Internet security and privacy technologies. He is also a licensed Architect, and is the former Chair of the Technology Council of the Silicon Valley World Internet Center in Palo Alto, California. He sits on the Boards of the Marina Technology Cluster in Marina, California, and other technology companies.

Ask the social engineer: Practice

by Chris Hadnagy

One reader wrote in asking: "How can one practice social engineering before using it in the wild?" Answering is Chris Hadnagy, the lead social engineer and developer of the social engineering framework.

I really thought this was an excellent question. In traditional penetration testing if we want to test our wares we can do a number of things: set up a virtual machine, a small LAN or we can even purchase a course that comes with labs to practice in.

That methodology works perfect for practicing that level of security auditing, but we can't really set up "fake" people and "hack" them to practice social engineering. Staged events rarely work the way real life does. Unless we are dealing with expert and experienced actors facial expressions, reactions to questions and body language are almost impossible to mirror the way a real target would react.

That being said, it is not wise to drive around and take videos of yourself shmoozing free food or getting into clubs for free. Although there might certain aspects that reflect social engineering, it will not prepare you for professional social engineering audits.

Another method that has been suggested, which I feel isn't really wise, is to practice lying to your friends and family, even for short periods.

Social engineering isn't about who is the best liar. Social engineering is about obtaining information from your target that can lead to a security breach. Even little bits of information (i.e. kids' names, favorite restaurants, etc) can lead to a security breach.

How can one go about practicing social engineering before trying his hand in the wild? In the recent release of the first framework for social engineers, there is a breakdown of the key components of social engineering. This framework outlines in logical progression these components and then dissects each one, defines its aspects and how to perfect it. Mastering all these components would make one a perfect social engineer.

It must be mentioned that not every aspect of social engineering is used in every audit. Regardless, here are the keys to acting and thinking like a social engineer.

Let's take the top five categories to focus on:

1. Information gathering
2. Elicitation
3. Pretexting
4. Psychological principles
5. Influence.

Each one of these can be practiced and enhanced without breaking the law or ruining relationships - actually, it may enhance your relationships with others. Let's take two examples.

Elicitation is basically extracting information through the use of questions. Sounds easy? Not really. Try walking up to a stranger and saying: "What is your name and where do you live?" and see what happens. Tell us when you get released from the slammer. If we practice using intelligent questions, questions that provoke thought, questions that cannot be answered with a YES or NO we can be on the road to perfecting elicitation.

One very detailed aspect of elicitation is preloading. Think of preloading as a trailer to a movie. A trailer will show you and tell you the things they want you to know and think. "Best movie of 2009" and then a display of some of the best scenes in the film. In a social engineering context you can practice preloading people with information that will make it easier to get the desired results from them.

Take a look at a practice session we just did and how it went, while at a local coffee shop:

SE: While sitting in a Starbucks drinking your coffee you see a target reading the paper. You see him sit a section down, look over and say. "Hey I saw an article there on the cover, if you are done can I just read that quick?"

Target: Most people, because they are asked nicely, will respond: "Sure, here it is."

SE: Takes a few minutes to read, folds and hands it back. "I was scared cause I am from here locally, live right over the hill in (name small local town) and the crime is ridiculous. You from here?"

Target: Most of the time they will respond with not even thinking, "No just passing through I am from Chicago."

SE: "Chicago, heck I was just out there for some business. I went to this place downtown called Morton's. You in the city or outskirts?"

Target: "Morton's heck I love that place, but expensive as hell. Yeah I live about 10 miles from the center city."

SE: Reaching over extending my hand "Hi my name is Chris"

Target: "Jim"

SE: "What do you do Jim, that you are traveling through here? I am in the IT field and do some training."

Target: "I sell paper, work for the largest paper company in Chicago. XYZ."

What did we learn? His name, location, place of employment, saw a wedding ring... all in about 3 minutes. We do nothing with this information, but it was great practice.

Microexpressions are the tiny involuntary movements of face muscles in reaction to emotions. Researchers like Dr. Paul Ekman and Dr. David Matsumoto are pioneers in this area. They have proven that regardless of age, sex, race, religion we all have universal expressions that display emotion. Even people who are blind have been proven to have the very same facial expressions to emotions.

