Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

CLOUD SECURITY

CLOUD COMPUTING LEGAL FRAMEWORK AND PRIVACY

CLOUD SECURITY: IS THE SKY FALLING ALREADY?

ON CYBER INVESTIGATIONS - CASE STUDY: A TARGETED E-BANKING FRAUD

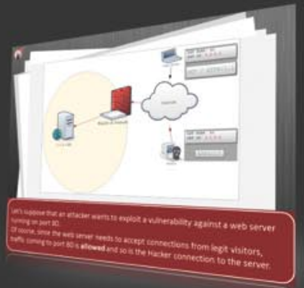
EXPERTS ON CLOUD:

- ANTIVIRUS IN THE CLOUD: FAD OR FUTURE?
- CLOUD COMPUTING STANDARDS: THE GREAT DEBATE
- CLOUD SECURITY: WHOSE RESPONSIBILITY IS IT ANYWAY?

Vol.6 No.5
Issue 05/2011(41) ISSN: 1733-7186

PLUS

AN ANALYSIS OF THE CLOUD SECURITY THREAT
BY JULIAN EVANS



Vulnerable Web Site
Victim
Penetration Tester

eLearnSecurity
Forging security professionals

There is no advertisement like reputation

> While the CEH certification program served as a launching point for students, into the various realms of security, I found it didn't go to the depths that eLearnSecurity's program has reached, on the technical portions of penetration testing. While CEH had numerous tools and usage details, eLearnSecurity's training really dove deep into the underlying concepts beneath such tools.
>
> Timothy E. Everson | Novell, Inc.

> I kept thinking "this is what the CEH/LPT should have been" and I am delighted to say that if students can master the topics and techniques in eLearnSecurity's Penetration Testing Pro, they should be well on their way to being an accomplished pentester.
> eLearnSecurity's course is easy to follow the whole way through with appropriate breaks for video and sprinkled exercises at every turn.
> I am very impressed by the product as a whole and congratulate Armando and Team in an exceptional first run of the course
>
> Jason Haddix | EthicalHacker.net

> If you are just starting out I think the course and the certification will definitely have a positive effect on your career.
> It goes into a lot more depth than courses like CEH and can really benefit your skills.
> The way in which the material is presented is a lot more interactive and interesting than many other courses out there with a good mix of words, images and videos plus a good theory/practical mix too.
> I wish there was something like this in 1999 when I was starting out.
>
> Shaolin Tiger | Darknet.org.uk

Amen.

www.elearnsecurity.com

hakin9 team

Editor in Chief: Karolina Lesińska
karolina.lesinska@hakin9.org

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Steve Lape, Shyaam Sundhar, Donald Iverson, Michael Munt

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Justin Farmer, Michael Munt

Top Betatesters: Rebecca Wynn, Bob Folden, Shayne Cardwell, Simon Carollo, Graham Hili.

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director: Karolina Lesińska
karolina.lesinska@hakin9.org

Subscription: Iwona Brzezik
Email: *iwona.brzezik@software.com.pl*

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by SmartDraw

The editors use automatic system AUPUS
Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,
The internet does not belong to one country or region. Therefore, international collaboration is a key area of focus and we need to continue to work with partners around the globe in support of our cybersecurity goals.(Howard A. Schmidt). And that's exactly why we devoted this issue to cloud computing security. Because of the growing popularity of cloud computing solutions and its future development, the risks associated to working with cloud are also growing. In this issue you will find several articles on cloud that deserve your attention: An Analysis of the Cloud Security Threat by Julian Evans, Cloud Computing Legal Framework and Privacy by Rebecca Wynn and Cloud Security: Is the Sky Falling Already? by Gary S. Miliefsky. I strongly advise you to read them and I am sure you will find lots of useful information there. We have also included some experts views in the topic of cloud for those of you who are looking for more enterprise oriented content.

Also, I would like you to meet Patrycja who will be the new editor of Hakin9. You will find her contact details on our website.

Enjoy your reading
Karolina Lesińska
Editor-in-Chief

REGULARS

6 in Brief
Latest News From the IT Security World
Armando Romeo, eLearnSecurity
ID Theft Protect

8 Tools
A Beginners Guide to Ethical Hacking
by Shyaam Sundhar

Coranti
by Michael Munt

44 ID fraud expert says...
An Analysis of the Cloud Security Threat
by Julian Evans

50 Experts on Cloud
Antivirus in the Cloud: fad or future?
by Malcolm Tuck
Cloud Computing Standards: The Great Debate
by Justin Pirie
Cloud Security: Whose responsibility is it anyway?
by Rik Ferguson

CONTENTS

ATTACK

10 IPv6 Secure Transition Network Architecture

by Michel Barbeau

The Internet has grown to a point where Internet Protocol version 4 (IPv4) can't handle the large number of addresses created by that growth. The long term solution has been the replacement of IPv4 by Internet Protocol version 6 (IPv6), which has the capability to handle an astronomically large address space. Because of the difficulty to switch from one Internet protocol to another, IPv6 deployment has been marginal and several less drastic solutions have been used to expand the address space of IPv4.

