[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 31 - September 2011

THE CHANGING FACE OF HACKING

A NEW APPROACH TO DATA CENTRIC SECURITY

THE FUTURE OF IDENTITY VERIFICATION THROUGH KEYSTROKE DYNAMICS

THE NEED FOR FOUNDATIONAL CONTROLS IN CLOUD COMPUTING

SECURITYBYTE CONFERENCE & WORKSHOPS 2011

blackhat usa+2011

VISITING Bitdefender IN ROMANIA

Entrust® Securing Digital Identities & Information

<Let's Talk Mobile Authentication

Strong mobile authentication. For a stronger enterprise.

Securing mobile devices. As mobile devices continue to expand in capability and popularity, they present tremendous opportunities for organizations such as email communication or remote access VPN. And as the use of mobile devices and applications grows, so does the rate and sophistication of identity attacks on today's popular mobile platforms.

Token Trade-Up Offer
Trade-in your hard tokens for comprehensive soft-factor and mobile authentication — *free from Entrust.*

Ready to go? Visit **tokentradeup.entrust.com >**

Soft tokens. Using mobile soft tokens to enable strong authentication to enterprise networks, applications and resources dramatically improves enterprise security. Not only are they simple to use and deploy, they increase user adoption and promote cost-savings by removing the need to issue expensive hardware tokens.

Mobile power. Whether it's via digital certificates or one-time-passcode (OTP) tokens, Entrust IdentityGuard Mobile gives users the power to leverage mobile devices for resource access and secure communication.

Let's talk. Visit entrust.com/mobile-security to discover how Entrust's proven approach can complement your existing enterprise authentication solutions.

+1 888 690 2424 | entrust.com | entrust@entrust.com | +44 (0) 118 953 3000

TABLE OF CONTENTS

Summer is slowly winding down and the security community continues its heavy work. Cyber thugs, obviously not slowed down by the heat, are in a severe need of a beat down.

Since the last issue of the magazine saw the light of day, we traveled the world and attended Black Hat in Las Vegas, the SecurityByte Conference in Bangalore and the fantastic Bitdefender re-branding event in Romania.

Meeting security professionals at all these gatherings gave us the assurance of having outstanding and talented people on our side of the fight, and we hope that thought will encourage you as it did us.

With that in mind, enjoy the 31st issue of (IN)SECURE!

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

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

Researchers identify flaws in the Advanced Encryption Standard

Researchers have found a weakness in the AES algorithm. The attack applies to all versions of AES even if it used with a single key, and shows that finding the key of AES is four times easier than previously believed; in other words, AES-128 is more like AES-126.

Even with the new attack, the effort to recover a key is still huge: the number of steps to find the key for AES-128 is an 8 followed by 37 zeroes. To put this into perspective: on a trillion machines, that each could test a billion keys per second, it would take more than two billion years to recover an AES-128 key.

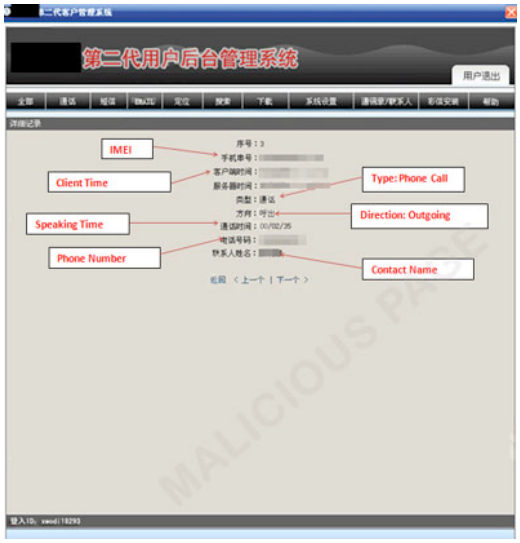
Because of these huge complexities, the attack has no practical implications on the security of user data; however, it is the first significant flaw that has been found in the widely used AES algorithm and was confirmed by the designers.

The AES algorithm is used by hundreds of millions of users worldwide to protect internet banking, wireless communications, and the data on their hard disks.

It is also used in more than 1700 NIST-validated products and thousands of others; it has been standardized by NIST, ISO, and IEEE and it has been approved by the NSA for protecting secret and even top secret information.

The attack is a result of a long-term cryptanalysis project carried out by Andrey Bogdanov (K.U.Leuven, visiting Microsoft Research at the time of obtaining the results), Dmitry Khovratovich (Microsoft Research), and Christian Rechberger (ENS Paris, visiting Microsoft Research).

Chinese mobile phone monitoring service found



What do you think cyber crooks do with the information collected from mobile phones by malware? Trend Micro has one of the answers to that question. Its researchers have recently discovered a Chinese website that provides a mobile phone monitoring service to those willing to pay between 2,000–3,600 Chinese yuan (US $300–540).

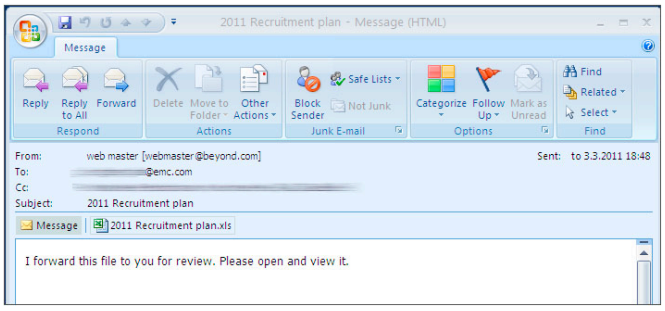
Once the payment is executed, the customer is provided with access to a backend server of the service, where all the collected information can be viewed.

The first step for every customer is to send out an MMS carrying the malicious payload to the target's cell phone, and he or she can customize it in such a fashion as to appear it comes from a phone number familiar to the recipient, making it more likely that the attached payload will be downloaded and installed.

Once installed, the malware is free to collect information and to send reports to the backend service. Reports about executed phone call, sent text messages, emails and the location of the device are also delivered.

For now, the service is available for those who want to spy on someone using a phone running on Symbian or Windows Mobile, but the researchers say that it is highly likely that users with Android devices won't be safe from it for long.

Is this the phishing email that caused the RSA breach?



"I forward this file to you for review. Please open and view it," says simply the email that is thought to have been the means of deploying the backdoor that resulted in the massive RSA breach in March.

Using a few of the details shared about it - namely, that the email contained an attachment called 2011 Recruitment plan.xls, and "2011 Recruitment Plan" in the subject line - F-Secure researcher Timo Hirvonen burrowed for months in the malware database shared by Virus Total with security companies, in the hopes that the attached file was uploaded for a check by someone.

As it turns out, both the email and the attachment were uploaded.

With a "From" email address spoofed to look like it was coming from the web master of recruiting website Beyond.com, it was sent to an EMC employee and CC'd to three others on the 3rd of March.

The attached Excel spreadsheet contained a Flash object that was executed by Excel and took advantage of a vulnerability to install the Poison Ivy backdoor on the victim's computer.

The backdoor then proceeded to contact a server from which the attacker was able to access remotely the workstation and other network drives, and from that, to the rest of the network.

Google servers as a DDoS tool

Google's servers can be used by cyber attackers to launch DDoS attacks, claims Simone "R00T_ATI" Quatrini, a penetration tester for Italian security consulting firm AIR Sicurezza.

Quatrini discovered that two vulnerable pages - /_/sharebox/linkpreview/ and gadgets/proxy? - can be used to request any file type, which Google+ will download and show - even if the attacker isn't logged into Google+.

By making many such request simultaneously - which he managed to do by using a shell script he's written - he practically used Google's bandwidth to orchestrate a small DDoS attack against a server he owns.

He points out that his home bandwidth can't exceed 6Mbps, and that the use of Google's server resulted in an output bandwidth of at least 91Mbps.

"The advantage of using Google and make requests through their servers, is to be even more anonymous when you attack some site (TOR+This method). The funny thing is that Apache will log Google IPs," says Quatrini. "But beware: igadgets/proxy? will send your IP in Apache log, if you want to attack, you'll need to use /_/sharebox/linkpreview/."

He says he has discovered the flaws that allow the attack on August 10 and that he contacted Google's Security center about it. After 19 days of receiving no reply from Google, he published his findings.

Linux source code repository compromised

The Kernel.org website - home to the Linux project and the primary repository for the Linux kernel source code - sports a warning notifying its users of a security breach that resulted in the compromise of several servers in its infrastructure.

The attackers are thought to have gained root access on a server via a compromised user credential, and to have escalated their privileges from there. After having done that, they proceeded to modify files belonging to ssh (openssh, openssh-server and openssh-clients) and add a Trojan to the system start up scripts so that it would run every time the machine was rebooted.

Luckily for everyone, the Linux kernel source code is unlikely to have been tampered with.

"That's because kernel development takes place using the git distributed revision control system, designed by Linus Torvalds," it is explained. "For each of the nearly 40,000 files in the Linux kernel, a cryptographically secure SHA-1 hash is calculated to uniquely define the exact contents of that file. Git is designed so that the name of each version of the kernel depends upon the complete development history leading up to that version. Once it is published, it is not possible to change the old versions without it being noticed."

The Linux kernel source code is unlikely to have been tampered with.

How the unredacted US cables were revealed to the public

A few days after former WikiLeaks staffer Herbert Snorrason refused to say who inadvertently made public the password for the encrypted file containing unredacted US diplomatic cables, some people managed to piece together the various hints dropped by involved parties and track down where it has been published.

In short, the password has been always in plain sight, printed in the book by Guardian journalist David Leigh titled "Inside Julian Assange's War on Secrecy". The Guardian claims that they were told by Assange that the password would be changed a few days after the journalist downloaded the file.

Unfortunately, the file was inadvertently picked up by Daniel Domscheit-Berg when he left the organization and took a dataset off the server containing the file with him. Once he returned that which he took to WikiLeaks, the whole content was shared online via BitTorrent by WikiLeaks supporters, who were also unaware that the file in question was there.

In the recent escalating war of words between Domscheit-Berg and Assange, the former tried to prove that Assange and WikiLeaks couldn't be trusted with sensitive data. According to Der Spiegel, people associated with OpenLeaks began hinting of the existence of the file "in the wild".

Finally, somebody pointed Der Freitag - a German weekly publication and OpenLeaks partner - in the direction of the location of the password. They didn't share the actual information with the public, but confirmed that anyone familiar with the material could find it. It took only a couple of days for that claim to be proven right, and the password was revealed.

WikiLeaks accused the Guardian and its journalist of being responsible for the leak and has spoken to the US State Department in order to commence legal action against the paper and the journalist, and to make sure that the informants mentioned in the cables were warned about the danger they might find themselves in following this mess.

Japanese defense contractor breached

Mitsubishi Heavy Industries has revealed that its networks have been breached in what is considered the first cyber attack to hit Japan's defense industry.

According to Reuters and Japanese newspaper Yomiuri Shimbun, the breach was discovered on August 11, and the investigation mounted by the company revealed the existence of some 80 infected computers in the company headquarters in Tokyo and various R&D and manufacturing sites in Kobe (nuclear power station components), Nagasaki (escort ships) and Nagoya (guided missiles and rocket engines).

A variety of malware has been discovered on said computers, including an information-stealing Trojan. The company has admitted that it is possible that confidential information was stolen by the attackers.

"We've found out that some system information such as IP addresses have been leaked and that's creepy enough," added a company spokesman. "We can't rule out small possibilities of further information leakage but so far crucial data about our products or technologies have been kept safe."

Bots troll hacker forums to discover data breaches

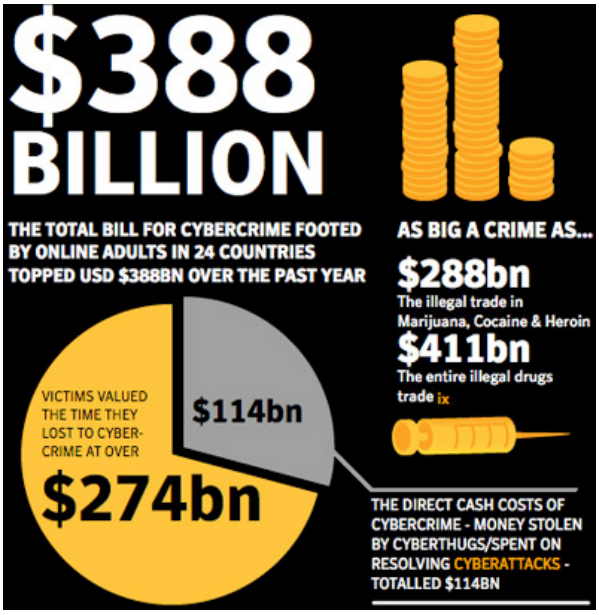
Texas-based CSIdentity has managed to develop software that can mimic the speech patterns of cyber crooks, allowing the company to simultaneously engage a great number of hackers looking to sell stolen information on online forums, chat rooms, blogs, websites and torrent sources.

As is customary for this type of transaction, the crook usually offers a sample of the wares he's selling to prove that it's good, and that is the information that the firm is after. The software collects this proffered information and sends it to the company's team of human investigators to analyze and figure out from where the information was stolen and to whom it belongs.
The bots are quite adept at posing as cyber criminals or people involved in the trade of stolen information. The company has analyzed thoroughly how these people interact online, and the specific lingo is recreated by the bots.

CSIdentity earns money from the companies and organizations that have signed up for its services, and the main goal for retaining those services is the ability to quickly discover that their systems have been compromised and its information extracted.

Unfortunately, the bots are unable to help law enforcement investigators involved in more complex sting operations aimed at well-organized cyber criminals usually coming from Eastern Europe and Russia. The bots should be able to be taught the language, but the appropriateness of their reactions is simply not to be trusted when it comes to such delicate operations.

Global cost of cybercrime? $114 billion annually



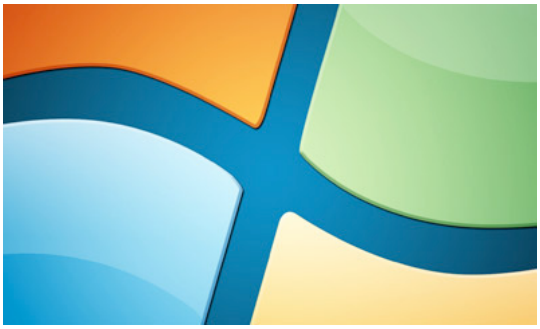
For the first time a Norton study calculates the cost of global cybercrime: $114 billion annually. Based on the value victims surveyed placed on time lost due to their cybercrime experiences, an additional $274 billion was lost.

With 431 million adult victims globally in the past year and at an annual price of $388 billion globally based on financial losses and time lost, cybercrime costs the world significantly more than the global black market in marijuana, cocaine and heroin combined ($288 billion).

According to the Norton Cybercrime Report 2011 more than two thirds of online adults (69 percent) have been a victim of cybercrime in their lifetime. Every second 14 adults become a victim of cybercrime, resulting in more than one million cybercrime victims every day.

The report reveals that 10 percent of adults online have experienced cybercrime on their mobile phone. In fact, Symantec reported there were 42 percent more mobile vulnerabilities in 2010 compared to 2009 – a sign that cybercriminals are starting to focus their efforts on the mobile space.

Windows 8 new security features



Setting aside usability, efficiency, speed and all the other things that are most important to regular users, what news does this preview bring to those of us most concerned about security?

Windows 8 has a built-in antivirus that actually works. "It stopped not only the EICAR test file, but more than a dozen malware items in Metasploit," confirmed a security instructor that has been testing the beta version of the new OS version.

Another crucial change is Microsoft's abandonment of BIOS ROM in favor of Unified Extensible Firmware Interface (UEFI), which allows for a quicker boot up of the machine, but also things like automatic scanning of a USB drive used to boot the OS.

This particular feature, which lets users boot up a portable Windows environment from an USB drive, and the purposefully infected USB triggered a warning about an "invalid signature" and stopped the booting process.

Windows Defender, Microsoft's antispyware software will also be upgraded "all the way up though antimalware, antivirus," according to Steven Sinofsky, president of Microsoft's Windows and Windows Live division, and users will be able to chose if they want to employ it or some other AV solution.

A curious new feature that will be available for users of touchscreen-equipped PCs is the ability to create passwords for accessing the machine by choosing a combination of pictures and gestures (taps, circles, straight lines, etc.), which will surely be a welcome addition to those users whose memory is more easily triggered by visuals and motions.

Botnet masters are spreading their resources

Having noticed that in some of the top spam countries the number of infected computers falls by a few percents as in others rises by nearly the same amount, Kaspersky Lab researchers have analyzed the information gathered on the top 11 countries on that list and have come to the conclusion that botnets in various countries are very likely run by the same people.

Taking into consideration the fact that the size of botnets continually changes and that there are smaller, "local" botnets in every country that interfere with the measuring of the weekly spam traffic, they have noticed that some of these countries present a similar dynamic when it comes to spam distribution.

"Synchronous distribution of spam from countries located on different continents does not mean that computers in these countries are united in one big botnet," explain the researchers. "Several small zombie networks can also operate synchronously, receiving commands for distributions from the same individuals."

As botnets can be run from anywhere in the world, it stands to reason that the bot herders have decided to concentrate their infection efforts on countries that still don't have effective laws regulating internet activity. Also, another logical step for them is to spread their botnets throughout various countries in case that one of them comes to the conclusion that a nation-wide alert to infected users (along with disinfection instructions) is a good idea.

DigiNotar breach report reveals lousy security practices

An interim report issued by security audit firm Fox-IT, who has been hired to investigate the DigiNotar breach, revealed that things are far worse than we were led to believe.

"The most critical servers contain malicious software that can normally be detected by anti-virus software," it says. "The separation of critical components was not functioning or was not in place. We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN."
All CA servers were members of one Windows domain and all accessible with one user/password combination. Moreover, the used password was simple and susceptible to brute-force attacks.

The software installed on public-facing web servers was outdated and unpatched, and no antivirus solution was installed on them. There was no secure central network logging in place, and even though the IPS was operational, it is unknown why it didn't block at least some of the attacks.

"In at least one script, fingerprints from the hacker are left on purpose, which were also found in the Comodo breach investigation of March 2011," they revealed. "Parts of the log files, which would reveal more about the creation of the signatures, have been deleted."

Researchers steal 20GB of corporate emails via doppelganger domains

According to researchers from the Godai Group, there is an easy-to-execute type of scheme that is likely already being perpetrated by individuals located in China. It consists of using so-called "doppelganger domains" and mail servers for intercepting emails sent by mistake to them.