The problem with these microexpressions or ME as they are called is that they usually last between 1/25th and 1/2 a second. The normal person may not be able to see that when they ask their wife how she is feeling, an ME of contempt passed across her face.

Being able to read microexpressions can enhance relationships and make you better in understanding people.

From a social engineering standpoint it can enhance your ability to detect deception in people.

How can you practice?

In Paul Ekman's book, Emotions Revealed, he talks about having a mirror and practicing making these facial expressions as described and feeling the emotions that occur when you do. In addition to practicing them on yourself, learning how and where and when to look for these on others.

Knowing that contempt shows only on one side of the face, knowing that disgust and anger differ in the way the eyebrows move and the eyes glare. Knowing that surprise and fear are different by the way the lips move. These things can change your understanding of people and how they react to questions. When you work on elicitation, reading facial expressions is a logical next step in being able to accomplish those tasks.

Naturally, there are many more aspects to social engineering. Information gathering, pretexting, interview and interrogation tactics, understanding psychology principles that will change the way you deal with people... all of this can be broken down and practiced on its own, without having to break any laws or hurt people.

Social engineering is not merely learning how to manipulate people into doing what you want, but it is about learning how to understand people. Once we understand how people think, how they work, how they react to certain situations then we can aid them down a path we want. For the purpose of security auditing we use this information to show where and how security breaches occur, then education makes people aware of these methods so they can guard against them.

Please send in your questions for the following column to logan -@- social-engineer.org with the subject of "net-security Ask The SE".

Chris Hadnagy is the developer of the social engineering framework (www.social-engineer.org). He works closely with the Offensive Security and Remote Exploit teams and advocates knowledge and awareness as the keys to what can protect people from social engineering attacks and help secure people from being deceived and influenced maliciously.

STORAGE EXPO

Report by Zeljka Zorz

Storage Expo, the only UK event for data storage, information and content management was held in October in London. With around 3,300 visitors and over 120 exhibitors, two specialized zones, roundtables, workshops and sessions, this year's event was all about virtualization, cloud, thin provisioning and de-duplication.

What follows are some of the many products presented at the show.

Neverfail 6 protects critical applications against downtime

Protects mission-critical applications across any combination of physical, virtual and cloud-based servers. The latest version adds new modules that integrate tertiary deployment and support maximum performance across WANs.

First 1TB portable hardware encrypted drive

Origin Storage launched their 1TB and 750GB Data Locker. The data on the drive is secured by AES hardware encryption and a 6-18 digit PIN number which is entered directly on the device itself.

SGI announced InfiniteStorage Total Control Suite

SGI introduced SGI InfiniteStorage NAS and SGI LiveSAN, two new storage offerings within the SGI InfiniteStorage Total Control suite, a set of modular software and hardware tools that enable storage customization using standard components.

Microsoft Hyper-V R2 backed up by Dell EqualLogic storage arrays

Dubbed as the ‘FREE’ add on for Windows Server 2008 users, the new R2 release offers new scope and new possibilities. However it is the prospect of a marriage to Dell EqualLogic storage arrays which caused quite a stir, even in today’s rapidly maturing server virtualization market.

Double-Take Software demonstrated new backup and availability products

Double-Take showcased Double-Take Availability and Double-Take Backup. The first solution is an updated version of their continuity product, the second provides real-time replication of data to continuously protect workloads.

Universidad Politécnica de Madrid
Escuela Universitaria de Ingenieria Técnica de Telecomunicación

10 - 11 December 2009

IBWAS '09

Iberic Web Applications Security Conference

Conference main topics

- Secure application development
- Security of service oriented architectures
- Security of development frameworks
- Threat modelling of web applications
- Cloud computing security
- Web applications vulnerabilities and analysis (code review, pen-test, static analysis etc.)
- Metrics for application security
- Countermeasures for web application vulnerabilities
- Secure coding techniques
- Platform or language security features that help secure web applications
- Secure database usage in web applications
- Access control in web applications
- Web services security
- Browser security
- Privacy in web applications
- Standards, certifications and security evaluation criteria for web applications
- Application security awareness and education
- Security for the mobile web
- Attacks and Vulnerability Exploitation

This conference aims to bring together application security experts, researchers, educators and practitioners from the industry, academia and international communities such, in order to discuss open problems and new solutions in application security.