24 On Cyber Investigations – Case Study: A Targeted E-banking Fraud Part 1

by Alisa Shevchenko

As money migrates into the virtual world, the crime follows. This article presents a brief journey into the industry of cyber crime and the methodology of cyber investigation, disclosed through a real world case study. The author's main objective is to highlight the general approach and the particular techniques of a cyber investigation process. The criminal case in question demonstrates a typical systematic approach to massive targeted e-money fraud. Due to this reason the article will also serve educational purposes to the professionals involved in cyber crime research and investigations.

DEFENSE

30 Cloud Computing Legal Framework and Privacy

by Rebecca Wynn

Cloud Computing is not a brand new term or concept. Since the days that you started to use AOL Webmail, MSN Hotmail, Yahoo, or Gmail you have been using Cloud Computing. If you use Facebook, Twitter, online data storage, Google Apps, many photo sites, etc. then you are using Cloud Computing. Simply stated Cloud Computing is using others' computer systems, hardware, and software to do things on your system. The data is yours but others take care of the server(s) and application(s).

40 Cloud Security: Is the Sky Falling Already?

by Gary S. Miliefsky

Everyone seems to be jumping into the Cloud with both feet and many before they have realized that there may not be a silver lining with their public or private cloud. Just take a look at the competitive nature of streaming video on demand, offered by NetFlix through the Cloud or Amazon or large cable TV operators like Comcast and others. Some of these vendors seem to be sending out TCP resets on their end-user customers to kill the smooth streaming of a video, over their internet service, because it comes from another video service provider. I'm sure there will be law suits flying soon, when users get upset about their movies hanging, restarting or playing at a lower quality than they expect. So there's already a battle taking place in the Cloud.

Not just Apple. Your smartphones are tracking you

iPhone and iPad have been revealed to store your every move unencrypted at least from September 2010. Yes because up to release of iOS 4.0 this information was kept in a system partition on the device and made available to Apple.

Location information can be found in file consolidated.db on the User partition.

This file can be included in iPhone backups and available to any other app on the phone.

This file indeed, can also be found on iPhone back ups on the PC of the device owner.

Trojans and Spyware are expected to soon include the capability of exploiting this *feature* looking for this information on the infected machine.

The now famous app called *iPhone Tracker*, graphs CDMA locations on a Map by readinginformation stored on this file.

The app and a video showing the use of the tool is available online.

The feature has never been documented by Apple, however law enforcement and specifically cyber police knew about this feature and used it for a long time to track movements of iPhone owners.

This feature indeed didn't sound surprising to companies working in the cyber-forensics field. The amount of information in the file could exactly prove the presence of that device in a position at a given time.

With very high precision. This feature seems to have been in use for a long time.

With time other devices are being studied and we already know that Android devices are doing something very similar already, with information being sent back to Google from time to time. According to famous hacker SamyKamkar, his HTC phone, powered by Android, is sending information about position and nearby Wifi networks to Google a couple times per hour. Including a uniqueidentifier of the phone.

Apple, in the beginning has tried to cover this fiasco using more or less the same excuse used by Google last year when it was found out to store Wifi SSID: a developer mistake.

No one seems to buy this excuse any more though.

Source: Armando Romeo,
www.elearnsecurity.com

Verizon DBIR report shows signs of improved security

One of the most awaited reports on data breach and incidents is the Verizon DBIR powered by Verizon Business. It's a report backed by actual data and actual stats, with very informative graphs and insights.

This year report is backed for the first time by the US Secret Service, bringing 800 new cases to analyze and making insights and stats even more reliable.

The report surprisingly opens with the numbers of records breached dropping from 361 million in 2008 to *only* 4 million in 2010. This can be due to a number of factors, one for all the change in the criminal's final goals.

Threat agents are becoming more sophisticated with money and espionage being the main driver.

Zeus for the first and Stuxnet representing the latter. Moreover hackers are tending more towards *safer* targets like restaurants, hotels and other smaller merchant accounts to perform frauds.

Verizon explains this for the number of arrests in the past two years for breaches happened in Financial institutions where reaction and response is faster to such attacks.

External agents still account for the vast majority of the breaches (more than 90%) and 65% of them come from East Europe and only 3% from Asia (including China), while malware is still the preferred way to steal data.

Source: Armando Romeo,
www.elearnsecurity.com

Hacker arrested for having hacked in Federal Reserve computers

Lin Mun Poo is an experienced Malayisian hacker. The 32 years old man, with a career as a hacker of financial institutes, was arrested at the JFK airport in October 2010. He was found with an encrypted laptop with over 400,000 credit card numbers that the guy was selling for $1,000 in Brooklin.

Police arrested Poo after investigations revealed his responsibility in the hack of ten Federal Reserve computer back in September 2010.

The man has now admitted the compromise of a number of other financial institutions and banks in the U.S.

Sentence is expected later this year. Poo faces up to ten years in prison.

Source: Armando Romeo,
www.elearnsecurity.com

Wordpress servers hacked

Company powering the most famous blogging platform on the internet and hosting million publishers blogs, reported a successful breach of their servers exposing code and information belonging to the company and to its partners.

The breach is a complete root of the servers although it's still unclear how it all happened.