151 of the Fortune 500 companies profiled by the two researchers are potentially vulnerable to this kind of attack, including IT companies such as Yahoo, Dell, Cisco, IBM, HP and IBM.

The main problem here is that almost all of those companies have regional subdomains that usually look something like this: xx.company.com (the "xx" stands for the top-level domain of the countries where the company is present). As it turns out, people quite often make the mistake of omitting the first fullstop when writing emails in a hurry. That would not represent such a big problem if these destination addresses were non-existent, but when someone takes the trouble to register a doppelganger domain, set up a mail server for it and configure it to to receive all email addressed to it, he is able to harvest all the information contained in these messages, without the company or the sender being none the wiser.

And this is exactly what the researchers did. The result? "During a six-month span, over 120,000 individual emails (or 20 gigabytes of data) were collected which included trade secrets, business invoices, employee PII, network diagrams, usernames and passwords, etc," they say.

All that information, and they were basically doing nothing. But, as they point out, the possibilities don't end here. The attackers can also execute a Man-in-the-MailBox type of attack.

The changing face of hacking

by Chris Burchett

On the morning of May 29, 2011, visitors of the PBS news website were probably more than a little surprised to read that the rappers Tupac Shakur and “Biggie” Smalls were not only still alive, but apparently in hiding in a small town in New Zealand. The story - headlined "Tupac still alive in New Zealand" - went on to describe how the rappers were living in seclusion in a town that could not be named "for security reasons."

Clearly, something was amiss.

In reality, the site had been hacked: broken into and a fake story placed on its main page as a part of a series of revenge attacks by the infamous hacker group LulzSec.

The group was angry with PBS over the handling of a story about Bradley Manning and his role in providing WikiLeaks with a large amount of classified documents.

While the PBS staff may have felt irritated and embarrassed, they were in many ways lucky. Within a couple of months, security giant RSA (a division of EMC) would suffer a far more serious and sophisticated attack that would open the way for a series of breaches hitting critical defense contractors such as Lockheed Martin and Northrop Grumman.
The scale and the repercussions of these two attacks were very different – yet they shared something in common. They both demonstrated that motivated and technically adept individuals (or teams) could and would exploit any weakness to penetrate and utilize systems for their own ends.

Hackers demonstrated that regardless of who you are or how well you think you have secured your computers – sooner or later someone is going to find a way in. Once that happens, all bets are off.

Hacking: What it means, and how it began

The computing term "hacker" (as opposed to its other uses, such as to identify amateur radio enthusiasts) dates back to at least the early 1960s, when students and researchers coined the phrase in reference to both their obsessive hacking at their keyboards and their capability to take code designed for one purpose and hack it into shape for something else. At the time it carried none of the pejorative implications is does now - if anything, it was a term of respect.

Around the same time, early attempts to manipulate telephone systems (phreaking) by generating rapid clicks using handsets or creating tones to place free calls, began to gain some visibility in popular culture. It threw up such characters as The Whistler and Captain Crunch, creator of the infamous "blue box" - a device capable of generating tones to give the caller control over parts of the phone system and essentially make free calls.

Nevertheless, while phreaking was used to perpetrate fraud, it was often essentially exploratory and even playful in nature.

These two subcultures developed side by side, and while phreaking is now little more than a historical term, "hacker" has morphed beyond all recognition, encompassing everyone from hobbyists and computer scientists, to full-blown criminal entrepreneurs.

While phreaking was used to perpetrate fraud, it was often essentially exploratory and even playful in nature.

For the sake of simplicity, I'm going to use the term only to refer to criminals who attack systems for profit or to gain notoriety - often also called "crackers". While most hacking activity is actually highly beneficial to the computing industry as a whole, throwing up new technologies and even whole industries, a small group of malicious hackers have become emblematic of both the Internet age and the evolving nature of crime in the twenty-first century.

As systems become increasingly interconnected, and as more and more saleable information went online, it became clear to criminals in general - and criminally minded hackers in particular - that the ability to enter a computer system and manipulate it without the permission of the owner could be turned to their advantage. These so-called "black hat" hackers (to differentiate them from the more legally responsible "white hats") have become such a staple of popular culture that it is hard to imagine a Hollywood thriller that doesn't feature someone hacking a computer system at some point.

The reality of hacking, however, is very different from the stereotypes. Malicious hacking, the kind that generates headlines on a weekly basis and causes disruption to online services, is nothing like the glamorous activities of Hollywood movies in which a few keystrokes and a pencil-chewing pause for tension result in a successful penetration of some target system. Nor are criminal hackers the archetypal "kid in a basement" eating pizza and drinking cola.

Criminal hacking has evolved and developed until it has become, like so many other uses of the Internet and information technology, big business.

The industrial age of hacking

January 20, 2009, was notable for two events. The first was the inauguration of the 44th President of the United States, Barack Obama. The second was the announcement made by Heartland Payment Systems about one of the largest credit card breaches in history.

Heartland Payment Systems is a credit card payment processor handling transactions for (at the time) around a quarter of a million businesses. Heartland's systems processed around 100 million transactions per month, and it became apparent to investigators that those systems may have been compromised as far back as a year before.

The potential scale of the breach was simply staggering.

But Heartland was by no means a solitary blip on the security radar - far from it. If anything, the attack on Heartland's systems was simply business as usual. Hacking, and especially stealing information from businesses, had entered an industrial age.

The previous year, 2008, had also been a bad one for big breaches. Earlier in the year, Hannaford Brothers, a Maine-based supermarket chain, announced that over 4 million credit card numbers had been stolen in a breach. Also in 2008, 7-Eleven suffered a breach, while RBS Worldpay suffered a smaller, but no less embarrassing breach affecting its customers.

A pattern of attacks was emerging: hackers targeted large processors of credit cards to steal saleable information before moving on to the next victim.

Anatomy of a hack

Apart from holding credit card data, the targets of many of these criminal hacks had little in common with each other. Nevertheless, the process of attacking them bore many similarities. Initially the attackers looked for a weakness in the victim's systems. This might be as simple as a poorly configured computer, perhaps left with default usernames and passwords or missing critical patches.

In other cases, vulnerabilities in the web-facing applications of the target were identified and used. These vulnerabilities often took the form of improperly written code to read information from databases accessible through the web application such as a customer account database. As such, the attacker could utilize a technique known as an SQL injection attack to literally turn the victims' applications against themselves, and gain access to a trusted system inside the target's defenses.

From that point onwards, the attackers continued to probe, looking for more systemic weaknesses, testing security (both technical security and the ability of the security personnel to respond to attacks) while they planned their next move.

Once a suitable target system was found and accessed, the attackers would insert custom software to quietly and steadily steal information such as credit card data as it transited through the network.

Once enough data was hauled in, the attackers would return and simply copy the information, before sending it on to their customers and cashing the check.

This type of hacking was, and is, very common. Indeed, even though SQL injection attacks have been well understood for ten years, according to one recent study by Verizon and the US Secret Service this technique is still used in around one fifth of this kind of criminal attack. Indeed, it is this ability to continue to use well-known (and therefore addressable) vulnerabilities than enables hacking to be such a profitable enterprise.

One of the great ironies regarding this series of breaches is that some of the biggest ones were perpetrated by a small team led by a single hacker – Albert Gonzales. In fact, Mr. Gonzales - who is currently serving 20 years in prison - managed to organize and pull off some of the largest data breaches in history while simultaneously working as an informer and advisor to the US Government.

A new age of hacking

With the arrest and conviction of the man responsible for such massive breaches, it might be thought that the security world would at least experience a small reprieve from attacks. But even though the number of spectacular, big breaches hitting the headlines diminished, their absence simply masked a far more serious problem.

As Kim Peretti, Former Senior Counselor, DOJ, said of Gonzalez, "…comparing him to other criminals out there, especially internationally, (he was) towards the upper end but certainly not at the top end of skill or ability."

Unfortunately, that core of highly capable criminal hackers usually operating outside of the US has been developing over the last couple of years, and they cooperate in targeting, infiltrating and attacking systems for profit.

These attackers typically use highly customized malware designed in such a way as to make it extremely difficult to detect and even harder to analyze after a breach has occurred.

Even the way in which organizations are targeted reflects this "business-centric" hacker ethos. While some organizations are certainly targeted specifically, in the majority of attacks that have been studied the hackers were actually searching for known vulnerabilities that they could exploit. If an organization exhibited these vulnerabilities, they became a target for an attack. If not, the hackers simply moved on to find a new target - it's just more efficient and, sadly, there is no shortage of potential targets.

While some organizations are certainly targeted specifically, in the majority of attacks that have been studied the hackers were actually searching for known vulnerabilities that they could exploit.

The post-industrial age

While the hacker-for-profit world underwent changes in the last few years, a new form of hacking began to make its presence felt: hacktivism. The term actually goes back much further, to the mid-1990s, and the act of attacking a computer system to make a political point predates that by at least a decade, but it is really within this last year that hacktivism has become a staple of main stream discussion.

The title of "most famous hacktivist group" would probably have to be awarded to the hacker collective Anonymous, which sprang energetically onto the cyber stage by perpetrating a number of attacks on credit card processors in defense of WikiLeaks, in addition to attacks on Sony to retaliate their lawsuit against George Hotz, who had "jailbroken" the Sony Playstation. Anonymous has also been active for some time hacking government sites around the world, including those in Zimbabwe, Egypt, Tunisia and The Netherlands.

Attacks often took the form of website defacements, but also included Distributed Denial of Service (DDoS) attacks, during which sites are flooded with incoming requests and simply get overwhelmed - a type of attack that is troublesome and difficult to defend against without adequate preparation.

Following hard on the heels of Anonymous came the highly visible attacks of LulzSec, an apparently smaller but highly active hacking group who went on to target Sony, Fox, PBS and high-profile government sites such as those belonging to the FBI and the CIA. Although LulzSec has been short-lived (there is evidence that other hacking groups turned on them and have forced the group to disband) it seems unlikely that hacktivism as a whole will vanish with them.

If anything, we may stand on the brink of a new era of hacking in which distributed groups can quickly form and make use of tools that are readily available to cause disruption to government and business targets alike.

Building on success, APTs, and the script-kiddie horde

Tools to attack systems are not just the prerogative of a professional criminals and hacker collectives. In fact, many automated tools requiring little in the way of technical understanding are freely available on the Web for download. These tools enable a kind of point and click hacking that has given rise to a new generation of so-called script kiddies - hackers who have little in the way of technical knowledge beyond the rudiments necessary to activate the programs.

While the technically adept hackers may scoff at the capabilities of these neophytes, they still represent a potential problem for businesses, if only because they can cause disruption to online services and potentially stumble upon valuable and poorly protected information.

Of greater concern, though, are attacks from the other end of the capability spectrum.

These attacks originate from overseas and don't target saleable data such as credit card information, but highly sensitive government or research information.

These threats are collectively referred to as APTs, an acronym for Advanced Persistent Threats, and are generally considered to originate mainly in the Asia-Pacific region. In January of 2010, Google described how their systems had been under attack for approximately a year in what later became known as Operation Aurora.

This attack also targeted a number of high-tech and defense businesses including Juniper Networks, Yahoo!, Dow Chemical and several others. Analysis later showed that it was highly likely the attack was state-sponsored and was certainly technically highly sophisticated.

These attacks typically use a combination of tried-and-tested social engineering methods (such as sending fake emails carrying malware payloads) in addition to using undisclosed vulnerabilities in software to gain access to systems. And unlike with the "hacking for cash", these attacks are highly targeted.

The attackers continue to attack an organization's systems for as long as it takes to find a vulnerability and exploit it.

Despite the alarming nature of APTs, security experts disagree over how widespread such attacks actually are - and in some cases simple criminal hacking may be incorrectly categorized as an APT. For most businesses, it seems likely that the professional criminal is a greater threat than state-sponsored cyber espionage.

For most businesses, it seems likely that the professional criminal is a greater threat than state-sponsored cyber espionage.

Adding fuel to the fire

If the situation seems complex and difficult to manage now, things may be about to get a whole lot worse.

One of the most powerfully disruptive forces at work in the world of information technology may be the concept of "cloud." Cloud computing models (at least public cloud models) essentially remove the physical hardware from an organization's infrastructure and replace it with services offered through the Internet.

While such services offer significant business benefits, including significant cost savings, rapid scalability and a high degree of self-service for business units, they also change the security landscape significantly.

Without actual physical control over the systems, security becomes much harder to enforce and measure. Add to that the fact that these systems may well be shared with other companies, and that they must be accessed remotely, and the problems of securing traditional, brick-and-mortar IT infrastructure may seem small by comparison.

Cloud computing has the potential to fundamentally change the face of malicious hacking in ways that are hard to predict at this point. There are, however, two elements that are difficult to dispute.

The first is that cloud models provide a high-degree of centralization of resources. Public clouds, the kind that are shared between many organizations, will become large repositories for information. Much of it will undoubtedly be of little value but, as business are driven by economic pressures to outsource more and more of their core business functions to cloud providers, more and more sensitive, and saleable, information will reside out there, in the cloud. That means that cloud providers could become the ideal target for hackers.

Willie Sutton, the prolific 1930s bank robber, famously responded to the question, "Why do you rob banks?" with the quip, "Because that's where the money is." If the same logic is applied to data theft, then cloud providers should expect to receive increasing and unwelcome attention from cyber criminals as the value of their data stores rises.

The second effect of cloud computing on criminal hacking is that it may offer capabilities and tools on a previously unimaginable scale.

The capability of cloud computing models to scale services at incredibly low cost means that for very modest fees significant computing resources can become available to individuals with nothing more than some technical skill and a credit card (theirs or someone else's.)

In January of 2011, Thomas Roth, a German security consultant, claimed to have cracked a WPA wireless network key using Amazon's Elastic Compute Cloud (EC2), in around 20 minutes at a total cost of less than $10.

While other researchers have pointed out that the passwords in these cases were short (6 characters) and therefore relatively insecure, the simple fact that cloud resources offer so much power on tap for so little cost is concerning.

Perhaps more concerning is the capability to leverage cloud resources to perform denial of service attacks, or host very large botnets (as has already happened).

This also raises the specter a cloud service being utilized by hackers to attack other cloud storage providers, or even itself.

Clearly, combining a highly powerful tool set with a new model for keeping information secure presents both opportunities to improve the way security is handled as well as significant risks. Such an opportunity will be to implement more effective and consistent security across public cloud environments possible with the limited resources of any individual company.

However, it will require investment and commitment on the part of the cloud providers, and their customers, to stake a claim to the new frontier of computing, ahead of the hacker/cracker communities.

Conclusion

Hacking is a term loaded with many meanings. While its original usage was intended to carry no pejorative meaning, it has sadly become synonymous with malicious and often illegal activity.

While many (probably most) hackers are genuinely beneficial to the development of technology, the criminal minority, so often in the headlines, now seems to have co-opted the term in the minds of the public.

Malicious hacking itself has gone through an equivalent evolution -- from pranks to isolated, technically adept attacks and now to full-scale organized criminal activities. Yet I believe we have still to see the full emergence of the new face of malicious hacking.

The new hackers will be highly organized and will continue to utilize emerging technologies such as cloud, perhaps even ahead of legitimate uses, to enhance their capability to perform attacks.

However, there is hope that the threats from such hackers can be at least reduced. With the change to highly distributed models of computing there comes an opportunity to rewrite the rules for security of systems and data.

The upheaval of the IT landscape, which we are just beginning to see, can be used to change the playing field to our advantage and will not necessarily only serve to benefit attackers -- if we can act quickly enough and in a sufficiently collaborative way.

Sharing information about attacks, greater openness about the way in which cloud systems are implemented, and a willingness to invest in improving security will pay greater dividends now as the change to cloud is occurring, rather than waiting until it is too late - before the hackers once again set the terms of the engagement in their favor.

Chris Burchett is an expert in both embedded firmware and enterprise software, and is the author of numerous patents. Since co-founding Credant (www.credant.com) in 2001 he has been the driving force behind the technical direction of the their product line. Burchett currently leads the development effort and product management team.

Review: [hiddn] Crypto Adapter

by Mark Woodstone

Over the years, I reviewed a number of secure USB devices that provide on-board encryption, offering an easy and secure way to migrate data. Crypto Adapter is a step up from this usual concept and offers its users a higher class of authentication combined with the possibility of transforming any USB drive into a secure one.

Patented by Norwegian company High Density Devices, [hiddn] is a top of the line, full disk encryption technology whose features include the possibility of setting key lifetime, read-only/write only keys, up to 32 different AES 256 bits encryption keys per user, a custom Master Boot Record, forensic capabilities and split key functionality.

[hiddn] is the basis of the company's product line that ranges from this type of a standalone device to laptop, desktop and even a SATA computer bus interface.

This article is based on the Crypto Adapter SOHO version, i.e. two devices that are paired to work as a "team".

The scenario I mostly practiced with this setup is using one device in my work environment and leaving one at home.

Crypto Adapter is a PIN-based input device that comes with an additional authentication factor - a smart card. Encryption keys are stored on the smart card you receive and each card has its own unique six-number PIN.

Crypto Adapter connects to your computer via an USB port. On the top of the device is an USB slot where you insert your portable media. When doing this for the first time, have in mind that the content of the drive will be completely erased since the drive needs a fresh start for the encryption.

When you insert your smart card and enter the right PIN code, the computer will mount the USB drive and you can use it as any typical USB drive.

Crypto Adapter is all about hardware encryption and I liked the fact that no software application has to be installed on the computer. The device also doesn't need the user to have administrative privileges.

The system is optimal for data migration between office and home

As no application is needed, Crypto Adapter is platform-independent and can be used on multiple operating systems - I used it on various Windows and Mac OS X computers.

The purpose of the second adapter in this paired variation of Crypto Adapter setup is to provide the user easy mobility for the encrypted data.

As the devices are paired, you can use both sets of smart cards to encrypt/decrypt your data on both hardware devices.

The system is optimal for data migration between office and home, but because of its extremely high security standards, I don't see why it cannot be used for other purposes.

For example, I carried it with me on a couple of business trips. It weighs only around a quarter of a pound (120 g, to be precise) and its width is that of two credit cards placed vertically one next to another - a size that can easily fit in a pocket of my bag.

The [hiddn] Crypto Module – the hardware encryption module that is the core of Crypto Adapter - is both FIPS 140-2 Level 3 and Common Criteria EAL4+ certified. According to the "Systems description" manual, the system has also passed NSA's extended vulnerability analysis.