Important dates

Submission of papers: **31st. October 2009**
Early-Registration deadline **15th. November 2009**
Conference: **10th - 11th December 2009**

Keynote Speakers

Bruce Schneier
Acclaimed Security Guru, Author,
British Telecom CSO

Jorge Martín
Inspector, High-Tech Crime, Logical
Security, Spanish National Police

http://www.ibwas.com, secretariat@ibwas.com

OWASP
The Open Web Application Security Project

OWASP SPAIN

OWASP Portugal

Malicious PDF files

(www.net-security.org/article.php?id=1308)

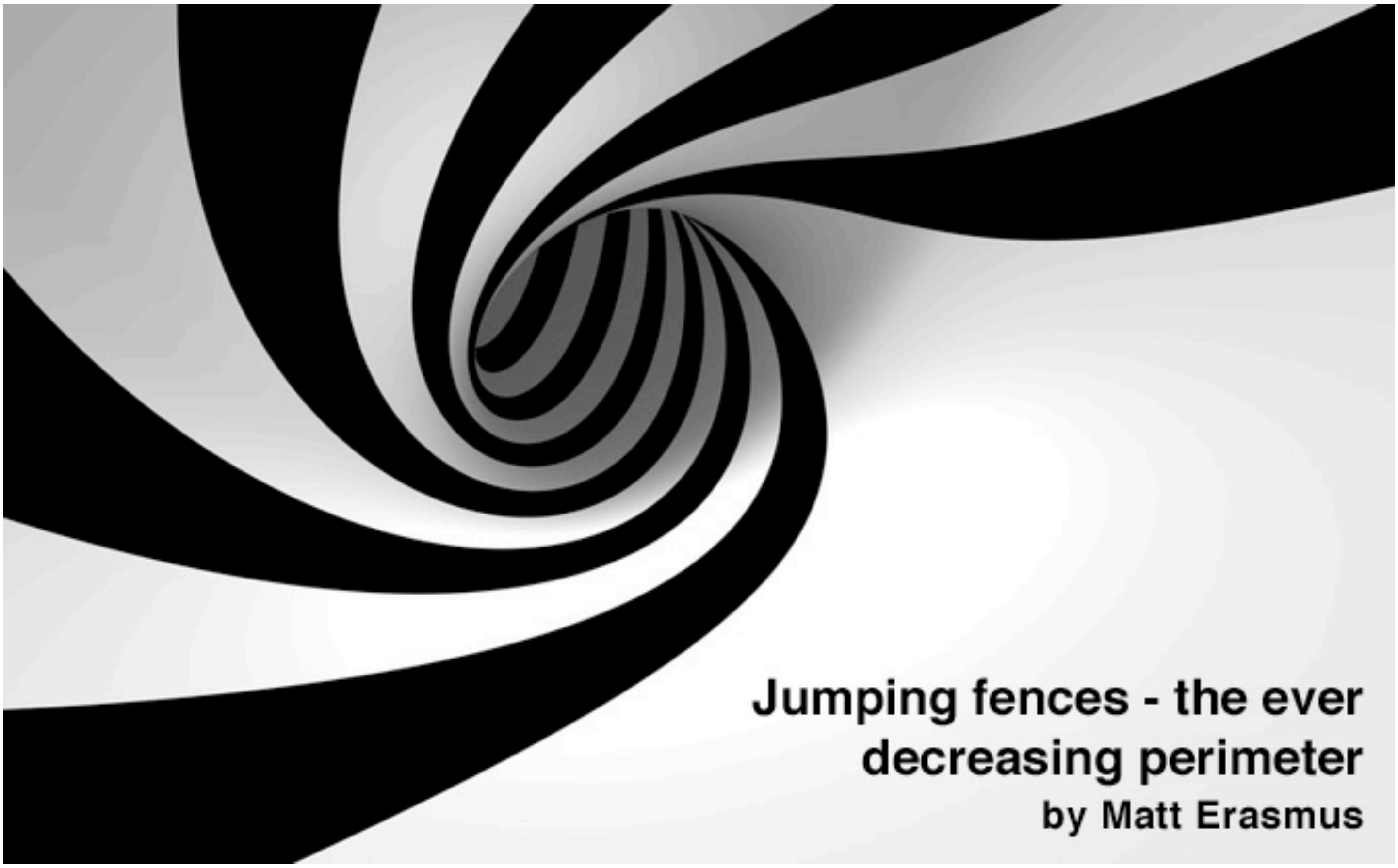
In this video, security researcher and expert on malicious PDF files Didier Stevens discusses how these files work and offers protection tips.