Hackers have had access to everything on the servers although passwords are *difficult to crack* according to Mullenweg, the company's founder.

Wordpress is not new to this kind of attacks, however this surely is the most important for impact.

Source: Armando Romeo, www.elearnsecurity.com

StartUp Britain website hosts malicious URL

StartUp Britain launched in the UK last month (March) in an attempt to champion the UK's start-up businesses. Unfortunately a malicious link was identified after it was launched. UK security vendor Sophos identified the link (which only affected Internet Explorer) which was featured in an article about the US investor Warren Buffet. It took users to a fake banking site called bankling.com where users were redirected to a fake anti-virus page which then gave a prompt saying the user's computer was infected and that they should download a fix.

Source: ID Theft Protect

PHP source code breach reported

It has been reported that there was a serious source code breach at the maintainers of PHP.net back in March. One of their servers had been hacked which led to PHP.net to investigate whether hackers had inserted malicious code to the PHP source code.

Wiki.php.net indicated that a server was compromised and hackers stole account credentials that could be used to gain access to the PHP repository. A flaw had been identified in the Wiki software and Linux operating system. The maintainers forced password changes on all accounts who had access to the compromised server.

Source: ID Theft Protect

NetQin from China accused of bundling malware

According to Chinese security vendors, they are investigating NetQin mobile anti-malware software for bundling malware with their anti-virus software. It appears NetQin was working with another mobile software company called Feiliu to deliberately infect smartphones with malware and charge for removing it.

When users downloaded NetQin, it downloaded the malware from Feiliu. It isn't clear from any reports what the malware was doing. Some reports suggest it installed four malicious files which would slow a smartphone down and NetQin would just delete the benign files to fix the repair. Once downloaded NetQin would detect the malicious (or benign file) trigger an alert and instruct the user to download the security update to remove the malicious files(s).The *malware* infection only affects Java-based versions of NetQin's app.

Source: ID Theft Protect

Exploit exploit Android malware threat

An Android (*http://bit.ly/eAj2oS*) app that used the exploit exploit was found in a legitimate app on Android Market last month. From initial research, it appeared that the exploit didn't work. The exploit used a backdoor shell which combined with the Zhash binary, left the root system on the Android phone open to dangerous exploits.

This same app has appeared on unofficial Chinese app markets, so if you downloaded from one of these, Google would not have initiated the Android 'remote kill' switch.

Source: ID Theft Protect

Adobe Acrobat, Flash and Reader exploit identified

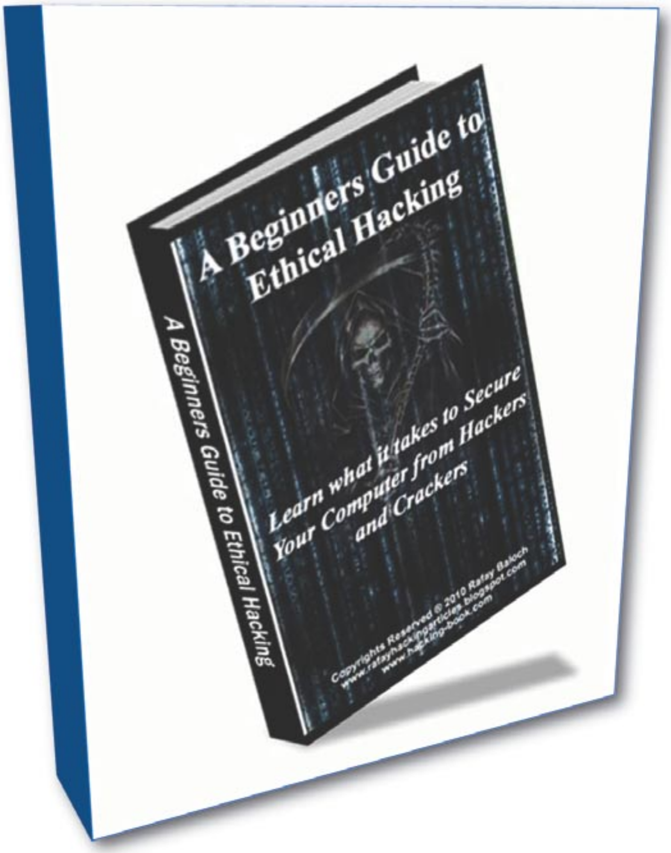
Adobe has reported a suspected zero-day vulnerability in Adobe Flash, Reader and Acrobat. The vulnerability exploits targets flash (.swf) files embedded in Microsoft Word (.doc) files which is delivered via an email attachment. It only targets the Windows system. There are no reported vulnerabilities associated with Adobe PDF.

The vulnerability would allow an attacker to crash or hijack the target PC. Flash Player 10.2.153.1/ 10.2.154.25 and earlier versions of Windows, Mac, Linux and Solaris operating systems as well as Chrome and Android. Also vulnerable are Adobe reader and Acrobat X and earlier 10.x and 9.x versions for Windows and Macs. Worth noting, if you use Adobe Reader X in *protected mode* this exploit will not execute.

No patch is currently available (as of April 20th), but Adobe say that a security fix (*http://bit.ly/gRIUkO*) is planned for June 14th as part of the next regular scheduled quarterly security update..