Besides being a perfectly transparent encryption solution for mobile workers, Crypto Adapters is also a great fit for the corporate environment.

The company offers enterprise versions of the product containing five or ten matched units.

As Crypto Adapter doesn't require any management resources, deployment in enterprises is easy and effective.

For more complex deployments, the company provides an optional key management system application that gives IT or security administrators a way to manage lifecycle functions of [hiddn] products within the organization.

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

SANS London 2011

December 3–12

The Most Trusted Name in

http://www.sans.org/london-2011/

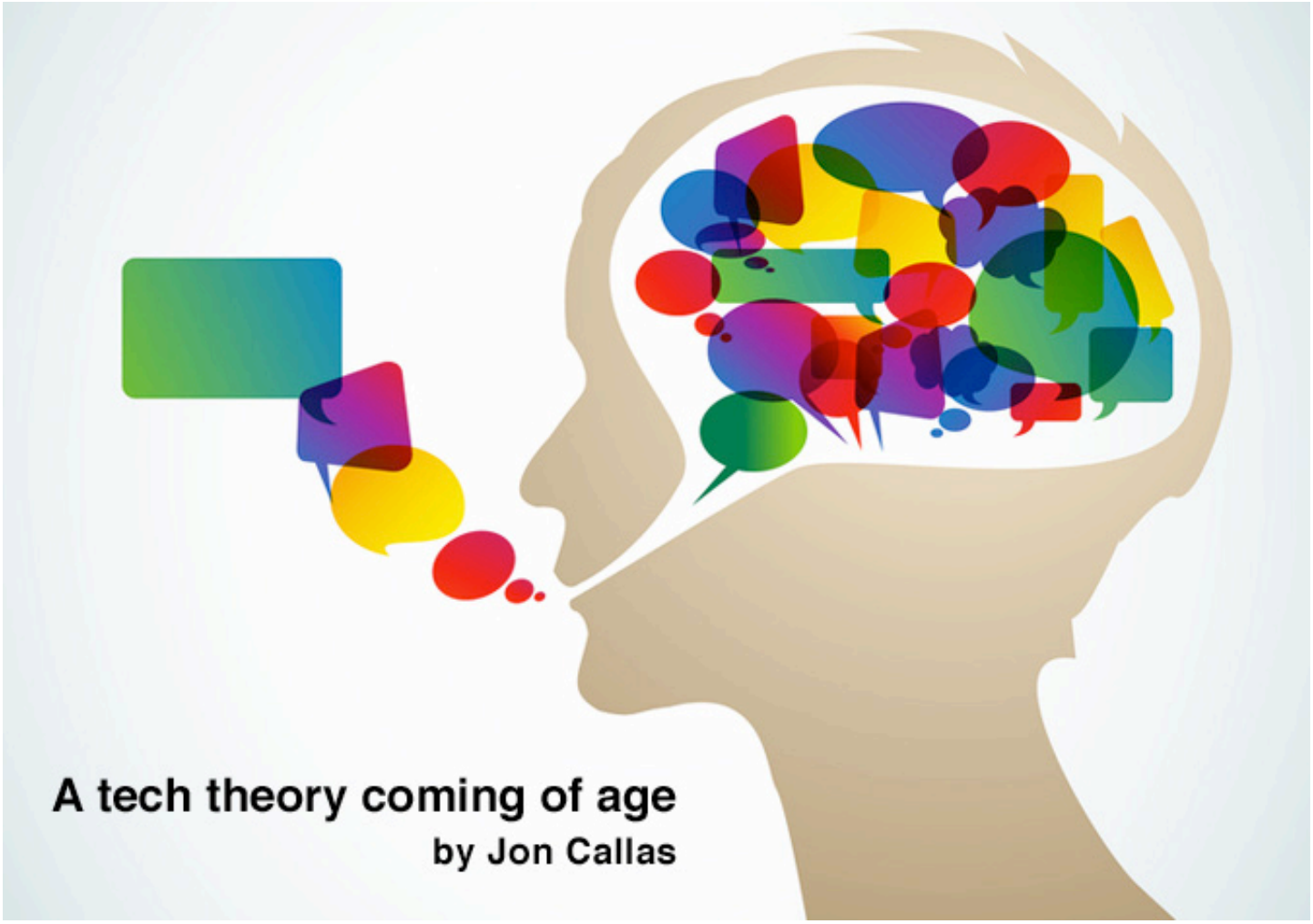
The SANS London Experience

Be Part of It!

- 16 OF THE WORLD'S BEST INFOSEC TRAINING COURSES
- EXPERT TALKS
- VENDOR EVENTS
- COMMUNITY NIGHTS
- NETWORKING OPPORTUNITIES

... AND MORE!

GIAC Approved Training



As early as 2005, many industry analysts predicted "consumerization" - the introduction of consumer-owned/purchased devices into enterprise and business environments - would become one of the most important technology trends through the next 10 years (Gartner 2005).

Six years later, the prediction has proven true. Employees now rely on personal smartphones, tablets or other mobile devices to send or receive corporate email, exchange sensitive information and intellectual property, and even access enterprise networks and applications.

Earlier this year, Gartner also surveyed today's CIO to gain perspective on consumerization in the enterprise. Gartner vice president Nick Jones' report, "CIO Attitudes towards Consumerization of Mobile Devices and Applications," shows that U.S.-based respondents believe that in two years, approximately 38 percent of their employees will be using employee-purchased mobile devices in the enterprise.

This technology migration introduces several IT security challenges, including identity access management (IAM) obstacles, mobile security and authentication requirements, compliance enforcement and general security policy. In fact, a late 2010 Morgan Stanley report, "Ten Questions Internet Execs Should Ask & Answer," states the market will hit an inflection point in 2012 where, conservatively, shipments of mobile devices and smartphones will surpass those of PCs. Understanding this shift, technology vendors like Dell, Apple, HP and Microsoft are heavily investing in the mobile consumer space.

Explosive growth: Mobile devices take over

Any number of logical reasons serve as catalysts for the growth of mobile device use - price, expansion of Wi-Fi, faster cellular data

speeds, always-on simplicity, or the ease of finding, installing and using mobile applications.

And as the mobile market share grows, so too have the challenges around mobility in the enterprise. The technology convergence of work and personal lives is real. But organizations shouldn't shy away from this shift. It's a permanent change in how people live, not a trend or fad.

As enterprise-specific applications are introduced — whether from the organization or third-party developers — efficiency will grow exponentially. In a 2010 Forrester study, "Insights for CIOs: Make Mobility Standard Business Practice," senior advisor Tim Sheedy found that "around 75 percent of organizations deploy mobile applications to increase worker productivity, and 65 percent to increase employee responsiveness."

It's also important, however, to embrace employee lifestyles during the development of new mobile strategies. Not every person will own the same device (e.g., Apple iPhone vs. Android), so broad interoperability will be necessary. The same Sheedy study discovered interesting growth statistics for enterprise environments once dominated by BlackBerry-friendly infrastructure.

While the RIM devices are supported by approximately 70 percent of enterprises in Europe and North America, Forrester released findings in April 2010 (Enterprise and SMB Networks And Telecommunications Survey, North America And Europe, Q1 2010) that shows support for Windows Mobile (41 percent), Apple iOS (29 percent) and Google Android (13 percent) is growing quickly in the corporate realm.

Additional evidence even goes beyond consumerization; 51 percent of enterprises plan to purchase tablets for employees in the next 12 months, according to a February 2011 Morgan Stanley Blue Paper, "Tablet Demand and Disruption Mobile Users Come of Age." This is in addition to another 16 percent of organizations that already allow employees to connect to sensitive networks with their own device.

THE TECHNOLOGY CONVERGENCE OF WORK AND PERSONAL LIVES IS REAL

Lifestyle convergence

Logically, true consumerization began when, in mass, consumers began purchasing mobile devices for personal use. Being affordable, easy to use and always on, the mobile platforms became the centerpiece of consumer lifestyles. And it didn't take long before this reliance shifted to the enterprise space.

Dual-purpose applications became available that further enabled convergence of personal and professional lives.

While five years ago it was mainly voice-only use, mobile device capabilities quickly expanded to email, calendar management, collaboration, business applications, general corporate connectivity and more.

With this growth, more opportunity for risk was introduced.

Mobile platforms at risk

Mobile growth has increased the incidence of fraud targeting mobile devices. Whether simple rogue text messages, fictitious billing scams or more malicious attacks using malware installed on the device, the number of attacks grow at an alarming rate; mobile malware increased by more than 45 percent in 2010. And with less education about mobile threats, users seem more inclined to fall victim to them during mobile sessions.

Further, online-banking users - both consumers and commercial users - continue to be the target of sophisticated attacks. Financial institutions are targeted by advanced malware threats that leave many traditional safeguards ineffective. Instead of phishing attacks that lead to fake websites designed to harvest usernames and passwords, the techniques are now more sophisticated and effective against previously deployed defenses.

Whereas once such attacks were the domain of amateur hackers, sophisticated cybercrime groups have emerged as online fraud leaders, targeting consumer- and commercial-banking users alike.

And while attacks are typically confined to the consumer space, these same consumer devices are gaining access to corporate networks and information. This is where consumerization directly affects the enterprise.

New thinking: Mobile vs. PC

The mobile migration is an intriguing shift for business productivity, but a potential nightmare for IT security and identity access management (IAM) - the processes and tools to manage user access to networks, applications and data.

To deploy the correct safeguards, organizations must prioritize areas of concern that are a hindrance to proper mobile convergence in the enterprise.

Risk
The general risk around consumerization is straightforward. As was seen with laptops issued by employers years ago, end-users will predictably fall into a pattern of common behavior that includes storing sensitive information on mobile devices; sharing passwords across devices, applications and networks; unknowingly introducing viruses to the enterprise environment; and potentially performing activities that expose employers to non-compliance.

Cost & Complexity
But risk isn't the only factor in play. Complexity and cost of new identity management systems remain top of mind for CISOs and IT directors. Gone are the days managing one identity for each employee or end-user. For true mobile convergence, organizations require infrastructure that provides diverse user and device identities, as well as complex mobile device management capabilities.

Lack of Control
The other major obstacle is based around control; or, more accurately, the lack of it. With desktops and laptops, IT staff could combat everyday challenges with antivirus solutions, device/file encryption, password policy enforcement, content-monitoring or even remote-swiping technology.

Even if some of these capabilities are available for mobile platforms - chances are they are not - they aren't proven in enterprise environments. And it's currently unknown which channels or methods sophisticated criminal groups will leverage next to attack corporations through employee-owned mobile devices. Until there is better visibility regarding mobile platform controls, this will remain an area of concern for most organizations.

An evolving enterprise architecture

As more services move to the cloud, more tasks will be executed via mobile devices. Whether in governments, enterprises or customer-focused organizations, the popularity of mobile devices will serve as a catalyst to cloud-based services and vice versa.

The adoption of cloud-based technology has been staggered. Enterprises were first to embrace the idea via hosted or software-as-a-service (SaaS) models. Government agencies, on the other hand, were more hesitant because of their responsibility to protect private or sensitive information. As security for mobile devices and the cloud improves, more governments are able to consolidate services with cloud-based infrastructure to take advantage of efficiencies and cost-savings.

As consumerization continues, the cloud remains one of the most effective solutions to support mobile services and applications; pressure exists on both ends of the technology spectrum. And as organizations seek methods to reduce costs and streamline operations, mobile- and cloud-based capabilities are capable or realizing those goals.

According to a recent Gartner webinar by vice president Nick Jones, "The Trends Driving Your Mobile Strategy Now Through 2015," consumerization will be a central theme in 2012. The session states end-users will gravitate toward multiple devices and platforms, and will synchronize information with cloud-based servers and services. Further, Jones says, "consumerization always wins and 'enterprise' devices are a declining category."

The nature of the server-based technology begs the question: does it even make sense to have centralized IT infrastructure?

A secure resolution

With the ubiquity of mobile devices established, what are the answers to solving the aforementioned challenges? And how can mobile devices themselves be used to actually increase enterprise security?

In short, organizations should layer security techniques and capabilities. Ideally, this approach is already the basis for general identity-based security within the enterprise, but it's equally valid for the mobile space.

Core to this theory is the use of a versatile authentication platform. This approach authenticates all identities - whether human, software or machine - within a government, enterprise or consumer space. Specific methods and technology are available that help secure the mobile platform, as well as transform the mobile device itself into a layer of the security architecture. The end goal is to secure every possible attack point to help reduce the vulnerability - whether perceived or realized - of mobile platforms.

Increasingly, organizations understand mobile devices are an important component to end-user lifestyles. Many carry their mobile device at all times, making it a prime candidate to serve as an identity credential. This behavior dictates that smartphones or mobile devices will increase end-user adoption because they're rarely "forgotten at home."

In fact, mobile devices are able provide even more security than what is available on the market today. As the market matures, and organizations adopt mobile as a credential, we will likely see many uses for mobile devices.

MOBILE DEVICES ARE ABLE PROVIDE EVEN MORE SECURITY THAN WHAT IS AVAILABLE ON THE MARKET TODAY

Mobile authentication

Transparent soft token

An authentication software module is embedded within the mobile application. End-users will only enter usernames and passwords into application fields. The mobile application automatically accesses the custom authentication module to generate a one-time-passcode (OTP) token in the background. The OTP token, along with the unique user ID, is transparently sent to the secure server. This all occurs in real-time with little user input.

Digital certificates

Leveraged more in the enterprise, digital certificates identify and secure a multitude of transactions, identities or communication. They enable trusted device authentication for access to corporate applications, VPNs, servers and more.

Mobile as a credential

Mobile smartcard reader

This is a mode of operation where a mobile device is used to read smartcards. For example, an employee can use a mobile device to read a smartcard, then use out-of-band authentication to gain access to a laptop/desktop or even verify a transaction. It also has practical applications for online-banking customers. In all examples, a smartphone equipped with RFID-reading capabilities, and possibly dedicated software, is required.

Mobile device as a smartcard

Similar to the mobile credential, this is a mode of operation where a mobile device is the credential, replacing the need for a physical smartcard. In the enterprise, end-users can bring their mobile device near a desktop or laptop for secure authentication. This is achieved via wireless, proximity-based transmission technology such as Bluetooth and/or near field communication (NFC).

Transaction verification

Basic transaction approval

Real-time transaction verification - right on a user's mobile device - is one of the most advanced methods of stopping malware and online fraud. This is particularly useful for enterprises and financial institutions as organized

crime groups target larger business transactions and ACH transfers.

Account and access control changes
A business-specific capability, employees can securely verify account or identity-related changes. This can include everything from simple account updates or password changes, to more advanced uses such as confirming logins for specific behavior patterns (e.g., employee logs in from location not within their profile).

Mobile enterprise workflow
The technology may be extended to increase employee productivity on mobile devices. No longer will enterprises be forced to sacrifice security for the sake of mobile convenience. Mobile verification can be tailored to confirm enterprise-specific tasks or transactions (e.g., expense approval).

Future technology

In the near term, existing technology such as Bluetooth and near field communication (NFC) will be extended to provide advanced mobile device authentication that's even simpler for the end-user. As mentioned, capable devices will securely authenticate the user via proximity.

Mobile devices will continue to disrupt incumbent technologies. One technology that stands a great chance of disruption is payments - the replacement of credit cards with a mobile device that will act as a wallet (e.g., Google Wallet).

Many industry experts believe that NFC will be a cornerstone of payments.

Beyond mobile payments, another application of NFC is the ability to securely authenticate a user/device via proximity.

Many organizations today are experimenting with the capabilities of NFC and constructing proof-of-concept models in anticipation of this technology becoming ubiquitous.

EXISTING TECHNOLOGY SUCH AS BLUETOOTH AND NEAR FIELD COMMUNICATION WILL BE EXTENDED TO PROVIDE ADVANCED MOBILE DEVICE AUTHENTICATION THAT'S EVEN SIMPLER FOR THE END-USER

Mobile devices: Here to stay

The growing use of mobile devices - and more importantly an aggressive digital lifestyle convergence - demonstrates the need for organizations to implement mobile strategies into current and future security and/or IAM roadmaps.

Ideally, organizations are at crossroads where general security and mobile IT operations can be merged to be managed under a single versatile authentication platform. This approach will streamline the management of identities and devices that access an enterprise's environment.

And it's important to foster, rather than discourage, the convergence of employee work and personal lifestyle that's achieved via mobile devices. This will help organizations better leverage the benefits of mobility and increase adoption of security policy - a strategic play that's core to securely capitalizing on consumerization.

Jon Callas is the CTO at Entrust (www.entrust.com). Callas co-founded PGP Corporation, which specializes in email and data encryption software. Over the course of more than 15 years, Callas held PGP leadership functions including CTO and CSO. Prior to Entrust, he also served as an operating system security expert with Apple. Callas has authored several Internet Engineering Task Force (IETF) standards including OpenPGP, DKIM and ZRTP.

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:

@mattcutts
Matt Cutts - Head of the webspam team at Google.
http://twitter.com/mattcutts

@TimelessP
Timeless Prototype - Security Analyst.
http://twitter.com/TimelessP

@WeldPond
Chris Wysopal - Veracode CTO and co-founder.
http://twitter.com/weldpond

@0xcharlie
Charlie Miller - Accuvant LABS principal research consultant.
http://twitter.com/0xcharlie

SecurityByte 2011: Cyber conflicts, cloud computing and printer hacking

by Berislav Kucan

SecurityByte 2011 is India's largest security conference. The event featured over 30 talks with 3 parallel tracks, challenging War games and thought-provoking panel discussions.

Located twenty kilometers south of the city of Bangalore, Electronic City is the Indian version of Silicon Valley. Ever since the first phase of the project was finalized, the area has specialized in attracting technology companies.

In the early 1990s, P.V. Narasimha Rao (the Indian Prime Minister at the time) started working on the liberalization of the Indian economy and soon - as a result of a successful combination of great ideas and a vision - this part of the Karnataka state became THE place for global technology outsourcing.

While flying here to Bangalore, I read a book that identified Texas Instruments as the first tech company that opened its offices in this area. Nowadays, while driving around Electronic City you will see big buildings with familiar names such as HP, Siemens, 3M and, of course, some of the India's own mega-companies like Wipro and Infosys. These organizations provide jobs, but it is also important to note that the area hosts a large number of educational institutions, mainly specializing in economics, engineering and IT.