Dissecting the hack: the f0rb1dd3n network

(www.net-security.org/article.php?id=1303)

In this video, Jayson Street talks about his book - "Dissecting the hack: the f0rb1dd3n network" - published by Syngress. The book aims to inform and educate executives and upper management on the importance of information security without alienating or losing them in the process. Though this book will also appeal to the layman and information security professional as well.

www.youtube.com/helpnetsecurity
Subscribe to our YouTube channel.
Get notified when we add security videos.



Jumping fences - the ever decreasing perimeter

by Matt Erasmus

At present, we are fighting a losing battle against an enemy with nothing to lose. Identities are bought and sold for a pittance; credit cards and personal information are leaked to the underground and botnets grow in size on a daily basis. There seems to be no end it sight.

Do we have ourselves to blame for the current state of insecurity? Are we catering too easily to the whims of the corporate monster? Yes, many are doing a terrific job at protecting the network perimeter and keeping the wolves at bay, but I get the feeling that it's all about to change again and we will be very hard pressed to keep up - let alone win the war.

In the late eighties and early nineties, there was little need for the kind of network filters that we have today. Prior to the dot-com boom, there were a only handful of servers with various services running on them that needed protecting. These services generally had to be protected from a list of "bad" hosts or generally not allowed to anyone who wasn’t on the "good" list. The early firewalls and network perimeter protection devices had a basic set of rules or access control lists in place to get the job done. This was the very beginning of the whitelist/blacklist practice. And then there was an explosion - the number of hosts on the Internet grew exponentially. Commercial and private use quickly became the norm.

Due to the vast number of machines online, port forwarding and network address translation became commonplace. This was especially true in Africa where there weren't that many ISPs or free IP addresses to begin with.

The mail server that was vulnerable to exploit X may not have had its own network interface on the public Internet, but with the advent of Linux and stateful packet filters it was possible to bring the server online with little effort. And then, it was taken offline by some nefarious character. The way we filtered traffic had to change to avert new threats. We stopped looking at traffic entering our network at the border gateway and began also tracking the things that were leaving it.

The insider threat added a new twist to the game. Now there was an unknown, usually angry ex-employee on the inside network trying to get our confidential data out of our network to his new employer, our biggest competitor. Egress filtering didn't change the perimeter that much, but it did change how security professionals treated it. The perimeter was now filtered for outgoing as well as incoming traffic. Along with improved filtering came the analysis of the traffic all the way down to the packet level. Intrusion detection systems looked at the traffic flowing through the network and alerted on anomalies or signatures of known issues. This is our current position. We have the technology to detect data leaving our network that shouldn't. Data leakage prevention or protection, depending on which text you read, is the new hot topic, along with other marketing buzz words like "cloud computing" and "software as a service". But that's another story for another day. The perimeter has moved so close to home that we now consider dealing with vulnerable hosts as the norm.

The Jericho Forum has very interesting ideas on the topic of network de-perimeterization and how we should consider the hosts we talk with on a daily basis to be compromised. Your network is not your own any more and instead of encryption being used between offices on either side of the world, it's being used for encrypting all traffic flowing from servers in the same rack in your own data center. Add to that the idea of how the Web is evolving on a daily basis. The idea of static pages displaying data on the latest and greatest product is an idea of the past. "User generated content", dynamic Ajax pages and the whole Web 2.0 era we are currently in, have moved the perimeter. Data flows from one server to another and there is no easy way to define where the line between the good and the bad lays.

Firewalls as hardware devices on the gateway into the corporate network are no more. They are still there doing their job, however the overall opinion is that you shouldn't rely on them for increasing the security of your network. We now have firewalls running on individual hosts. Intrusion detection systems have moved from first being network based, then host based, to finally being system based, looking at traffic flowing over specific protocols.