Source: ID Theft Protect

A Beginners Guide to Ethical Hacking


A Beginners Guide to Ethical Hacking
Learn what it takes to Secure Your Computer from Hackers and Crackers
Copyrights Reserved © 2010 Rafay Baloch
www.rafayhackingarticles.blogspot.com
www.hacking-book.com
A Beginners Guide to Ethical Hacking

URL: www.hacking-book.com
Author: Rafay Baloch
Cost: $20

A Beginners Guide to Ethical Hacking is a great resource for people interested in ethical (white-hat) hacking. It is targeted at „beginners”, but some „intermediate” users may find value in this book as well.

Some people think that there is nothing ethical about hacking – I think that there is nothing ethical about attacking, but hacking can almost always be done ethically. Hackers are thinkers who seek to determine their limitations through challenging their skills, and this book serves to educate readers about how they can challenge themselves in an ethical way.

The book starts by defining the ethical boundaries of hackers – what the cognoscenti considers *too far*. It then quickly jumps into the realm of programming and how code-writing can be leveraged to achieve the readers' goals. Some might argue that programming or reverse-engineering is *old school*, and the *new school* is all about root, but just like in school, you have to start with the *Introduction to* classes before you can move on to the *Advanced* ones. A solid foundation makes for a sturdy building. Programming doesn't mean learning a coding language from scratch, it means finding the resources you need, when you need them. And this book does just that.

The author then moves on to hacking and cracking of passwords, Microsoft Windows OS, Wi-Fi, and websites. In the website section, the author details the web-application side of hacking, then covers malware and virii. This book not only helps you learn the hacking (or *offense*) side of information security, but also the anti-hacking (or *defense*, or *counter-measures*) side of the coin, detailed in the last chapter. By providing a good balance of both offense and defense, the reader is presented with the tools needed to make accurate and educated decisions regarding not only ethical hacking, but also how to properly secure themselves when doing business online.

Overall, I give this book a thumbs-up!

SHYAAM SUNDHAR

Coranti Review

As it was announced that Coranti has won yet another VB100 award bringing their total to three now (*http://www.virusbtn.com/vb100/archive/test?recent=1*) (for those of you that haven't heard of Virus Bulletin, they test all the anti virus platforms on a regular basis and produce reports on how well each product has dealt with the various virii that they throw at it) I was intrigued to see what all the fuss was about as it wasn't a product I had used before.

With 3 anti-virus and 1 anti-spyware engines integrated into 1 product, this then creates a layered defence on your computer which means that you are less likely to incur any viral infections onto your machine.

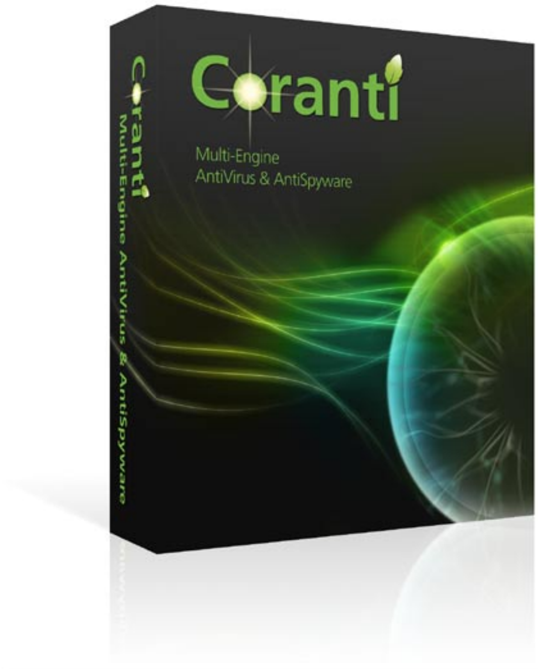
Each of the engines that is integrated into Coranti, have their own excellent perfomance when it comes to detecting and preventing virii infections. BitDefender, F-Prot , Lavasoft Anti-Spyware and Lavasoft Anti-Virus have all been around for quite some time and are well known in the anti-malware industry.

It is good practice to actually scan a machine with more than one program as there are some virii that are designed to bypass specific anti-virus engines and then there is the issue regarding false positives. If you happen to find a file that is identified as possible suspect, you always need to scan it with at least one other program just to see if it is indeed suspect.

Once the program was installed and the system rebooted, it was time for the first pattern update and boy was it huge. 272mb! But you have to remember it isn't just one program your updating this time it is four individual programs, and each one will require their own pattern file/engine update.

The main console is nicely laid out so that everything is easily found. It is clear from the your first glance you can see the exact state of your protection and which engines are running and you have the ability to disable them if you so wish. Some of the lower specification machines (it is recommended to use a Dual Core machine due to the processing power required to run four scanning engines at once) may struggle to run all four engines at the same time, so there may be times when you will switch one or more off to improve the speed of your machine.

You are asked to set off a system scan once the download is finally completed and it will do this with all the engines enabled unless you decide to turn one off. I found that turning off the anti-spyware scan and running it separately after the anti-virus scan was actually quicker than running all four at once. (My machine is very low spec though and this needs to be taken into consideration).