After the inaugural event in New Delhi, held in November 2009, the SecurityByte team is back with this year's edition of the conference. The move to Bangalore was strategic and definitely makes sense - there is no better place for hosting an information security conference than the IT capital of India. The event was planned to be held at the Sheraton hotel in center of Bangalore, but a couple of months ago a definitive decision was made to host it in the Electronic City's deluxe Crowne Plaza.

This year's conference is organized in three parallel tracks - technical, management and developer - but if you ask me, for an audience of around 600 individuals, that is one track too many.

The event started with a series of keynotes by influential people in information security,

as well as those in the local government.

Dr. Whitfield Diffie, one of the icons of the industry who now serves as VP for Information Security at ICANN and Scientific Advisor to Uniken (one of the event sponsors - a global technology solutions provider with innovation center in Pune, India), addressed the public first.

He talked about the importance of the invention of the radio back in the day and how the addition of cryptography had a huge impact on its usage, and compared that with cloud computing and the absolute need for new encryption mechanisms for it. He believes that cloud computing is as revolutionary as the radio was a hundred years ago.

Everybody welcomed the networking opportunities during breaks.

As controversial as it might initially sound, Dr. Diffie also explained that he does not share the opinion of one of his colleagues who said that if he had the chance to go back in time and build the Internet from scratch, he would integrate strong authentication mechanisms in it.

"The incredible, commercial and cultural force that is the Internet is something that would not come about without the free communication that the lack of authentication produces," he said, and added that he strongly believes that authentication mechanisms would have killed the Internet.

The second keynote speaker was Edward Schwartz, RSA's CSO who was hired after the breach. He shared his opinion that we cannot protect everything and that in a number of daily information security programs there are a lot of aspects that are mostly waste of time.

He also noted that there are three winning strategies we should employ:

• Information centricity (understanding what really matters to us versus the broad view; knowing what is useful for the information assurance process and making that operational).

Edward Schwartz, VP and Divisional CISO, RSA.

• Risk focus (developing adversary-based threat model).

• Agility (certain aspects of security principles should be built-in from scratch).

The first day keynotes were closed by speeches by His Excellency Shri HR Bhardwaj, The Governor of Karnataka and Shri S. Prabhu, Principal Account General of Karnataka. They applauded SecurityByte's move to India and stressed out the importance of positioning Bangalore as a center of IT and security research, as well as pointing out the need for a nodal agency that would deal with cyber security.

According to Mr. Prabhu, SecurityByte is a perfect example of a public/private partnership and that the level of research and knowledge that will be shown at the event should be continued in Bangalore on a more permanent level.

After the keynotes, I attended a couple of talks. Two of the most interesting ones were "Implementing a Joint Computer Emergency Response Team (J-CERT)" by John Bumgarner, Chief Technology Officer of the U.S. Cyber Consequences Unit, and "From Printer to Owned: Leveraging Multifunction Printers During Penetration Testing", held by senior security engineer Deral Heiland who already exhibited variations of this presentation to fully packed rooms at ShmooCon and Defcon.

Mr. Bumgarner is a person with immense experience in intelligence and information security and his speech was an interesting take on the current status of global intra-CERT relations as told through the perspective of cyber conflicts and the events such as the Georgian cyber war.

The conclusion is that joint CERTs are a way to go, but prior to this there is a need for establishing international standards.

Deral Heiland's talk on hacking printers is a reality check that shows how easy you can wreak damage with multi-functional printers in corporate environments.

The majority of printers connected to local networks - and some of them connected to the Internet - contain some type of a vulnerability.

His Excellency Shri HR Bhardwaj, The Governor of Karnataka.

If you ask yourself how can a printer endanger your network, just think about some of the usual functions in these type of devices - scanning to files, saving copies locally, LDAP connectivity, sending over email and so on.

All of these functions can produce some type of data that can either generate information disclosure or become the first phase of a successful full network compromise.

The practical examples he talked about showed that the current status of security of these devices makes it seem like we are back in the mid 1990s.

Berislav Kucan is the Marketing Director of (IN)SECURE Magazine and Help Net Security.

RSA CONFERENCE EUROPE 2011

11 -13 OCTOBER | HILTON LONDON METROPOLE | U.K.

Could your organisation hit the headlines for all the wrong reasons?

With information security threats becoming more targeted and sophisticated, how can you and your organisation stay on top of the situation and out of the news?

Find out at RSA® Conference Europe 2011 - the place for Europe's smartest information security professionals who want to discover the latest trends, technologies and threats affecting the industry. Benefit from:

- 70 educational track sessions
- Keynotes from industry thought leaders
- Interactive programmes
- Demonstrations from leading vendors
- Time to meet and collaborate with peers

Dates: 11th – 13th October
Venue: Hilton London Metropole Hotel, U.K.

Be educated. Be informed. Register now.

www.rsaconference.com/2011/europe

the adventures of alice & bob

The need for foundational controls in cloud computing

by Harold Moss

Cloud computing is enjoying tremendous growth. But like any nascent technology, it is not without its challenges. In fact, many consumers of cloud computing state that security remains a significant inhibitor to widespread adoption despite the fact they are already in the cloud. However, the cloud has the promise to be more secure than traditional enterprises, especially when designed to meet unique industry demands and regulations.

Ultimately, many of us are already accessing services in the cloud as individuals, if not on a larger scale as organizations. We may leverage a web-based set of sales tools, connect to our company via our mobile device or get our email from the web - all these things are delivered via the cloud.

When we look at how cloud has permeated our lives, the security question goes beyond whether the cloud provider has the right level of confidence required. Organizations now need to consider the best way to leverage the cloud in a secure manner.

More importantly, companies need to ask how they can adopt cloud technology given the probability that they will likely have multiple instances of clouds in an organization. In response to the last challenge, I often recommend to clients to assess their foundational controls over cloud security.

Although foundational controls sounds like a cool new phrase, it's really a structure that provides a framework for applying an organization's unique security needs and considerations to cloud computing.

Foundational controls are the subset of controls that capture the security culture of the organization, and provide the basis for how the organization implements security and applies that security to both its internal and external obligations. Once established, these controls can be leveraged to span the multiple instances of cloud and at the same time communicate what is important to the organization and why in as simple a form as possible.

After all, one of the biggest challenges in developing the right security approach is not necessarily addressing one specific threat but in the understanding and application of the right security approach.

So what exactly are foundational controls? Simply put, they are high-level security categories that represent the organization culture. Overall, an organization rarely exceeds 70 or so controls, and rarely has less than 20 controls over security. They are something everyone in the company should be able to communicate and understand. In fact, they often appear throughout the organization's day to day operations.

This leads to the question of how organizations should benefit from foundational controls in the real world. Ultimately, foundational controls form a basis for cloud adoption. Let's assume an organization has decided to purchase expensive software-as-a-service offering from a vendor. The organization would first assess the foundational controls to provide a guideline for attributes that the customer must have in each cloud instance. In this case, maybe the vendor has a different password policy - for example, it requires six characters, but the foundational controls dictate that an organization needs at least eight.

Clearly, that vendor does not align with the organization's culture, so they might decide not to engage with them. At the same time, the next vendor has a minimum password length of nine. One might assume that makes it more secure, but in reality that may not be the case. The fact that the vendor and client policies don't correlate means that it's not possible for employees to have consistency. If we were to expand that example to five or 10 clouds - all with different policies and rules - employees would then be attempting to manage multiple discreet passwords.

ONE OF THE BIGGEST CHALLENGES IN DEVELOPING THE RIGHT SECURITY APPROACH IS NOT NECESSARILY ADDRESSING ONE SPECIFIC THREAT BUT IN THE UNDERSTANDING AND APPLICATION OF THE RIGHT SECURITY APPROACH

In the above example, it can be seen how foundational controls might shape an engagement. Let's consider one more scenario, which is occurring every day for consumers of the cloud. An organization could decide to use collaborative software as a service cloud to reduce collaboration costs. The CIO or IT professional is aware that his or her organization has specific regulatory requirements it must adhere to, but is unclear what needs to be captured or how interfaces occur.

Fortunately he has a foundational control assessment, which describes how clouds are governed, and can leverage this information to ensure that interfaces and/or reports exist that enable the company's auditors to evaluate the cloud.

So where does an organization start when identifying foundational controls? The best place to begin when building a list of foundational controls is to look at the existing governance models for your organization. Most of the key controls for operation in organizations have a security slant. For example, an organization may have a key control over operations for Sarbanes-Oxley compliance, which states that only authorized personnel have access to your company's chart of accounts. The IT professional doesn't need to actually know what a chart of accounts means, but what he does need to know is that the company believes in limited access to some types of information.

As the IT professional looks across the company's business controls, he will probably notice that the phrase "only authorized persons" appears quite a bit. This indicates that from a foundational level, the company values privilege access to certain data or applications. It's really quite simple, in fact the company's lead IT executive or security executive already knows what the foundational controls are; they just need to be documented in the cloud security plan.

As those controls are documented, it helps to categorize them into key areas that simplify understanding. At IBM, we have identified eight key areas for organizing foundational controls:

Access and identity - In this area we include all foundational concepts relative to how access and identity should be applied across all cloud engagements. This can sometimes result in improvements as to how access and identity is currently managed, as it requires a retrospective look at how we address who has access, and who really should have access to information.

Data protection - This category really focuses on understanding that certain classes of data have different needs, and the ways the organization approaches those needs. When one looks at cloud security, the notion of protecting only what's inside a building's walls becomes limited. Instead, the focus is on identifying data and figuring out how it can be protected at a granular level. Also, organizations might ask if they really have the right levels of protection for the information in their cloud.

Release management - Organizations often leap to the cloud without thinking about the consequences associated with moving beyond the confines of their traditional environments. Release management sets guidelines for how information and solutions migrate to the cloud, especially in terms of complex systems that have interdependencies, which might result in failures or increase vulnerabilities.

Security event and vulnerability management - This category deals with setting guidelines for what should be monitored in the cloud and how - a key challenge for those moving to the cloud. This is combined with specifying how patches are managed and applied, which can help reduce the cloud threat landscape dramatically.

Physical security - Identifying key physical security requirements relative to who has access and what redundancy exists can enable an organization to survive major catastrophic events.

Problem management - The problem management controls subset provides clarity as to how to address issues and who really needs to be aware of events. By documenting key resources for events, organizations can more rapidly respond to events and mitigate damages and/or vulnerabilities.

Governance and compliance - Auditing remains a key challenge to cloud adoption. Often there are explicit needs for audit and compliance identified by the organization, and failure to consider the challenges the cloud brings can create immense challenges for organizations. More important is creating a structure that enables active monitoring of cloud technologies, which is key to successful utilization of cloud technologies.

Change and configuration management - The cloud is by its very nature dynamic. As a result, the evolution and life cycle of cloud implementations make it prone to the inadvertent introduction of vulnerabilities. This also offers a fertile ground for the introduction of malicious code as elements are reverting through their various life cycles. Having controls that help the organization manage cloud instances reduces the probability that such vulnerabilities will be exposed in the cloud.

Foundational controls help to navigate the critical details that shape an organization's future experience with the cloud. By leveraging this critical tool in cloud efforts, an IT professional can more easily select a vendor which will work best with the organization and not require special security bridges, which reduce the value proposition of the cloud for the organization. Foundational controls also help to build continuity between cloud initiatives by removing the skills and resource challenges associated with managing multiple cloud instances. While foundational controls are not an end-all solution to a company's cloud needs, they do represent the first step in the journey to secure cloud computing.

Harold Moss is the CTO Cloud Computing Strategy, IBM (www.ibm.com).

Data classification: A new approach to data centric security

by Michael S. Oberlaender

The security of data is defined through the following three parameters:

• Availability
• Integrity
• Confidentiality.

Classification is the approach to standardize or categorize something according to specified classes in order to sort out special attributes or subjects from a group of assets. Commonly, data has been – if at all – classified only by its confidentiality (sensitivity) requirements.

This has often led people to focus mainly on access control, and to a lot of money being spent on additional assessment rounds focusing on availability and integrity control.

Thesis

1. Data has to be independently classified based on availability, integrity and confidentiality.

2. Classification needs to be data-centric, not focusing on the systems or databases (those will be addressed after the classification is done), and to be stored within the data itself. This way, the data keeps these attributes while it "travels" through the infrastructure and doesn't rely on source systems. It will, therefore, allow decentralized filters or decision controls of what needs to be done with this data.

3. Finally, to allow for an easy to understand data and control markup, I introduce the Oberlaender-(C^3) cube. It will also help to follow the necessary (and to be defined) practices and mechanisms to safeguard such data that is available in printed (document) form. On one hand, this approach serves for the secure control of the data flow(s), on the other hand it supports a pragmatic organizational implementation of data security measures.

Data owner

As a matter of principle, it will be defined that all data will get assigned an owner (in the sense of an administrator), whose duty is to classify the data according to a data classification table. From a legal (property-rights) perspective, the data of cause is and will remain

the property of the company or owner. The herein described data owner (or trustee) (in analogy to the Bell-LaPadula model - tinyurl.com/68uhkoz) is the person responsible for the correct allocation of the data into one of the classes provided in the next paragraph. This same person also serves as "administrator" for any possibly upcoming reclassifications.

Fundamentally, the person who creates the data for the first time becomes the data owner in the above sense. In cases where data is created by an automated process, the process owner (who created/designed the process) is the formal data owner. This role can later be transferred to another person, but as a result of that it may never become "empty" ("void" or unassigned to a real existing person). For existing data, appropriate terms will be defined in which the data will be assigned (to the owner) and afterwards be classified.

The objective of this approach is that, in the long run, all data will be classified accordingly to achieve an economic and relevant secure handling and custody of this data. Upon the leave or change of an employee, the role of the data owner will be assigned to the respective manager until the role is assigned to another real person. This may happen in a recursive way upwards in the organizational structure (ultimately the CEO and the board of directors of the company is data owner in the above sense).

Data classification table

The table below is a reality-based example of how one could define the different levels and related requirements for the three-parameter-approach defined earlier.

The specified damage values need to be adapted to each company or property owner willing to use the presented classification approach. To provide a common ground, I used a percentage value of the IT budget. This will allow for a realistic and value based classification, and is a necessary step for the adopter of the scheme presented in this article.

The below listed classes may exist in all column-combinations (see also further below the C^3) – the columns are (mathematically spoken) "orthogonal" to each other.

Level / Class	Availability	Integrity	Confidentiality
0	Unclassified. ~90% as a guidance level. Recoverability not guaranteed.	Unclassified. Integrity not guaranteed.	Unclassified. Confidentiality not guaranteed.
1	Offline Backup, one-time storage (de-duplication acceptable), 99% <= 0.5 week recovery time objective. The loss of the availability of this kind of data for several days is uncritical, but must be possible nevertheless. The maximum possible damage is <= 0.01% of IT budget. Ex.: archived historic data, older emails (older than a year), old annual reports (>3 years).	CRC or similar check sums. The loss of the integrity of this kind of data calls for a limited work effort, but is negligible. The maximum possible damage is <= 0.01% of IT budget. If the error will be recognized depends on the user's discretion and is not critical for the organization. Ex.: standard documents, simple architectural plans, telephone lists, internal emails, project plans, price information.	Un-restricted. This kind of data doesn't need to be encrypted. Information, which may become public without risk for the parties involved at the time of the classification. The maximum possible damage is <= 0.01% of IT budget. Ex.: year end (annual) reports, public website content.

Level / Class	Availability	Integrity	Confidentiality
2	Online backup. 99.9% <= 1 day recovery time objective. The loss of availability of this kind of data for a maximum of 1 day is uncritical, but needs to be possible during this time period. It doesn't create a directly measurable damage, but with further delay an image damage might occur, or a maximum possible damage <= 0.1% of IT budget. Ex.: normal documents, emails (newer than one year), actual price information, product charts, brochures, telephone lists.	HASH MD-5 / SHA-1 without time-stamp. The loss of the integrity of this kind of data entails a heightened work effort for the re-creation of the data, or leads to a direct loss. Maximum possible damage <= 0.1% of IT budget. It is necessary that the error is recognized, therefore a hash is being required. Unintended change to the data by third parties should be barred. Ex.: product information, network / infrastructure plans.	Internal. Information which is only to be seen by the persons directly involved in the case at hand. Therefore, this data needs to be symmetrically encrypted, and the used key is only to be made available to the intended group of persons. Maximum possible damage <= 0.1% of IT budget. Ex.: architectural plans, telephone lists, internal emails, project plans, price information.
3	Highly available. 99.99% <= 1 hour recovery time objective. The loss of availability of this kind of data is critical. It generates a directly measurable damage or image damage <= 1% of IT budget. Ex.: public web site content, annual report at the time of publication, information to crisis management (call trees).	HASH SHA-256 without time stamp but with digital signature. The loss of integrity of this kind of data entails a high work effort for the re-creation of the data, or leads to a directly loss. Maximum possible damage <= 1% of IT budget. It is necessary that the error is recognized. Therefore, a secure hash algorithm is required. The unauthorized change to the data by third parties must be securely excluded for a long period of time. In addition, it is necessary that the source of the data can be definitely attributed to a specific person or organization. Ex.: personal data, annual report before the actual authorized publication.	Confidential. Information for which the publication to unauthorized individuals or the public has a maximum possible damage <= 1% of IT budget. Therefore, this kind of data has to be asymmetrically encrypted, and the used personalized keys are only to be handed to the respective, authorized individuals (use of a PKI is recommended). Ex.: Personal data, annual report before the actual authorized publication.

Level / Class	Availability	Integrity	Confidentiality
4	Highly available, multiple redundant (hot site), <= 1 minute recovery time objective. The loss of the availability of this kind of data is business critical and has a direct impact to the business (balance sheet). A direct measurable damage or image damage of > 1% of IT budget is generated. Ex.: breakdown of the business process(es).	HASH SHA-256 with time stamp and qualified digital signature. The loss of integrity of this kind of data entails a high work effort for the re-creation or leads to a direct loss, maximum damage > 1% of IT budget. It is necessary that the error is recognized; therefore a secure hash algorithm is required. The unauthorized change to the data by third parties must be securely excluded for a long period of time. In addition, it is necessary that the source of the data can be distinctly attributed to a specific person or organization. Also, that the exact point in time of the data creation (e.g. publication) is definitely and verifiably possible. Ex.: particular personal data, annual reports at the time of publication, tender competitions.	Strictly confidential. Information, of which the loss or the publication to unauthorized individuals or the public can create a maximum damage > 1% of IT budget. The emergence of this kind of data can create long term image damage. Therefore this data needs to be asymmetrically encrypted, and the used personalized keys are only to be handed to the respective authorized persons (usage of a PKI necessary). Ex.: particular personal data (sex, race, religion etc.), business plans (M&A, initial public offerings / listings), marketing plans, strategy documents.