We have mostly ourselves to blame for this. Because of the way that everything seems to be moving into the cloud, the attackers have moved up the stack from the network layer to the application layer. Where once the network perimeter was defined and protected by a specific set of tools and devices, we are now reliant on a more finely tuned machine to protect us - a machine that is constantly misconfigured or not configured at all. Attacks at the application layer are harder to define and single out simply because they can look so much like legitimate traffic that it's hard to tell the good from the bad.

The biggest problem I have with the ideas behind network de-perimeterization is that it all seems to hinge on compromise. The goal posts are being moved by forces beyond our control and yet we as a group seem to accept this. While some are very vocal about not accepting the changes, the rest seem to accept this fate and continue regardless. While there are some great concepts behind the ideas, is it enough to ensure that we maintain security? Encryption is not the silver bullet many expected it to be (tinyurl.com/yzbbgc3). We constantly seem to be trying to secure protocols that had never any security built into them to begin with. As was recently shown (tinyurl.com/mjm2jy, tinyurl.com/lcde6b), even the solutions that were believed to be the answer to so many problems are showing chinks in its armor.

All that being said, I don’t think we’re going about de-perimeterization the wrong way. The idea of end-to-end encryption is great, but what happens when that encryption is broken? Do we move to the new and unchartered territory of quantum computing and quantum encryption? It seems a long way off before we see a practical implementation of this new technology. But, that also brings back the question of layering security on top of insecurity. Actually, the whole notion of de-perimeterization has me torn. There are both pros and cons to the entire idea. While to some it may seem like the silver bullet we have been looking for all this time, it has been proven time and time again, that there is no such thing in information security.

There is never going to be one magical solution that will cover all grounds. Information security is not a destination, it is a very long and bumpy road. Let’s just hope we’ll be able to travel it without steering off course.

Matt Erasmus is an information security geek with a strange obsession for malware, zombies and packet Fu.

MIS TRAINING INSTITUTE'S

INFOSEC WORLD 2010

April 17-23 • Orlando • Disney's Coronado Springs Resort

▸ CONFERENCE & EXPO

InfoSec World 2010 Agenda Preview

KEYNOTE PRESENTATIONS

Schneier on Security

Bruce Schneier, *Chief Technology Officer,* BT Global Services

Technology Trends That Will Shape Tomorrow's Organization and Change Your Life

Jeff Jonas, *Chief Scientist,* IBM Entity Analytic Solutions Group; IBM Distinguished Engineer

The State of Cyber Security: How the Information Assurance Paradigm Is Shifting and What It Means To You

Israel Martinez, *Co-Chair,* The National Cyber Security Council

Managing Security Risk and Complexity: Marching to the Drums of Business and National Security

Michael Assante, *Vice President and Chief Security Officer,* North American Electric Reliability Corporation (NERC)

TOPIC HIGHLIGHTS INCLUDE…

- Cloud Computing: A Look Into the Usage and Risks
- Attacking and Defending SSL VPNs
- Preventing Data Leakage in the Web 2.0 Environment
- Auditing VMware
- Defending Against the Worst Web-Based Application Vulnerabilities of 2010
- Testing Your Firewalls and Other Perimeter Defenses
- Performing an IT Governance Audit
- Responding to a Wireless Attack on Your Network
- 2010 Privacy Update
- iPhone Fuzzing and Payloads
- Advanced Pen Testing
- Conducting a Forensic Computer Investigation for Non-Law Enforcement
- Risk and Controls in an IP-Based, Unified Messaging Environment
- Locking Down Windows Clients: XP, Vista and Windows 7
- Google and Beyond: Advanced Search Engine Hacking and Web-Based Intelligence Gathering
- Advanced Power Tools for Free: A Security Pro's Guide
- Spear Phishing: Why it Works and How to Thwart It
- Secure SDLC for Software Assurance
- Meaningful Metrics and GRC: What to Measure and Why
- Using Free Tools to Assess and Audit Your Wi-Fi Network

▶ FOR AGENDA UPDATES VISIT: www.misti.com/infosecworld