URL: http://www.coranti.com/
Cost: € 39.99 per Computer

I tested the Coranti anti-virus engines first against the usual Eicar test (which every anti-virus should pass) and also against suspect files that my own AV had declared as being unsafe but Virus Total had declared as safe, so it was a good test to see if it would come out as another false positive. It didn't see any issues with the files at all and found them all safe to use (which was the correct response I was looking for).

For testing the Anti-Spyware I went to the spycar website which has been designed specifically to test anti-spyware programs as it will attempt to change various options on Internet Explorer and then allows you to clean it all up afterwards (and they are totally benign, nothing serious should happen to your machine using these files). Each and every spyware attempt was detected and prevented from running locally on my machine.

All in all I am quite happy in using Coranti and I like the way I am given defence in depth which is always a good thing to have nowadays as the sophistication of the criminal element is always improving and this provides an excellent line of defence against them.

MICHAEL MUNT

IPv6 Secure Transition Network Architecture

IPv6 has the capability to handle an astronomically large address space. IPv6 deployment, although, has been marginal and several less drastic solutions have been used to expand the address space of IPv4. The non-drastic solutions have reached the limit of what they are able to handle. The transition to IPv6 is imminent.

What you will learn…

- a description of an hypothetical Departmental network architecture,
- a review of the known IPv6 vulnerabilities and security, and
- a detailed examination of the IPv6 security aspect of the Departmental network architecture.

What you should know…

- basic knowledge about network architecture and IPv6,
- IPv6 routing, support protocols such Internet Control Message Protocol (ICMP) v6, Neighbor Discovery (ND) and Duplicate Address Detection (DAD), and
- network security.

The Internet has grown to a point where *Internet Protocol version 4* (IPv4) can't handle the large number of addresses created by that growth. The long term solution has been the replacement of IPv4 by *Internet Protocol version* 6 (IPv6), which has the capability to handle an astronomically large address space. Because of the difficulty to switch from one Internet protocol to another, IPv6 deployment has been marginal and several less drastic solutions have been used to expand the address space of IPv4. The non-drastic solutions, however, have reached the limit of what they are able to handle. It becomes difficult for an *Internet Service Provider* (ISP) to obtain blocks of IPv4 addresses for its subscribers. The transition to IPv6 is imminent, but progressive. Very likely, both versions of IP will cohabit for several years.

This feature examines, from a security point of view, the case of an hypothetical departmental network transiting from IPv4 to IPv4 and IPv6. The case, shown in Figure 1, is applicable to several organizations currently running IPv4 and planning a support of IPv6. The goals, in this case, are a partial transition to IPv6, support of external facing e-services over both IPv4 and IPv6 and ability to serve IPv4 and IPv6 clients on the Internet.

The network is structured into three successive zones: *Restricted Zone* (RZ), *Operations Zone* (OZ) and *Public Access Zone* (PAZ). Each zone is guarded by a firewall. Each firewall has two network interfaces and is responsible for the implementation and enforcement of network security administration rules between the two zones to which it is attached. In particular, it protects the first zone from threats coming from the second zone. The PAZ firewall plays the role of Departmental network edge firewall. It is assumed that the ISP provides IPv4 and IPv6 connectivity and mobility support is not required. The RZ consists of an IPv4-only network. It contains servers (such as storage networks and management servers) and client stations that need a high level of protection. Traffic is restricted, but the RZ is interfaced with the OZ. Servers within the RZ may be related to public servers, in the PAZ. The OZ is IPv4-only. It contains servers, as mail proxies, web severs and client stations (their users are department personnel). It is interfaced with the RZ and PAZ. Traffic transiting in the OZ is from internal sources and authorized external sources. The PAZ is an IPv4 and IPv6 zone. It contains external web servers and external *Domain Name System* (DNS) servers providing on-line services. The PAZ is interfaced with the OZ and Internet.

Aspects of IPv6 that are at risk are auto configuration, dynamic routing, dynamic address resolution, name resolution, ICMPv6 messages, extension headers and addressing. There are tools available for hardening IPv6 networks, such as IP security (IPsec), firewalls, *Secure Neighbour Discovery* (SEND), *Intrusion Prevention Systems* (IPSs) and

Intrusion Dectection Systems (IDSs). In principle, any implementation of IPv6, compliant to the standard, should support IPsec. There are a fairly good number of platforms supporting IPsec. IPv6 firewalls, IPSs, IDSs and implementations of SEND may not be ready or/and have the properties needed to secure IPv6 adequately. For instance, current implementations of SEND may solely be of demonstration type and may not be ready for a production environment. Firewalls may be able to filter ICMPv6 packets, but may not have the capability to exercise rate control, verify consistency of reply and request messages, and validate extension headers.

Dynamic configuration mechanisms of IPv6 facilitate the management of a network. If they cannot be secured properly, then it is best to disable them, because of the risks to the security they represent, and operate with static configuration, particularly for small scale IPv6 networks.

The risk level acceptability is different for each instance of this Departmental network. IPv6 security mechanisms should be selected according to the business requirements of a department and the outcomes of a threat and risk assessment. It is the goal of this feature to explore the different relevant IPv6 security issues and available countermeasures.