Figure 1: Classification table.

The above data classification table serves as an example of how data could be classified based on the descriptive terms and values in each respective column.

The classification and compliance cube (C^3)

Not all data needs always the same level of security in regards to availability, integrity and confidentiality.

Instead, it can occur in all possible variations of these three parameters, and it is helpful to remember the data space cubicle illustrated on the following page.

Here, the black marked single cube stands for the completely unclassified data. The red one depicts data that is very available, but has not undergone a classification for integrity and confidentiality.

The green single cube stands for data with very high integrity needs, but without a rating for availability or confidentiality. The yellow single cube depicts data that needs to be particularly available and requires high integrity, but has no classification requirements for confidentiality.

Finally, the white single cube represents data that has the highest requirements for all three parameters.

The chosen color selection seems discretionary at the first glance, but is, in fact, very well intended. It is based on the RGB color model (used in electronics and IT), and shall clarify, where the to-the-organization-critical data resides (white).

To bring the notation sequence (availability, integrity, confidentiality) in line with the RGB color model, the assignment of the color red to availability, green to integrity and blue to confidentiality has been performed.

Therefore due to the 5 levels (0-4) and the RGB approach with 255 as a maximum value per parameter, one has to add 64 each time for the color value per level, to assign each cube the correct color code.

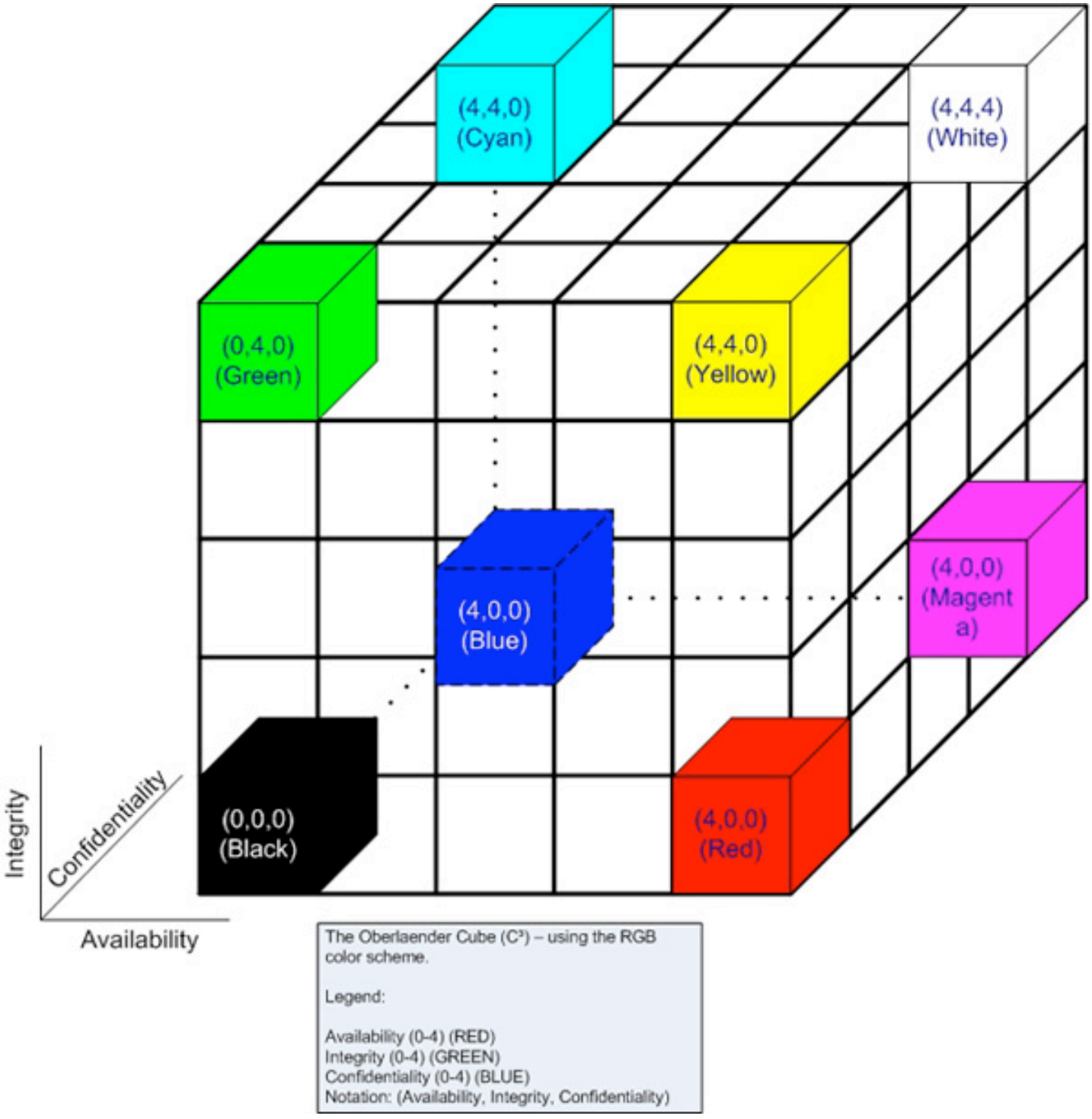


Figure 2: The Oberlaender Cube (C³).

Example: The cube in the middle of the top C3 level with the coordinates (2,4,2) receives the color: (2*64, 4*64, 2*64), respectively:

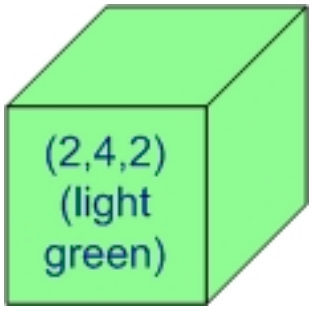


Figure 3: The 2,4,2 - Cube.

At this time, we have understood that the cubicle color scheme is a 3-D-representation of the availability, integrity and confidentiality assignments one can perform.

Color distribution

For the overall color distribution of the data within the C³ applies that, depending on industry, company philosophy, and history, most of the data will be "black", meaning it has no particular requirements to A, I and C.

For instance, banks and insurances will put relatively high requirements to all three parameters, as false (such as a couple of zeros too much) or unavailable (online banking), but also unintended publicized actual confidential data (such as account balance and account change information) can become very costly very fast.

In the producing industry in average, medium requirements in regards to the three parameters (A,I,C) will be imposed to the affected data. And there is still again special information that has the highest requirements to confidentiality (coke formula) and also integrity (mixing ratios in the chemical industry).

As an opposite, the retail sector will have the most (but not all) data which is not confidential, and also their requirements in regards to integrity and availability – in comparison with the above industry sectors– will be far less.

Now that the data gets classified appropriately, one can achieve a clearly apparent classification by either an appropriate color imprint for paper documents (the RGB model is very easy to implement for all IT systems or is already implemented almost everywhere) or also by a naming convention (such as „2_4_2_filename_version123_YYYYMMDD“) for electronic documents (in addition to the color marking in the page header or footer). To hinder unwanted manipulation by third parties, one could also list the classification (like 2_4_2) in the page headers or footers, create a hash (SHA-256) for the file, and store/save and transfer this hash separately of the file. Public domain software and tools at no charge such as GNU PGP deliver a good service in that regard.

Complementary, attention is invited to the already existing security models of Bell-Lapadula, Biba, Clark-Wilson, Brewer-Nash, Graham-Denning, Harrison-Ruzzo-Ullman, and Take-Grant (to start, look at: en.wikipedia.org/wiki/Computer_security_model).

One could now conclude to depict the confidentiality axis via Bell-LaPadula and the integrity axis via Biba respectively Clark-Wilson. However, these models also fall back to the trustee (respectively trusted subject, owner, transformation procedures) model, to perform the assignment or re-allocation of data into the correct class(es). Also, the availability axis would not be normalized by such a model, and therefore the author is following a different approach, namely the "enablement" of the "data owner".

This role is the linchpin for the whole classification, and shall be commissioned accordingly for all three dimensions, to perform the correct allocation in the classification (and also

the re-classification). The incurred costs are to be accounted for by this data owner. Thus the necessity to identify a "business owner", who is able to allocate these costs to a cost center, is obvious.

The above represented color model provides for a clear overview, which kind of data is more expensive (the more “white” the data is, the more effort is necessary to secure it): (4,4,4) – data (marked white) is much more expensive than unclassified (0,0,0)-data (marked black) or low classified data such as (1,1,1).

More extreme cases (more examples)

To be clear, data containing one or more zeros (such as (0,2,4) or (3,0,3) etc.) simply was not yet classified in that dimension. However, there might be data with a low classification in one (or more) dimension, but with a high rating in another dimension. We will put some focus in examples of that kind to make it more understandable.

In general, data with a low availability classification (1,I,C) could be any sort of phone book. There will be other ways to find out a number of a person to call (operator, contact, friend, another phone book etc.).

Data with a low integrity classification (A,1,C) can be thought of any type of online polls where there is no authentication and access control at all, simply press a button to vote for your favorite, or do it twice. Low confidentiality data (A,I,1) is all type of directory information, and not intended to be confidential, so people can find it.

However, there is also information which may have received a high integrity rating but only a low availability and confidentiality classification, such as a lottery (1,4,1) where it is important that the data is correct, but it is not confidential and there are many ways to obtain it should the data source be lost.

Similar is the patient’s blood type information in a hospital. Another example here is endorsed public health information i.e. by the CDC, telling people to take certain drugs during outbreaks or similar.

A good example for (1,1,4) data (with high confidentiality) is a department staff listing containing personally identifiable information (PII) that combines the phone book with some very stringent and protected data such as a SSN or account numbers. Another example might be the data of a court (expunged court cases).

For the (4,4,1) data I can think of emergency contact information for the public – it should be highly available and also be integer, but it doesn’t need to be (nor should it be) confidential. So in essence, there are all possible combinations of these dimensions with all the various triplets.

It always depends on the specific circumstances, how the owner classifies the data in regards to all three dimensions.

ROI of the C^3

It should be clear by now, that while putting some effort into the correct classification is somewhat burdensome and needs proper planning and discussion, the large benefit of this approach is that finally all the classified data received the correct and appropriate handling, cover and protection.

Simply put, the one-size-fits-all approach is far more costly and mainly inappropriate in today’s corporate or organizational environment. Most of the data breaches have not followed these best practices, and huge amount of storage chunks are becoming bigger and bigger, without questioning the data category/type/classification first.

Completely without any classification, a lot of data may be unnecessarily secured against losses (in A, I, or C regardless) as there is no way of telling if the data needs a more secure environment or protection requirement or doesn’t need those at all.

Having a proper classification routine in place will enable even the largest corporations to handle their initial as well as the update process well and ensure a cost savvy, smart approach to keep the data available, integer and confidential to the right amount.

This could save huge sums of money, depending on industry, organization type and data structure. The specific ROI needs to be calculated by the implementer.

Conclusion

After having defined and argued about the importance of all three of the main parameters representing security (availability, integrity and confidentiality), we have learned about the potential orthogonality (independence) of their classification distribution.

We have seen a pragmatic example of how to assign values and handling requirements in table 1, and understood the requirement to adapt these for each company according to its specific situation. Afterwards we learned about the C3 cube, which depicts a representative 3D model of a helpful color scheme adoption of the standard RGB model to these three main parameters.

This will then help to easily assign a classification notation such as (2,4,2) respectively the color markup as shown in figure 3.

Having found an easy notation scheme both in algebra (with easy to understand transformation formulas) as well as in color will certainly help vendors to introduce solutions to help to further reach our common goal of appropriate and useful data classification.

The ROI case development is reduced to a simple math calculation. Asking the BCP or marketing teams about their approximated values might be helpful here.

This article is appropriated as a think tank approach, to perform further going research, to finally reach the ultimate goal of data centric classification.

Michael S. Oberlaender is currently serving as Chief Security Officer for the largest European cable network provider and has held senior information and security roles in both the US and Germany for two decades. He is member of (ISC)², ISACA, and several industry associations and is certified CISSP, CISA, ACSE, and GSNA. He holds a diploma of physics (MS) of the University Of Heidelberg, Germany. His public profiles can be found at: www.linkedin.com/in/mymso as well as www.xing.com/profile/Michael_Oberlaender.


Secunia
Stay Secure
Reduce the window of opportunity
Why are end-points increasingly vulnerable to attacks?
Access the Secunia Yearly Report 2010 to:
• Understand the state of the security ecosystem
• View vulnerability data and trends
• Plot your optimal defence against vulnerabilities
Stay updated, stay secure.
Download Report:
http://secunia.com/company/yearly_report
Secunia.com

VB2011 - 21st Virus Bulletin International Conference

www.virusbtn.com/conference/vb2011 - Barcelona. 5-7 October 2011.

RSA Conference Europe 2011

www.rsaconference.com/2011/europe/ - London. 11-13 October 2011.

The 2011 Governance, Risk Management and Compliance Summit

www.thegrcsummit.com - Boston. 1-3 November 2011.

SANS London 2011

www.sans.org/london-2011 - London. 3-12 December 2011.

Black Hat Abu Dhabi 2011

www.blackhat.com/html/bh-ad-11/bh-ad-11-home.html
Abu Dhabi. 12-15 December 2011.

When someone mentions biometrics, the first (and sometimes the only) thing that comes to mind to many people are physical characteristics on the basis of which people can be unequivocally differentiated and identified: DNA, finger and palm prints, iris shape, and more. All in all, characteristics that people don't have control over.

But as useful for verification and identification as these characteristics are in the real world, the online one is another matter. The technology behind their exploitation for online authentication is still simply too difficult and too obtrusive to integrate and use and, let's face it, too costly.

Still, there is another class of biometrics that can prove to be useful and way easier to use for this particular purpose - behavioral biometrics. The term is self explanatory: it's the biometrics that are related to a person's behavior.

We all have a way of walking and talking that is typical for us, and the same goes for the way we type. Typing is something we all must do in order to interact with the computer and, through it, with people and online services. Our typing behavior is much easier to record and store, and that process doesn't require special (read: expensive) devices.

It's no wonder, then, that a lot of companies have set their sights on developing a solution that will use keystroke dynamics for identifying or verifying users, often in conjunction with other authentication factors.

But, to my knowledge, a German firm by the name of TM3 Software is the only one so far that has been able to develop a solution that works with any text entered by the user, which means that the user's workflow does not have to be disrupted and that the user can even be unaware of the authentication or identification

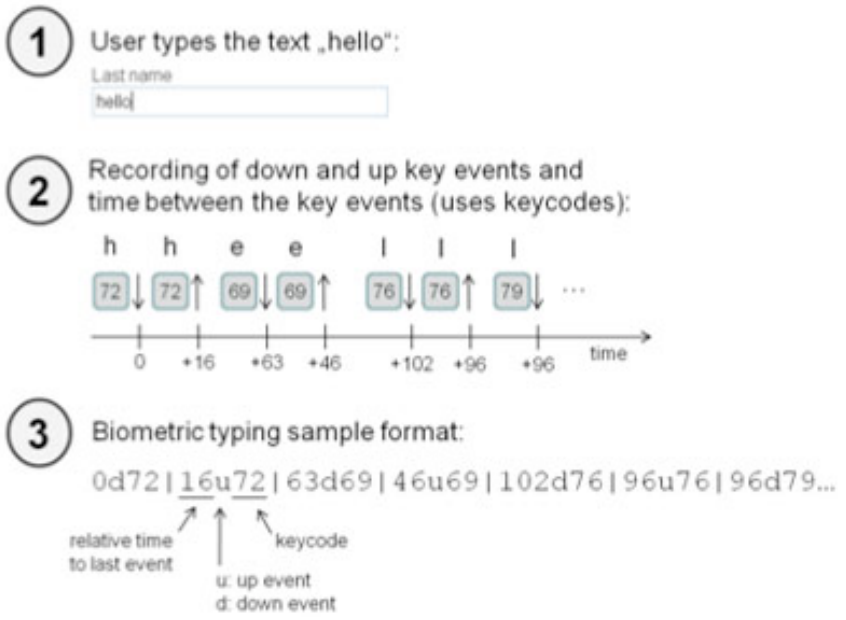
process - perfect for thwarting fraud attempts.

The name of the solution is KeyTrac, and has been available to the public only for the last four or five months. The solution and the company are a direct result of the work that Dr. Thomas Wolfl - the company founder and CEO - and his team of software development and artificial intelligence experts have been doing at the University of Regensburg.

How does KeyTrac work?

As with all biometric solutions, the first step is to collect the data and use it to create a profile. The KeyTrac recording module can be integrated into an existing form - whether it's a registration form, a form for entering address and banking data, product descriptions, forum posts, and more - or into a standalone application (e-mail programs, Office solutions, etc.)

The module records the way that the user types and not what the user types, and turns the collected information into biometric keystroke data:



The best part of it is that the collected data does not contain any type of personal information or information that can be used to draw conclusions about the user. The text becomes anonymous as its being typed, and the contents of the text can't be reconstructed by the system operator or by KeyTrac.

It also doesn't matter in what language the user types, it only matters that he is familiar with it. It even doesn't matter what keyboard the user uses, since every key is assigned a keycode and it is the keycode that gets recorded, which allows the solution to be used with any international keyboard layout.

Once the collected keystroke data is sent to the KeyTrac Core Engine, a user profile is calculated on the basis of several attributes that are extracted from it and stored in a database, to be used after in the identification process.

The identification process starts when an unknown user types in text into a form or an application. The keystroke data is collected again and sent to the KeyTrac Core Engine, which compares that information with the information in the user profiles collected in the database.

If the goal is to check if the registration is a duplicate - for example, if the user has forgot his login credentials and is creating a new account - the data will be compared to all the profiles in the database. If the aim is to detect an intruder with stolen credentials, the data will be compared only to the profile of the user whose account the fraudster is trying to hijack.