This feature contains an overview of IPv6 vulnerabilities, threats and security. Then strengths and weaknesses of the Departmental network architecture are examined. The threats to the security of the architecture are scrutinized and countermeasures that may be put in place to mitigate the risks associated with the security threats are discussed. A summary of the recommendations concludes the article.

Overview of IPv6 Vulnerabilities, Threats and Security

Threats to IPv4 security are also threats to IPv6 security. IPv6 networks can be secured with IPsec. In IPv6, support of IPsec is mandatory. The actual use of IPsec is, although, optional and marginal because its deployment and management are cumbersome. Without the actual use and deployment of IPsec, IPv6 and IPv4 are equally vulnerable. We hereafter focus on IPv6 specific vulnerabilities, attacks, threats and security.

IPv6 Threats

The main threats to IPv6 security are discussed in this subsection.

Attacks Due to a Lack of IPv6 Awareness

There are dual stack operating systems that come with an active IPv6 protocol entity, by default. When such systems are being installed, *Information Technology* (IT) network managers may be unaware that IPv6 is running in their network. Systems may also create IPv6 in IPv4 tunnels to reach IPv6 servers. Because of the lack of awareness of IPv6 activity, IT network managers may not protect their system adequately. IPv6 may not receive the same level of protection as IPv4. Unprotected IPv6 nodes may be victims of exploits. IPv6 nodes may also have errors and create network problems. A node, with IPv6 enabled by default, can be flipped into the IPv6 mode by an adversary on the same link, i.e., the IPv6 initialization and activation are invisible to the system manager.

Attacks Due to a Auto Configuration

Auto configuration of an IPv6 address is achieved by combining the network prefix with the *Media Access Control* (MAC) address of the network interface. MAC addresses can reveal the make and model of a computer. This can be exploited for hardware specific attacks and simplify network scanning, since it bounds the range of possible addresses. Moreover, auto configuration uses ICMPv6 messages for network prefix discovery and detection of duplicate IPv6 addresses. Adversaries, on the same network, may inject false ICMPv6 messages to subvert their victim.

Reconnaissance Attack

The goal of an adversary perpetrating a reconnaissance attack is to collect knowledge about the victim's network, topology and composition. The adversary may perform active scanning and use sources of information such as search engines and documents.

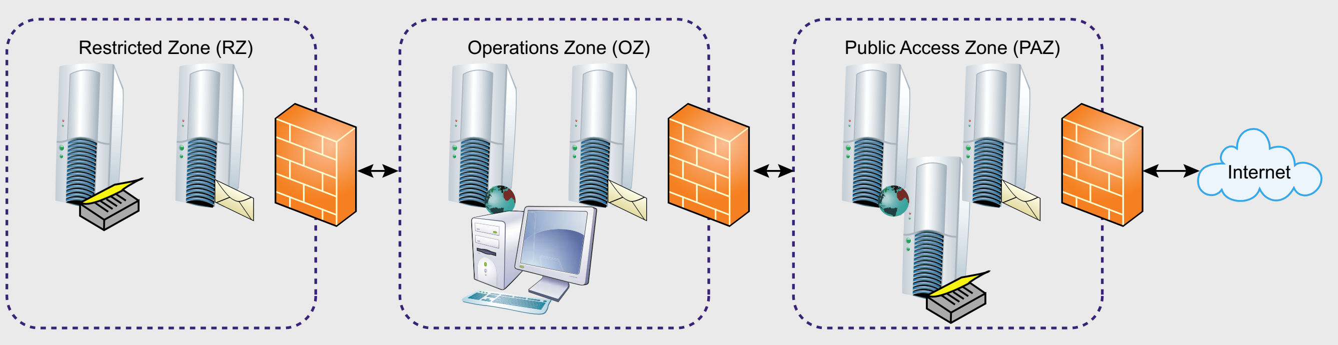


Figure 1. *Departmental network architecture*

Techniques devised for IPv4 transport layer-port scanning and application vulnerability scanning apply as well to IPv6. The main differences are in the identification of valid IPv6 addresses. In contrast to 32-bit IPv4 addresses, 128-bit IPv6 addresses make address scanning, with techniques such as ping sweep, theoretically 2 power 96 times more complex. The size of the default address space of an IPv6 subnet is 2 power 64 addresses, versus only 256 addresses for IPv4. Address scanning strategies devised for IPv4 don't scale up to IPv6. New strategies are being developed to address the challenge. New IPv6 multicast addresses make finding certain network elements easier such all *Dynamic Host Configuration Protocol* (DHCP) servers, routers and *Network Time Protocol* (NTP) servers. The use of a sequential numbering scheme also makes address scanning easier. An adversary may query a DNS to resolve the address of public servers. IPv6 numbering schemes based on the IPv4 addresses or hardware addresses may simplify the work of an adversary. For example, the adversary may reduce the range of addresses to scan by trying IPv6 addresses constructed using hardware addresses of popular network interface manufacturers. Because of the difficulty for users to work with long IPv6 addresses directly, it is expected that not only servers but hosts as well will be named and registered with a DNS, ideally internal. An adversary who successfully compromises the DNS may directly obtain the list of hosts and their IPv6 address. Along the same line, hosts and servers successfully compromised may return the content of their neighbor cache.

Router Advertisement Spoofing and Router Redirect Attack

Router Advertisements (RAs) are ICMPv6 messages sent using multicast to dynamically provide network prefixes and advertise gateways. The network prefixes may be used for auto configuration of IPv6 addresses. Spoofed RAs may be used by an adversary to provoke the (re)numbering of nodes with a wrong network prefix. They may also be used to carry on a man-in-the middle attack or hijack traffic. The victims may be denied access to desired destination networks.

The ICMPv6 Redirect message is sent by a router to inform about the existence of a better router to use to reach a destination. In the router redirect attack, the adversary forges and sends a false ICMPv6 Redirect message to its victim. The traffic of the victim is hijacked. This attack is an enabler for a man-in-the-middle attack.

Forged Neighbor Discovery Message

The ICMPv6 ND protocol is used for address resolution, which is dynamically mapping IPv6 addresses to hardware addresses. There are two types of ICMPv6 messages involved: *Neighbour Solicitation* (NS) and *Neighbour Advertisement* (NA). An adversary, attached to the same link as its victim(s), may forge NS or NA messages to confuse the normal operation of the ND protocol and to disrupt packet forwarding on a network. For instance, a NS message is sent by a node to determine if a self-configured IPv6 address is being used by another node on the network. An adversary, on the same network, may systematically and repeatedly reply positively using a NA message each time an address is tested. The victim is denied network access. NS messages are also sent, using multicast, to resolve the IPv6 address of a node to its hardware address. An adversary may inject a corresponding NA message mapping the IPv6 address to its own hardware address and hijack the traffic of the victim.

Extension Header Attack

An IPv6 packet may contain a chain of extension headers, inserted between the mandatory IPv6 header and transport layer header. There are destination option headers, interpreted solely by the final destination of a packet, and hop-by-hop headers, interpreted by all intermediary routers involved in the forwarding of a packet. Extension headers must be inserted according to strict protocol rules. Hop-by-hop extension headers should appear first in the chain of extension headers, while destination option headers should be placed last. Each type of hop-by-hop extension header can be inserted only once, while each type of destination option header can appear twice. An adversary may create long chains of extension headers to force fragmentation of packets. An adversary may also insert invalid extension headers. Both cases lead to extra work for routers and are forms of *Denial of Service* (DoS) attacks. With the Routing header 0 attack, an adversary may use and hide behind an intermediary node to reach another node on the same network. The Routing header 0 may be used to force routing of packets through certain nodes, cause the exhaustion of their resources and make their services unavailable. The Router Alert hop-by-hop header, processed by each router on a path from a source to a destination, might be used by an adversary to consume resources.

Attacks to Multicast Groups

IPv6 defines global multicast addresses for special groups of devices such as link-local addresses, site-local addresses and all site-local routers. Multicast amplification is a kind of DDOS attack. An ICMPv6 request requiring a response is sent to a multicast address. A large number of replies can potentially be returned. The IPv6 specification prohibits sending replies in response to ICMPv6 requests sent to IPv6 multicast addresses, except for the packet too big message. It is expected that most of the operating systems follow the specification. Besides, an adversary may send a message to force members to leave a multicast group.

DHCPv6 Spoofing

The adversary sends false advertisement and reply messages to its victims. For example, the adversary may supply a false default gateway address of a false DNS address. This attack is an enabler for a man-in-the-middle attack.

Worm Propagation

Worm propagation and vulnerable target detection by address probing are rendered more difficult in IPv6, with respect to IPv4, because of the large address space created by the 128-bit format. Theoretically, with respect to IPv4, the time complexity of address probing in IPv6 is multiplied by a factor of 2 power 96. Worms that don't use address probing and use other techniques, such as email, will not be affected by IPv6. To cut the search space and speed up address probing, worm propagation strategies can take advantage of local knowledge, patterns in address-space assignment and an IPv4-IPv6 dual stack environment.

DNS Attack

There are two kinds of DNS updates: publication of a name and an address for forward lookups and publication for reverse lookups. False updates may be inserted in a DNS. As a propagation strategy, a worm may query, with random strings, a DNS to uncover valid IP addresses.

IPv6 Security

As part of a transition to IPv6, a security plan is highly recommended. The plan should include security measures and protection elements. The use of IPsec can mitigate several threats. In principle, any implementation of IPv6, compliant to the standard, should support IPsec. There are actually a fairly good number of platforms supporting IPsec. When IPsec is not used, SEND can mitigate IPv6 address spoofing attacks. SEND uses cryptographically signed addresses and provides address ownership demonstration. Current implementations of SEND, however, may solely be of demonstration type and may not be ready for a production environment.

Major vendors of IPv6 hardware and software do publish the known vulnerabilities of their products. Systems must be maintained up-to-date with the latest security updates installed to address the known vulnerabilities. This reduces the likeliness of compromising host, router and server software.