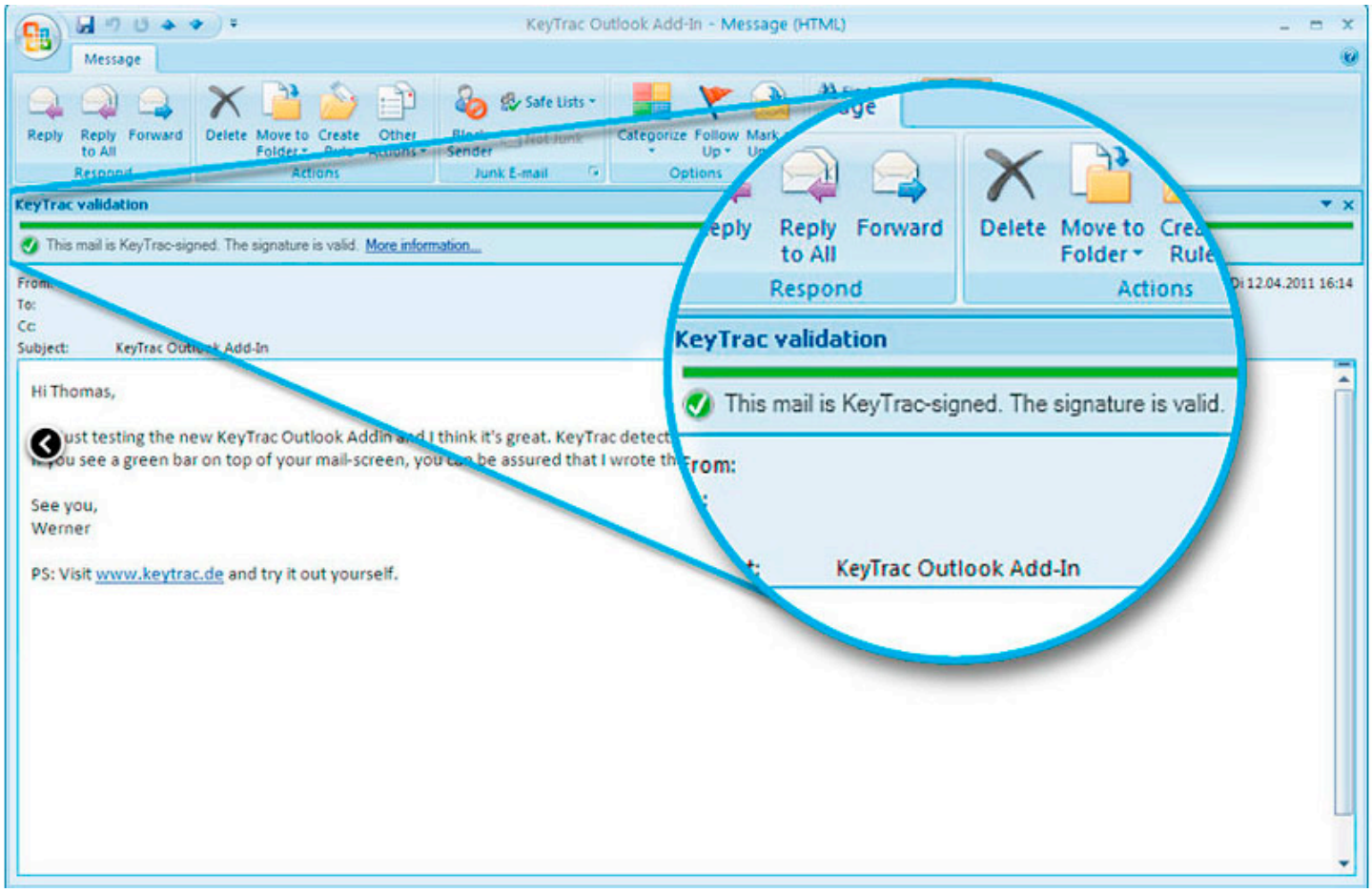
Among the things that KeyTrac can be used for is also online fraud prevention. Fraudsters could be recognized by their typing pattern, regardless of whether they are using stolen credentials or have opened a new account with bogus information.

If a central database of online fraudsters and their typing behavior is set up, the data can also be compared against the profiles in that particular database, preventing, for example, the initiation of fraudulent transactions.

There are other authentication solutions using keystroke dynamics out there, but the fact that the process can be performed without the user knowing about it or without the requirement of typing in a predefined text is the feature that differentiates Keytrac from them.

"All other traditional keyboard biometrics solutions can only be used for password hardening or authentication with always the same fixed text (for enrollment and for authentication)," points out Dr. Florian Dotzler, TM3 Software's Head of Product Management. "KeyTrac can identify the user by any typed text." And this is what makes it perfect for e-payment providers, online retailers and banks for securing online banking.

KeyTrac can also be used to prevent subscription or account sharing - very handy for software providers who offer Software-as-a-Service or use the "named user" license model. Furthermore, it can also be utilized to verify the identity of the individual taking an online test, of the author of a digital document, and even to digitally sign emails or documents:



Seems like a dream come true, doesn't it? And what's more, the integration of the various KeyTrac solutions is easy.

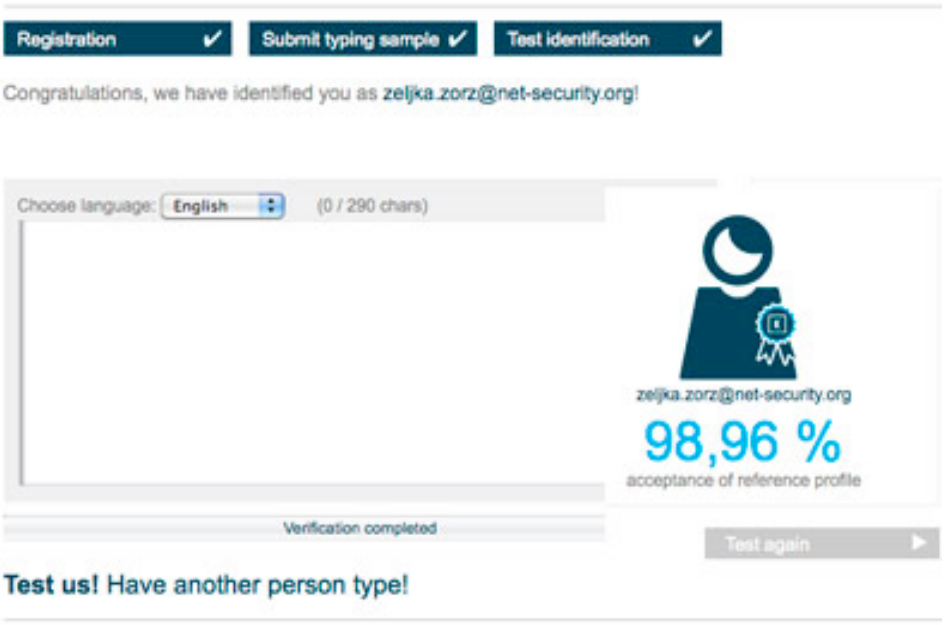
"It takes only one or two days to integrate it in web environments," explains Dr. Dotzler. "In web scenarios, you only have to integrate a short JavaScript in the header of the website in order to record the typing samples, and then deploy a WAR-File (KeyTrac core system) on the webserver or you integrate our web service."

"Integration in legacy systems also needs two-three days," he adds. "But this depends on the use case."

Is it effective?

When it comes to authentication, behavioral biometrics are usually considered less reliable than physical biometrics because they are different in nature. With physical biometrics, you're dealing with absolutes - pass or fail. But behavioral biometrics are more about statistics and percentages.

For example, when I tested the KeyTrac online demo, I was consistently identified, but I never achieved a 100% acceptance of reference profile.



It is actually practically impossible even for the same person to replicate the exact pattern recorded and used as reference. But, a 98,96% probability that the I am the person that created the reference pattern was high enough for the system to let me "pass".

I don't know what percentage is the set cut off point on this demo, but I know that when I tried to pass off two of my colleagues as me and have them type in a text, they were rejected. And the same happened when I changed my typing pattern by slowing it down and pausing between letters in a word.

The point is, keystroke dynamics is probably not accurate enough to be used as the only identification and authentication method, but combining it with others might just prove to be the missing ingredient for a foolproof solution.

Dr. Dotzler points out that every biometric system has false positives, and that one can lower their number but one can never completely avoid them. The issue can be resolved in a number of ways which depend on the use case.

Keystroke dynamics does present one significant benefit over other authentication methods: keystrokes can be captured constantly, making situations like someone forcing a person to login into a service by typing his password and then taking over the keyboard easily detectable.

But what about the fact that the way one types changes with the time of day, emotional or physical state?

"The system works with algorithms from artificial intelligence," explains Dr. Dotzler. "These algorithms learn the different characteristics when a user uses different keyboards. During that learning process, there is a lowering of quality of the method."

But, there are ways to solve this problem. "You can create a second profile for the user (for the second keyboard)," he says. "Also, if the user brakes an arm, his keystroke dynamics will differ so much that the system must be retrained. But small injuries are not a problem."

Conclusion

Every technology has its weak spot. As we recently witnessed, the RSA breach has showed that even proven technologies such as the SecurID tokens can be bypassed and misused if one knows where to look and what to do.

The saved reference patterns needed for KeyTrac to work could probably be stolen somehow, but can they be used to recreate the typing pattern and execute an successful attack? If the technology itself proves effective and begins to be used by many, there is no doubt in my mind that, in time, someone will figure out how to trick it.

In the meantime, a number of e-payment and e-commerce providers have started using KeyTrac. It may be too early to tell if it is the missing piece of the puzzle that will solve the issue of digital identity verification, but it certainly looks promising.

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

SECURITY AS A SERVICE

NOW AVAILABLE AT A BROWSER NEAR YOU

Software-as-a-Service (SaaS) has been described as the most disruptive delivery model to ever face the enterprise software market for one simple reason: ***it works***

Qualys is the first company to deliver an on demand solution for security risk and compliance management. QualysGuard® is the widest deployed security on demand platform in the world, performing over 150 million IP audits per year — with no software to install and maintain.

For a free trial, go to a browser near you.

www.qualys.com/SaaSTrial

There is no doubt that the cloud is revolutionizing the implementation of IT and application architectures. The issue that we face today is how exactly should we move to the cloud while maintaining the security of our data.

According to a recent survey by Kaspersky Lab, over 62 percent of IT managers state concerns about security as an obstacle to cloud adoption. Prioritizing security activities and implementing new controls to address the new realities of the cloud is the fundamental problem organizations struggle with today.

In this article, I will address the issue of how the fundamental split in ownership of the application "stack" from the computing resources upturns traditional security assumptions of how to build walls around data, and how we can re-build walls back into the amorphous cloud.

Challenging our assumptions

In order to solve the security problem that arises with the move to the cloud, we must challenge our assumptions. The cloud has changed how we think about IT architecture and application infrastructure, and the same must happen to our security perspective. To be specific, there is a physical ownership assumption built into traditional security models that simply doesn't carry over into the cloud. To be fair, the consumerization of IT and the loss of strict network boundaries have also forced changes in ownership-based models. However, these earlier changes represent a finer degree of segmentation and specialization rather than a change in how we must approach security in the cloud.

The history of PCI is a great example of how this assumption played out in real life. PCI 1.0 began with a strict data encryption requirement (Section 3.4) as the best practice to protect cardholder data. It became immediately apparent that just about every organization would be unable to adhere to these guidelines because of more fundamental reasons related to data discovery and data elimination

before they could even reasonably think about doing encryption.

PCI 1.1 provided a stop-gap risk mitigation strategy by letting organizations compensate for the lack of Section 3.4 compliance by documenting and putting in place controls that essentially assume physical ownership of the resources.

You could pass a PCI audit if you owned the infrastructure, proved solid segmentation, passed additional checks against malware and other threats, and implemented best practices around the systems that control this data.

These were all very valid controls and one could reasonably assume data protection given the strong control of the entire implementation stack.

The problem, of course, is that this level of ownership is not possible in - and is, in fact, entirely in opposition with - cloud-based infrastructures.

The break in the foundation

One of the most difficult things for people to assess is who is responsible for data security in the cloud. The short answer is everyone.

Your organization will secure the part of its infrastructure that it places in the cloud and cloud providers will secure and attest to the security controls they have in place in their part of the cloud.

The easiest way to understand this is to think about the cloud from an OSI model perspective: the stack is essentially going to be split between the two parties.

To simplify things, we'll focus here on Infrastructure as a Service, or IaaS. (SaaS is generally the responsibility of the cloud provider and a matter of attestation and contract negotiation. PaaS is an extremely variable architecture too complex to cover here.)

In IaaS, the cloud provider essentially owns everything at and below the hypervisor, shimmed in just below your OS. You own everything above. As a result, a tremendous amount of existing security controls remain the same. The thing that changes is who implements them.

1. Partial ownership by the cloud provider

Your IaaS provider is responsible for physical security and the proper vetting and training of employees. They own the switch fabric and are responsible for the proper segmentation and VLANing.

They also own, to some degree, the network isolation around you as a customer within their IaaS environment. Yes, you will have your own firewalling and topology to work with, but the cloud provider is responsible for separating you from the other "tenants" in the multi-tenant architecture. You would expect them to deploy good firewalls with proper configuration.

They take care of DNS integrity, proper routing and so forth. Other than that, the burden of security controls for the rest of the application and hosts above the hypervisor fall onto you, the cloud customer.

2. Partial ownership by the cloud customer

On the flip side, as a customer, you would still be responsible for patch management. Even if the IaaS provider gave you the instance, you are still responsible for patch and configuration management. You're still responsible for host integrity and anti-malware.

You're responsible for configuration control, proper training and vetting of your employees who work with these systems, and building a solid security and change management process around it.

You are responsible for application code on top of it, adhering to secure coding principles and practices, and even conducting regular security reviews and possible pen testing.

In actuality, a lot of what organizations do here doesn't change dramatically from non-cloud activities. What does need addressing is the loss of the physical isolation and controls that were once a given in the traditional proprietary data center.

Setting a solid footing

Knowing that physical ownership and isolation are no longer a given and that host instances are sitting on new, possibly vulnerable hypervisors, we can turn to encryption to isolate our information, provide segregation of duties, and reduce your overall information risk profile.

1. Instance and volume encryption

The great, untapped opportunity to reduce risk in the cloud is encryption at the lowest layer owned by the customer: the instance and volume level. Implementing encryption, when done properly, can provide a fourfold benefit: it can protect data in off-line dormant images and storage, reduce the overall exposure to data leakage, provide segregation of duties when authentication is separated from the cloud provider, and give another audit and reporting mechanism to monitor the cloud.

2. Cloud attestation of controls for hypervisors and dormant instances

Encryption dramatically reduces the overall risk profile but in itself isn't perfect. It only reduces the number of vectors attackers can use to gain access to the data.

To complement the use of encryption, you will need to check that the cloud provider has controls for preventing data breaches that could happen in running instances (after all, data has to move to clear text to be used). On the hypervisor front, ISO standards and SSAE 16 (formerly SAS 70) attestations can help assure you of hypervisor controls.

In addition, using an encryption system that uses key obfuscation in memory reduces exposure of the critical encryption keys. Finally, good cloud providers won't store running instances to avoid exposure of data in memory, or provide APIs to let security products know to do encryption key wiping prior to snapshotting or storage.

3. Reexamine data encryption

Organizations that don't already encrypt data at the application or database level should reexamine doing so in workloads that are moved to the cloud. It is an easy risk mitigation technique that complements lower-level encryption at the instance and volume level.

Regulations like PCI require it and, specifically, new PCI guidelines on virtualization put even more pressure on encrypting at multiple levels.

4. Customer controlled proper encryption key management

Doing key management wrong can completely undermine the security of the entire crypto system and negate the non-repudiation and trust an auditor will look for in your implementation.

FIPS 140-2 certifications, adherence to NIST 800-57 guidelines, and an experienced track record of key management by vendors can help ensure proper deployment.

Look specifically for proper key storage (for instance, not storing keys with images), strong key derivation beyond simple password-based keys, key granularity enabling individual instance/volume/data elements to be separately encrypted, the ability to easily perform key rotation in adherence with best practices, and customer retained control of the encryption keys to help ensure proper key management deployment.

5. Elastic encryption

Finally, it is imperative that the implementation guidelines listed above support the elasticity, dynamic provisioning and agility that is the reason organizations are moving to the cloud in the first place.

Specifically, these implementations should integrate with cloud management platforms being deployed over the cloud, support the capability to automate authentication and authorization based on the activities of the cloud management system, and provide interfaces to these systems to help integrate security into the overall cloud process workflow.

Dean P. Ocampo, CISSP, is the Director of Cloud and Compliance Solutions, SafeNet (www.safenet-inc.com).

Visiting Bitdefender's headquarters

by Mirko Zorz

Recently (IN)SECURE Magazine visited Bitdefender in Romania as it unveiled a complete reinvention of its brand spanning the entire product line and offered a glimpse into the features that we can expect in future products.

Bitdefender's headquarters are located in Bucharest and house around 380 employees.

Alexandru Catalin Cosoi (up left), the Head of Online Threats Lab at Bitdefender, was our guide for the tour that took us through a large portion of the Bitdefender offices.

Bitdefender CEO Florin Talpes illustrated the story behind the re-branding process in an event packed with both media and partners.

Google search results much cleaner than in 2010

It used to be that among the first ten pages of search results for popular terms, up to 90 percent of the offered links would take the users to a malicious page serving malware. Now, the same sample contains only up to three malicious links, and the great majority of these links take users to pages offering fake AV.

There are many reasons behind this fortunate decline. It seems that not only have the hosting companies begun reacting more quickly when it comes to the takedown of malicious domains, but that webmasters have also begun cleaning up their sites more speedily as well.

There is no doubt that Google deserves some credit for this last change, as it has begun educating webmasters by popping up warnings in Google Webmaster Tools and by sending them emails notifying them that their site was hijacked.

But, it's not all good news. Malicious search results for popular terms might have declined considerably, but cyber crooks have extended their interest to a broader range of topics and types of searches - for example, poisoned Google image searches.

"Searches for buying software online remains 90 percent malicious, redirecting users to fake stores, says Zscaler's Julian Sobrier. "There has been no significant improvement on that front, with 60 different fake store domains observed in July 2011." But, as he points out, this is a problem shared by all search engines.

Install one Trojan, get three more

Downloader Trojans are often used by cyber crooks to thoroughly infect systems in order to extract anything that might be of value to them.

Trojan.Badlib is a particularly effective piece of malware belonging to that particular category, effectively acting as a malware distribution network.

When Badlib is firstly installed and detects an Internet connection, it tries to reach a C&C server in order to receive commands from it. It searches for it on a number of hard-coded domains, and if it doesn't find it, it proceeds to check out several IP addresses on a default list.

Once the C&C is contacted, it instructs the Trojan on where to download further malware. The response includes the number of files it has to download and their digital signature so as to make sure it downloads the right ones.

According to Symantec researchers, Badlib is currently downloading three distinct Trojans: Trojan.Badfaker (disables present AV solution, hides that fact from the user), Trojan.Badminer (uses the power of the infected computer's GPU to mine Bitcoins), and Infostealer.Badface (harvests login credentials for a number of popular social networks).

Improved SpyEye variant actively attacking Android devices

The first SpyEye variant, called SPITMO, has been spotted attacking Android devices in the wild.

“When a user browses to the targeted bank a message is injected presenting a 'new' mandatory security measure, enforced by the bank, in order to use its online banking service," Trusteer’s CTO Amit Klein explains.

"The initiative pretends to be an Android application that protects the phone’s SMS messages from being intercepted and will protect the user against fraud. How’s that for irony!”

Once the user clicks on "set the application" he is given further instructions to walk him though downloading and installing the application.

To complete the installation, the user is instructed to dial the number "325000"; the call is intercepted by the Android malware and an alleged activation code is presented, to be submitted later into the "bank’s site". Besides concealing the true nature of the application, this "activation code" does not serve any legitimate purpose.

Once the Trojan has successfully installed, all incoming SMS messages are intercepted and transferred to the attacker’s Command and Control server. A code snippet is run when an SMS is received, creating a string, which will later be appended as a query string to a GET HTTP request, to be sent to the attacker's drop zone.

“What makes all of this so scary is that the application is not visible on the device’s dashboard, making it virtually undetectable, so users are not aware of its presence and will struggle to get rid of it."

Morto worm spreads via RDP, brute-forces Administrator accounts

There's a new worm in town and it's the first one that spreads by taking advantage of the Remote Desktop Protocol (RDP).

"Once a machine gets infected, the Morto worm starts scanning the local network for machines that have Remote Desktop Connection enabled," explains F-Secure. "This creates a lot of traffic for port 3389/TCP, which is the RDP port."

When such a machine is found, the worm proceeds to try to brute-force its way to an Administrator account. It tries around thirty most often used passwords (admin, password, 111111, 12345, and similar).

"Once a new system is compromised, it connects to a remote server in order to download additional information and update its components," warns Microsoft.

"It also terminates processes for locally running security applications in order to ensure its activity continues uninterrupted."

According to Microsoft's analysis, Morto's main functionality seems to be launching DDoS attacks against attacker-specified targets.

Morto is capable of infecting both Windows workstations and servers. According to some comments by infected users, it seems that running a completely patched system doesn't do much for protecting it, as the worm does not exploit a vulnerability in the software, but the unfortunate user tendency of choosing a poor password.

As a number of Morto variants have been spotted already, and the number of infected hosts is rising, users are advised to either change the password for the Administrator account to something much more complex, or to disable their Remote Desktop Connection if it's not needed.

Additional analysis of this worm revealed more than one never-before-seen characteristic.

Morto is capable of infecting both Windows workstations and servers.

Not only does it spread by using the Remote Desktop Protocol, but it also uses a novel way to contact its C&C in search for instructions: via DNS (Domain Name System) TXT records.

"While examining W32.Morto, we noticed that it would attempt to request a DNS record for a number of URLs that were hard-coded into the binary," said Symantec's security response engineer Cathal Mullaney.

"This is by no means unusual or unique, but when we examined the URLs, we noticed that there were no associated DNS A records returned from our own DNS requests. On further investigation, we determined that the malware was actually querying for a DNS TXT record only – not for a domain to IP lookup – and the values that were returned were quite unexpected."

All in all, the information provided was a binary signature and an IP address from which the worm can download further malware - the same information that most threats receive using more established communication channels.

Bitcoin mining botnet also used for DDoS attacks

A recently discovered P2P Bitcoin mining botnet has acquired DDoS capabilities, warns Kaspersky Lab expert Tillmann Werner.

It's main reason of existence has so far been Bitcoin mining, as the bot installs three Trojans with that function (Ufasoft, RCP and Phoenix), but it also functions as a way of delivering other malicious software to the infected machines.

And among the delivered files are two DDoS program. Their targets change as different victim lists are delivered to it by the botnet operators.

The first module - which uses HTTP flooding - has been spotted attacking estate agency portals and food industry sites. The second one, using UDP flooding, was targeting the IP addresses of companies that offer anti-DDoS services.

Unfortunately, given the P2P architecture, this botnet will be extremely hard to take down. As things stand, the number of infected machines taking part of it is increasing. And, as its targets are easily updated by its operators, the next ones will likely be determined by the people who will rent its services in the future.

The number of infected machines is increasing.

Cyber crooks misusing audit tool to breach VoIP servers

SIPVicious - the popular bundle of tools designed for auditing SIP (Session Initiation Protocol) based VoIP systems - is currently being used by crooks that aim to compromise and likely use vulnerable VoIP servers for placing unauthorized calls to premium rate numbers or for vishing (voice phishing) scams.

It all starts with the user visiting a compromised legitimate site injected with a malicious iFrame, which redirects him to a site hosting the Black Hole exploit kit.

The exploit kit does its thing - it searches for vulnerabilities present in the visitor's system and, if it finds one, downloads a Trojan (jqs.exe) and executes it on the system.

After contacting its C&C server and downloading instructions, the Trojan tries to connect to a .cc domain, from which it downloads the SIPVicious toolset, a Python interpreter and an unraring tool.

"The Trojan invokes Microsoft installer and installs Python silently in the background," shared the researchers. "It also unrars the SIPVicious toolset."

Under orders from the C&C server, SIPVicious is used to scan for SIP devices inside the network, which are then hit by a bruteforce attack. If the attack is successful, the Trojan attempts to register extensions on the device, which will then be misused by the crooks.

Pay-per-install services attempt discreet comeback

"Pay-per-install businesses can be temporarily compromised by welcome law enforcement action, but the crooks will always find a way to return," says McAfee's Francois Paget, who shared his recent discovery of a newly opened forum offering free malware to its users.

The offer was obviously made to attract as many users as possible at that moment, but it lasted only seven days, during which the forum was opened for registration to anyone.

Once the seven days pass, inactive users are deleted and aspirant members are able to join only by invitation.

To make the forum seem hopping with activity, the site administrator and various moderators have resorted to opening threads and copy-pasting information from (uncredited) sources all over the Internet. But, the threads dedicated to the buying and selling of goods and services seems to be thriving without their help.

Paget ran into an offer mentioning, among others, the well-known fake antivirus business Best AV, whose operation was seemingly disrupted back in July due to efforts by law enforcement agencies in the US and other countries. Pay-per-install services - most of which had their websites recently shut down - are also present.

"The pay-per-install forum sponsors services that will install malware for a price. Many countries are available, though not Russia and some others in Eastern Europe," says Paget. "I suspect all these services reach a unique group that is engaged in designing a new business model they hope will be more discreet."

Cybercriminals impersonating government agencies

Notable threats for August 2011 included spam and poisoned search engine results targeting fans of Harry Potter, Trojans posing as electronic traffic tickets from the New York State Department of Motor Vehicles, and phishing emails disguised as official notices from the Department of Defense.

"Last month, we saw scammers out in full force," said Christopher Boyd, senior threat researcher at GFI Software. "They tried to exploit the incredible public interest in the launch of the Harry Potter fan site Pottermore, and they concocted fresh schemes to impersonate government agencies in order to defraud the public."

"In many cases, cybercriminals are recycling the same tactics. That underscores how much work still needs to be done to educate the public, but it also helps the security community anticipate new threats."

The FBI recently issued a warning against fraudulent charity organizations soliciting donations for victims of Hurricane Irene, a tactic that cyber scammers continue to employ in the wake of natural disasters.

New Zeus-based variant targets banks around the world

Another Zeus-based offering has been unearthed by Trend Micro researchers, and by the look of things, this one seems to be better crafted than the recently discovered Ice IX crimeware that doesn't deliver on its promises.

Having analyzed the code, they believe that it was created by using version 2.3.2.0. of the Zeus toolkit and that it was created specifically for a professional gang comparable to LICAT.

This solution is likely to succeed where Ice IX has failed: an updated encryption/decryption algorithm that should prevent trackers from analyzing its configuration file.

Also, an update of the Zeus builder capability of checking for bot information and uninstalling it should make antivirus solutions unable to use it for detecting the bot and automatically purging the system of it.

"It is also worth mentioning that this malware targets a wide selection of financial firms including those in the United States, Spain, Brazil, Germany, Belgium, France, Italy, Ireland, etc," say the researchers. "It targets HSBC Hong Kong, which suggests that this variant may be used in a global campaign, which may already include Asian countries."

BIOS rootkit found in the wild

Security researchers have recently discovered a new rootkit that targets computers' BIOS, making the infection harder to detect and eradicate, and persist even if the hard drive is physically replaced.

According to Webroot, the malicious package contains a BIOS rootkit, a MBR rootkit, a kernel mode rootkit, a PE file infector and a Trojan downloader. Once it downloaded on a computer, the malware first checks which BIOS it uses. If it's Award BIOS - used by motherboards developed by Phoenix Technologies - it hooks itself on it so that every time the system is restarted it can infect it all over again if the need arises.

Once it's there, it proceeds to add code to the hard drive's master boot record (MBR) in order to infect the winlogon.exe (Windows XP/2003) or winnt.exe process (Windows 2000), which will be used to download an additional file and execute it. It is another rootkit, and this one aims at preventing the MBR code being cleaned and restored to normal by an AV solution.

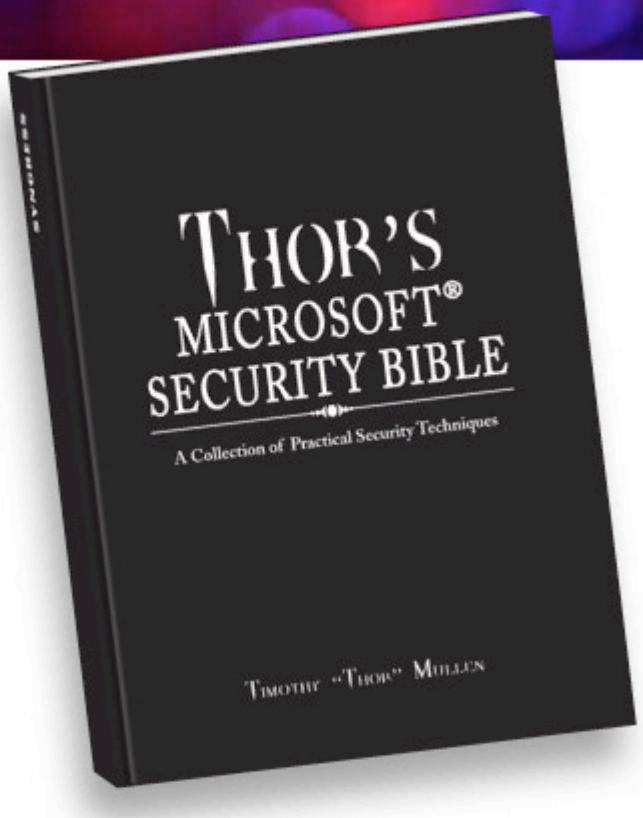
Mebromi is currently targeting Chinese users, which is obvious by the security software it tries to find and block. And even if the victim's computer isn't using Award BIOS, the threat isn't thwarted - it simply omits the first step and goes directly for the MBR.

Webroot's Marco Giuliani speculated that the reason why Mebromi only targets Award BIOS ROM is because it has been modeled after the IceLord rootkit - a PoC that did the same thing. To make Mebromi a major threat, its creators must make it fully compatible with all major BIOS ROM out there - and that is a difficult feat.

SYNGRESS

Delve Deeper Into Security

with Syngress



Thor's Microsoft Security Bible

A Collection of Practical Security Techniques

By Timothy "Thor" Mullen

978-1-59749-572-1 | August 2011
Hardback | 322 pp.
$59.95 | €42.95 | £36.99 | $74.95

World-renowned security expert, Timothy "Thor" Mullen, presents a fascinating collection of practical and immediately implementable Microsoft security techniques, processes and methodologies uniquely illustrated through real-world process examples!

Securing the Cloud

Cloud Computer Security Techniques and Tactics

By Vic (J.R.) Winkler

978-1-59749-592-9
April 2011
Paperback | 290 pp.
$59.95 | €42.95
£36.99 | $74.95 AUD

The first book that helps you secure your information while taking part in the time and cost savings of cloud computing!

Security Risk Management

Building an Information Security Risk Management Program from the Ground Up

By Evan Wheeler

978-1-59749-615-5
May 2011
Paperback | 340 pp.
$49.95 | €35.95
£30.99 | $62.95 AUD

The definitive guide for building or running an information security risk management program.

syngress.com

IBM's Lotus Domino is a unique server platform that blends the traditional web, application, and database servers into one. Its unique structure creates a very different set of security concerns, and its small market share has left it largely ignored by the security community.

Many standard attacks such as SQL injection are simply not possible with Domino although, at the same time, many other - often more serious - vulnerabilities are present. Most of the commonly used tools have very limited coverage of the attacks that are unique to Domino, and very little literature seems to exist.

If you want to test Domino applications, you're going to need to know about its structure and some of the unique vulnerabilities it may present.

IBM's Lotus Domino (formerly known as Lotus Notes Server) is a server platform that can be used to build custom applications. Intended by IBM to be a groupware and application middleware platform, it can act as a web server, perform business and application logic, and contains a custom database format whose files use the .nsf extension.

Within a Domino database (which is contained in a .nsf file), are several components that can be accessed; the primary ones are documents, views, and forms. There are also special Domino objects such as the icon, help, and about objects.

Because all of these items reside within the Domino database, the client accessing the application is actually running Domino database commands directly through the browser. The URL of an action in a Domino application actually contains the database command to be run. The Domino database uses its own proprietary command format and the number of possible commands is far more limited than any SQL server on the market.

The syntax for accessing objects in a Domino database is as follows:

```
http://server/database.nsf/DominoObject?Action
```

The DominoObject can be a view, frameset, form, navigator, agent, document, or page. Special identifiers may be present which begin with the $ symbol. The following chart details the possible actions that can be issued to each object type. When entering as a URL, there is a question mark between the object and the action. Special identifiers usually have a slash instead:

`http://server/database.nsf/$SpecialIdentifier`

View
- Openview – opens the view
- ReadViewEntries – accesses the view data in XML format
- $first – returns the first document in the view
- $searchform?opensearchform – opens a search form from which the view can be searched

Frameset
- OpenFrameset – opens the frameset
Form
- OpenForm – opens the form
- ReadForm – displays the form without its editable fields
- CreateDocument – sent using an HTTP post. Domino will create a document with the contents of the HTTP post packet
Navigator
- OpenNavigator

Agent
- OpenAgent

Document
- EditDcoument
- SaveDocument – sent as an HTTP post. Domino will update the document with the contents of the form
- DeleteDocument
- OpenDocument
- $file/attachmentName – returns the document's attachment with the name "attachmentName"

Page
- OpenPage

There are several special actions and object that can be accessed from the root of the Domino database. All of the following strings can be concatenated onto the end of a URL that ends with .nsf.

- ?Redirect – allows redirection to another database based on it's ID.
- ?openDatabse
- /$about?OpenAbout – opens the "about this database" document
- /$help?openhelp – opens the help document
- /$icon?openicon – opens the icon for the database
- /$defaultview – returns the default view (if there is one)
- /$defaultform – returns the default form (if there is one)
- /$defaultnav – returns the default navigator
- ?openpreferences – opens the preferences setting.

These actions can be combined. For example, the following syntax is valid, and will allow the user to edit the first document located in the default view of the database "database.nsf".

`http://host/database.nsf/$defaultview/$first?editdocument`

Domino uses views to access data from within the database. Each view is created by the developer, and has access to certain data within the Domino database. Because each view is requested by the client through the URL, the client can request any view it desires, and if it has permission to read it, it can see the results. This can be thought of as similar to a stored SQL procedure, except the client can call these stored procedures directly. To find generic names of views that may be used in any given Domino databases, the Domino documentation was searched for sample code and the most common view names were found to be:

1. By Category (135 occurrences)
2. View A (36 occurrences)
3. All (31 occurrences)
4. Main (26 occurrences)
5. Categorized (23 occurrences)
6. Main View (22 occurrences)
7. All Documents (13 occurrences).

There are also default databases that can often be found on Domino web servers.

Although the potential list of default databases numbers in the hundreds to the myriad of configuration options and versions available, the most common ones include:

• names.nsf - often the most important database of any Domino server, it contains the Domino directory, the repository of all users and roles within that database
• log.nsf - shows events on the server
• WebAdmin.nsf - a web version of the admin client.

There are also default databases that can often be found on Domino web servers. When doing a security review of a Domino application, do not rely solely on the standard web application review process. Check for the various special identifiers and Domino objects.

As with any default resources that may be left over from any other application or platform, default objects may contain valuable information about the application, help you fingerprint the infrastructure more accurately, and on occasion will even provide access to additional functionality. Always check the about object to see what notes the app developer may have left - not knowing it could be publicly read. Checking for default views, navigators, and documents may uncover private data.

Enumerating views, using both the common view names provided here and educated guesses based on the application itself can uncover serious information leaks. Ensure that sensitive data cannot be accessed via manipulation of various Domino objects.

Make a special point of checking for a default navigator (/$DefaultNav?OpenNavigator) - if it is accessible, it will list all non-hidden views in the database. This is analogous to getting (and being able to run) all of the stored SQL procedures in a database. Domino allows views to be marked as “hidden”, however they can still be accessed through the browser by putting parenthesis around the view name.

For example, if you want to see if the view named “All” is available in database.nsf, and “All” is hidden from view, you must enter /database.nsf/(all) as the URL. Unless the developer has explicitly set various security controls to protect the documents within a hidden view, they can still be accessed. Many times an application will rely on views being marked “hidden” to protect their contents, however hidden views are not actually part of the Domino security model. Hiding a view is a cosmetic feature that can be abused if used as a security control.

Domino’s search form is another object with security implications. When a client requests a search form, Domino will by default first look for a custom search form. If there is none, it will look for a search template. If there is none, it will use the default search page.

The default search page can return any data that has been indexed, whether the client is meant to have access to it or not. If a database has been indexed, and the developer has not created a custom search form, any view that is searchable becomes a means of exfiltrating all data from the database.

Domino agents could potentially create a vulnerability to DoS attacks. Since they can be activated directly by the client, a client could request an agent be run an arbitrarily a large number of times. Unless there is anti-automation logic built into the agent logic, it could result in excessive CPU or memory utilization. This is also a concern when using automated scanners as they may accidentally cause an undesired DoS attack.

Since the standard three-tiered architecture is not possible with a Domino server (the application logic and the data are too tightly coupled to be reasonably separated), clients have the ability to gain greater access to the internal application logic. Lax permissions that usually would go unnoticed due to protections from another tier will be far easier to exploit in a Domino environment.

As a security tester you have to understand Domino’s unique structure and capabilities in order to adequately review it for vulnerabilities.

Ari Elias-Bachrach (www.angelsofsecurity.com) is a CISSP, CEH, and GWAPT. He works as an in-house information security engineer focusing on web and mobile applications.

BLACK HAT IS THE WORLD'S MOST IMPORTANT INFORMATION SECURITY CONFERENCE

[dates]

TRAINING: DECEMBER 12 – 13

BRIEFINGS: DECEMBER 14 – 15

EXPO: DECEMBER 14 – 15

Two day training courses

- Advanced PHP Hacking
- Cyber Network Defence Bootcamp
- Hacking by Numbers: Unplugged Edition
- Infrastructure Attacktecs & Defentecs: Hacking Cisco Networks
- Mobile Hacking
- Assessing and Exploiting Web Applications with Samurai-WTF
- The Exploit Laboratory
- Incident Response: Black Hat Edition by MANDIANT
- Malware Forensics & Incident Response
- TCP/IP Weapons School 3.0

Gold sponsor

NETWITNESS
Know Everything. Answer Anything.

Silver sponsors

McAfee · rune Information Security Corporation Pte Ltd · QUALYS Q On Demand Security · CAMBRIDGE EDUCATION

ICT Partner

DUBAI INTERNET CITY

Official media partners

CPI · cnme computer news middle east · NETWORKWORLD THE CONNECTED ENTERPRISE MIDDLE EAST

Official news wire

PR Newswire
United Business Media

Organised by

UBM

Register to attend www.blackhat.com

To discuss how you can benefit or to learn about sponsorship opportunities contact:

E : becky.crayman@ubm.com // T : +971 (0) 2 4064317 // M : +971 (0) 50 1052466

Black Hat USA 2011 took place at Caesars Palace in Las Vegas, July 30-Aug 4. Members of the security industry were able to choose between over 50 multi-day training sessions, 7 briefings tracks with the latest research, and 2 workshop tracks dedicated to practical application and demonstration of tools.

(IN)SECURE Magazine was on-site, and what follows is a photo walkthrough.

At the event, Qualys announced QualysGuard Web Application Scanning (WAS) 2.0, the new QualysGuard User Interface (UI) as well as the new QualysGuard Consultant Edition.

The new UI for the QualysGuard IT Security and Compliance SaaS Suite features interactive dashboards, streamlined workflows, actionable menus and filters with improved visual feedback, making it easier for customers to utilize the comprehensive services in the QualysGuard Suite.

QualysGuard WAS 2.0 enables organizations to leverage the power and scalability of the cloud to discover, catalogue and scan large numbers of web applications. The new version simplifies the complexity and reduces costs of web application scanning with an automated solution with an extremely low false positive rate and a rich dynamic UI that simplifies the workflows for scanning and reporting.

A new edition of the QualysGuard Consultant service features virtualized scanner appliances and a report customization module. It brings the power of the SaaS model to consultants, delivering accurate network auditing, comprehensive vulnerability assessments, policy compliance and web application scanning, reducing time on-site for consultants and providing data-rich, customizable reports.

Aruba Networks, which provided and maintained the wireless network for last week's Black Hat USA 2011 conference, provided some interesting statistics around the network's use.

The device-fingerprinting capabilities of the Aruba network enabled visibility into exactly who was using what on the network:

• Apple devices were most prevalent at 43.3 percent of all devices (28.4 percent alone for iOS iPad and iPhone, with another 14.9 percent running OS X).

• Linux users composed 35 percent of the total.

• Windows users represented 21.8 percent.

The network was accessed by more than 2,400 attendees, with 853 as the maximum number of concurrent users.

The network detected and contained more than 8,790 independent security events, including 670 rogues, 191 AP flood attacks, 489 instances of AP spoofing, 579 instances of IP spoofing, 1,659 "Hotspotter" attacks and 1,799 "Block ACK" attacks.

One of the most talked about presentation at this year's event was certainly "SSL And The Future Of Authenticity" by Moxie Marlinspike.

While it's amazing that SSL has endured for as long as it has, some parts of it - particularly those concerning Certificate Authorities - have always caused some friction, and have more recently started to cause real problems.

It provided an in-depth examination of the current problems with authenticity in SSL, discussed some of the recent high-profile SSL infrastructure attacks in detail, and covered potential strategies for the future.

It concluded with a software release that aims to definitively fix the disintegrating trust relationships at the core of this fundamental protocol.

In another high-profile presentation, Dan Kaminsky played with systems the old fashioned way, cobbling together various interesting behaviors with the last few shreds of what low level networking has to offer:

• IPv4 and IPv6 fragmentation attacks, eight years in the making.

• TCP sequence number attacks in modern stacks.

• IP TTLs: not actually expired.

• Inverse bug hunting: more things found on the open net.

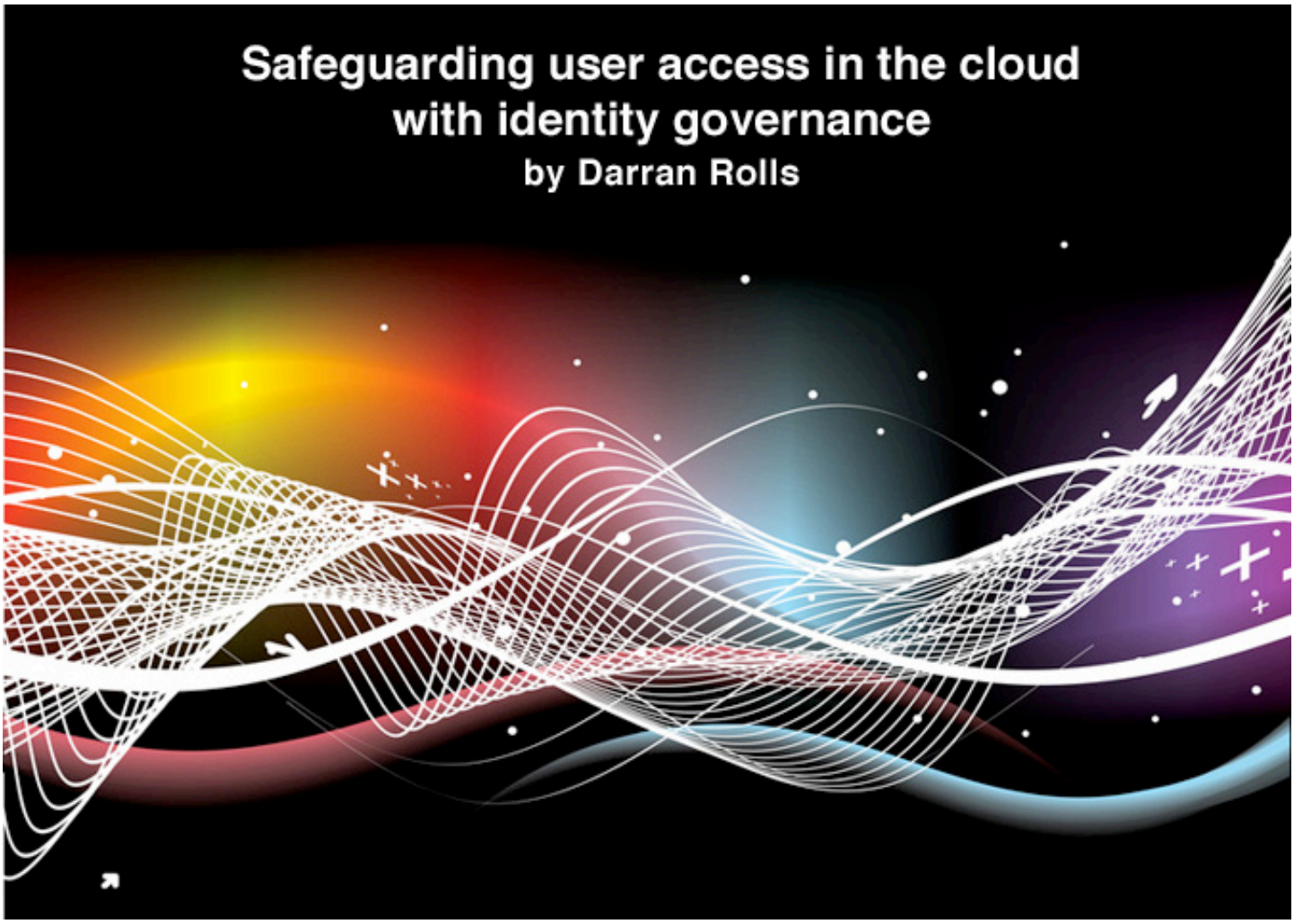
• Rebinding attacks against enterprise infrastructure.

• BitCoin: network manipulation for fun and (literal) profit.

• The net neutrality transparency engine.

Safeguarding user access in the cloud with identity governance

by Darran Rolls



As you build your cloud infrastructure strategy, identity management for software-as-a-service (SaaS) applications needs to be on your radar screen. Since business units are already buying and deploying SaaS applications, sometimes even without consulting the IT department, they could be putting sensitive information into the cloud without understanding the security and compliance risks. Inevitably, sensitive data will find its way into these projects and systems, putting the organization at risk.

Don't assume that by their very nature SaaS applications are not mission-critical. One of the most popular and well-known SaaS applications, Salesforce CRM, provides an example of how many companies could be exposing sensitive data in the cloud.

Salesforce is often used to track a company's sales forecasts, customer and prospect lists, and customer support records, including customer satisfaction details. This is highly confidential and private data, and data that could be very damaging in the hands of a competitor.

You should have additional concerns if the IT staff dedicated to your identity management and compliance requirements is not involved with the user administration of these SaaS applications. Because SaaS applications are often purchased and deployed outside of IT, it's very common for an employee in marketing, sales, or customer support to function as the application's user administrator.

Does this person understand the data security and compliance implications of the actions he carries out? Are the right privileges being given to the right people? Is there a solid business process in place that ensures that these application privileges are removed when users change roles or leave the company? These questions are all critical for your compliance and security initiatives, but most likely not at the top of the mind of business users.

One final area of concern comes from the fact that SaaS applications do not exist on a technology "island," but are integrated with other applications within the enterprise. Some SaaS applications connect to and exchange data with other mission-critical systems, such as ERP systems.

Under the rules of Sarbanes-Oxley (SOX) and other legislative mandates, if an application integrates with core financial applications such as an ERP solution, then that application (whether SaaS or not) also becomes compliant-relevant.

What is required for identity management of SaaS applications?

From an identity management perspective, the same administrative and governance functions are needed for SaaS applications as are needed for core datacenter applications. Organizations must protect and govern access to critical applications, systems and databases in the cloud - and be ready to answer the critical question: "Who has access to what?" In order to meet compliance requirements, it's important that users are only granted access privileges to SaaS applications that are appropriate to their job functions and that the access privileges of all SaaS users are reviewed on a regular basis to ensure they are correct.

Making things more complicated, there is still a lot of uncertainty as to the specific regulatory requirements applicable to the cloud. There are currently no compliance standards specific to cloud computing.

Many service providers undergo SAS 70 (now SSAE 16) audits to prove compliance, but it behooves enterprises to look for service providers that proactively incorporate risk management standards and practices, such as those recommended by ISO 27001 and NIST, who has published very helpful guidance on cloud computing.

Just as important as compliance concerns, organizations must also ensure their ability to meet business demands for higher levels of service for identity management. As new employees and contractors come on board, they need prompt access to a variety of IT systems and applications, including both cloud and datacenter hosted resources.

As users' relationships with the organization change (e.g., a job change or termination), their access must be updated or revoked in a timely manner across all systems, regardless of where they are hosted.

These joiner/mover/leaver business processes need to be automated, controlled and monitored for SaaS applications. Effectively managing these provisioning and de-provisioning processes is critical to keeping the business running, but is also important from a cost control perspective.

Many SaaS application providers invoice their clients based on the number of active user accounts, so organizations need to rigorously manage application usage.

SaaS roadblocks to identity governance

While many identity management requirements will look familiar to enterprises, SaaS applications do present some unique challenges around data access and management control. For example, many SaaS applications do not provide the necessary interfaces and reporting capabilities to support identity governance requirements. This places an increased burden on IT organizations to manually manage users and enforce corporate and regulatory policies in order to meet audit and compliance requirements.

Additionally, cloud service providers often do not expose information to user organizations about how deep their authorization models go in terms of enabling access to their SaaS applications. For example, it is common practice in Salesforce to allow complex, direct entitlement assignments between people and data.

The implications of these assignments are often very hard to effectively manage and even harder to comprehend and govern. As part of a broader identity governance strategy, it is therefore increasingly important for the organization to know exactly "who" is accessing "what" within the SaaS application employed.

A third challenge is that cloud service providers are not always required to share audit and

security information pertaining to how the application infrastructure is managed. To meet various industry and government regulations, an organization must have control and visibility of IT staff and privileged users who have access to application infrastructure. Most compliance mandates require visibility not only to who has privileged access, but also to log data that shows what those users did with that access.

IT organizations should require cloud service providers to disclose how they govern and monitor administrative staff access as part of standard vendor evaluation and vendor risk management practices.

Extending identity governance to SaaS applications

In an ideal world, an IT organization will have the ability to consider these challenges and to plan their strategies for identity management based on a clear understanding of what capabilities their SaaS provider can deliver. But since business users are already rapidly deploying SaaS applications without IT involvement, frequently little or no consideration is given to the ability to integrate the SaaS application back into the organization's core identity management processes and audit controls. Instead, IT organizations must retroactively address these identity management concerns.

For those situations, there are three strategies to help IT organizations gain control over SaaS applications:

1. Focus on an integrated IdM strategy that looks at the datacenter and SaaS applications holistically.

2. Educate business users about the risks of SaaS applications and build their involvement in the broader identity governance strategy.

3. Partner with the cloud service provider to understand how they will open up their interface to allow the organization to more easily manage and govern user access to SaaS applications.

IT ORGANIZATIONS SHOULD REQUIRE CLOUD SERVICE PROVIDERS TO DISCLOSE HOW THEY GOVERN AND MONITOR ADMINISTRATIVE STAFF ACCESS

Focus

Since accountability for compliance and security of SaaS applications falls directly on the enterprise, it is critical that organizations put the right controls in place to gain this assurance regardless of whether the data lives in the datacenter or in SaaS applications.

What's needed is an integrated approach to governance that leverages a consistent set of controls across the entire IT portfolio, regardless of where the application or data is deployed.

Organizations can't approach SaaS applications with ad hoc approaches to identity management. Instead, a centralized governance and control model needs to be in place that helps provide enterprise-wide visibility into the identity data, which in turn allows organizations to move forward into the cloud while maintaining the security and compliance standards the business requires.

Educate

At the same time, IT organizations need to educate their counterparts in the various business units about the IT risks associated with SaaS applications.

Fortunately, identity and access governance technology helps address the unique challenges of managing user access to SaaS applications in line with an organization's existing identity management processes from integrating internal controls with the service provider to knowing on both sides who accessed what data and when. But, you can't manage what you don't know about.

Although SaaS applications allow business units to circumvent much of the traditional IT procurement process, they need to understand the direct implications those solutions have toward a company's IT risk posture.

Partner

From the beginning of working with a SaaS service provider, organizations need to be prepared to partner with them to ensure they are adequately addressing identity management requirements in the cloud.

To do this, it is crucial for end-user organizations to make sure the service level agreements with cloud providers are comprehensive and balanced enough to ensure a necessary level of compliance and the ability to incorporate their own identity governance capabilities into the application.

By taking a proactive approach to governing the user access to cloud applications, organizations can eliminate potential gaps in control and visibility over sensitive data and help facilitate the safe adoption of cloud computing and the operational efficiency it promises.

ONCE THE LARGEST CLOUD SERVICE PROVIDERS ADOPT SCIM, IT WILL PROVIDE GUIDANCE FOR THE SMALLER CLOUD VENDORS

Looking to SCIM to address IdM challenges in the cloud

Fortunately, some of the challenges outlined above are not lost on technology vendors. Many are working with the largest cloud providers, including Google, Webex and Salesforce.com, and systems management providers to define the Simple Cloud Identity Management (SCIM) interface standard.

This will create a much-needed uniform management interface for SaaS and cloud applications to make automated account provisioning possible for even more SaaS applications. The SCIM specification is currently being designed to build on existing efforts, placing specific emphasis on simplicity of development and integration, while supporting existing authentication, authorization, and privacy models.

In short, SCIM will make it easier for Web 2.0 applications to interface with each other to create and manage identity. Its intent is to reduce the cost and complexity of user management operations by providing a common user schema, and a much needed unified set of CRUD (Create, Read Update & Delete) operations.

SCIM's ultimate goal is to make it faster and easier for SaaS applications to move user accounts in, out, and around the cloud. SCIM is designed with simplicity in mind to ensure that major cloud providers all use the same REST-based (representational state transfer) model for their user management automation.

Once the largest cloud service providers adopt SCIM, it will provide guidance for the smaller cloud vendors and help take the guesswork out of governing SaaS applications.

As is typical with all industry standards, it will take some time for everyone to come together and agree on the final SCIM specification. Adoption of it will likely take even longer still.

The good news for the industry is that technology vendors and service providers agree on the need for the approach and the key players are already involved to help make it a reality. As more end-user organizations education themselves on the need for identity governance in the cloud, and in turn demand that service providers help address the identity management challenges for their SaaS applications, the process will only accelerate.

Darran Rolls is the CTO of SailPoint (www.sailpoint.com), a provider of identity management solutions.

The 2011 GOVERNANCE, RISK MANAGEMENT and COMPLIANCE SUMMIT

Develop and Align an Integrated Control Framework

NOVEMBER 1-3, 2011

HILTON BACK BAY • BOSTON, MA

Earn up to 24 CPE Credits!

Best Practices and Case Studies Presented in...

4 Topical Tracks...

... with over 25 learning sessions

IT • ERM • Compliance • Finance

- ✓ Discover a methodology that links operational decision-making and strategic planning in an integrated control framework
- ✓ Effectively bridge the gap between process and technology, aligning enterprise risk management, information technology, compliance, legal risk, and financial processes
- ✓ Mitigate systemic risk and regulations to navigate today's challenging economy
- ✓ Connect with industry colleagues through our unique speed networking and interactive topic table presentations.

Register Today! 888.409.4418 www.thegrcsummit.com or www.gsmiweb.com