Reconnaissance Attack Mitigation

To prevent reconnaissance attacks, internal multicast addresses, used to identify standard services such as DHCP and NTP, should be blocked at the network perimeter and not reachable from the outside. Non essential ICMPv6 messages should be blocked, such as inbound echo request and outbound echo reply messages. All other internal use addresses should also be blocked. When relevant, the IPv6 Privacy Extensions may be utilized to make identification of multiple addresses to the same node more difficult. This mechanism makes troubleshooting and tracing back a host more difficult because addresses are random and changed regularly (the extension a may be employed solely for nodes making external communications). When static addresses are needed for servers and gateways, it is best to use non standard and non obvious addresses.

DNS Attack Mitigation

DNS updates secured solely according to source address validation are not recommended, particularly when ingress filtering is not performed. The reverse+forward DNS check is also considered to be very weak. This consists of verifying that the reverse and forward DNS contents match, i.e., making sure that the name and IP address mutually point to each other and that the name is configured and corresponds to a domain. A mechanism for update origin authentication must be in place. The mechanism must be based on shared secrets or public-private keys. A security association may be needed between the DNS and each node. In cases where periodic address generation is used such as when SEND is used, then additional load for the DNS may be expected. IPsec or DNS Security (DNSSec) may be considered to secure communications with a DNS. DNSSec is an extension that may be used to sign DNS queries and replies. There are platforms supporting DNSSec, but so far its deployment seems to have been marginal. Alternatively, all DNS updates could be done manually and entered in static tables.

Firewalls

IPv6 firewalls are available. They support separate sets of policies for IPv6. Tasks typically performed by an IPv6 firewall include address-based packet filtering, ICMPv6 message filtering and validation of packets with extension headers. However, IPv6 firewalls do not have a level of maturity equivalent to IPv4 firewalls. Network edge firewalls are required to protect the network from external attacks. Personal firewalls are needed to protect hosts and servers from insider attacks.

An adversary can bypass packet filtering of an IPv6 network using IPsec encrypted packets. To address this issue, the distributed firewall architecture has been introduced. It handles ICMPv6 threats and active web threats. The architecture consists of network firewalls, host firewalls and a policy centre. The network firewalls do packet filtering according to rules on addresses, port numbers and protocols. Host firewalls perform packet filtering by inspecting their content and finding matches with patterns defined by rules. Filtering rules are defined and provided to firewalls by the policy centre.

Intrusion Prevention and Detection Systems

Intrusion Prevention Systems (IPSs) are being developed for IPv6. Few signatures are available. IDSs have also been developed to detect suspicious ND protocol messages.

DoS and DDoS Attack Mitigation

Regarding DoS and *Distributed Denial of Service* (DDoS) attacks, the challenge is pinpointing the nodes perpetrating the aggression. Adversaries committing DDoS attacks hide using spoofed IP addresses. The traceback problem consists of finding the true source of an IP packet. The Unicast Reverse Path Forwarding (uRFP) mechanism, when supported, makes possible traceback and verification of an IP source address. The uRFP mechanism is also useful to traceback sources of malware attacks (e.g., viruses, worms). The source of an IP address can be traced back to the node, in the best case, or the subnet, in case privacy addressing is used.

Inbound and outbound packet filtering, based on IP source address, mitigates the risk of DoS attacks. Collaboration with the ISP is recommended to develop a plan for containing and pinpointing the source of DoS and DDoS attacks. The plan should contain contact information and a traceback procedure. However, because of the huge number of sources that may be involved in a DDoS attack, pinpointing all sources is considered to be a difficult problem. There seems to be no efficient way to deal with the problem at this time.

Worm Attack Mitigation

Regarding worm propagation, a honeypot-based strategy may be employed. A honeypot is a dummy DNS server that doesn't reply to queries, provokes their retransmission and introduces delays in worm propagation, assuming the worms aren't aware of the dummy DNS servers.

Transition Techniques

There are three IPv4 to IPv6 transition techniques, namely, dual stack, tunneling and translation. Each technique has its own benefit(s), downside(s) and security vulnerabilities.

Dual stack

A dual stack system runs simultaneously both IPv4 and IPv6, together with their corresponding support protocols such as *Address Resolution Protocol* (ARP), ICMP and ICMPv6. Each application can push its data units to any of IPv4 or IPv6. The system can receive and handle both IPv4 and IPv6 traffic.The main benefit of the dual stack technique is that IPv6 can be used to communicate with an IPv6 node while IPv4 can be used to communicate with an IPv4 node. There is neither data translation nor transformation involved. Most of the recent operating systems run dual stack by default. Client operating systems give preference to IPv6 for communicating with a server, when both versions are available. In principle, a dual IP network layer is transparent to most of the applications, unless they have to process and look at the format of IP addresses (for instance, if they have to create log entries). When relevant, it is although best to test applications for compatibility with a dual IP stack.

The downsides of the dual stack technique are that servers need to store two routing tables, one for each version, run two routing protocols and manage two sets of timers. The main vulnerability of dual stack is the lack of IPv6 awareness. Indeed, there are dual stack operating systems that come with an active IPv6 protocol entity, by default. When such systems are being installed, IT network managers may be unaware that IPv6 is running in their network. Systems may also create IPv6 in IPv4 tunnels to reach IPv6 servers. Because of the lack of awareness of IPv6 activity, IT network managers may not protect their system adequately. Worm propagation may be facilitated by

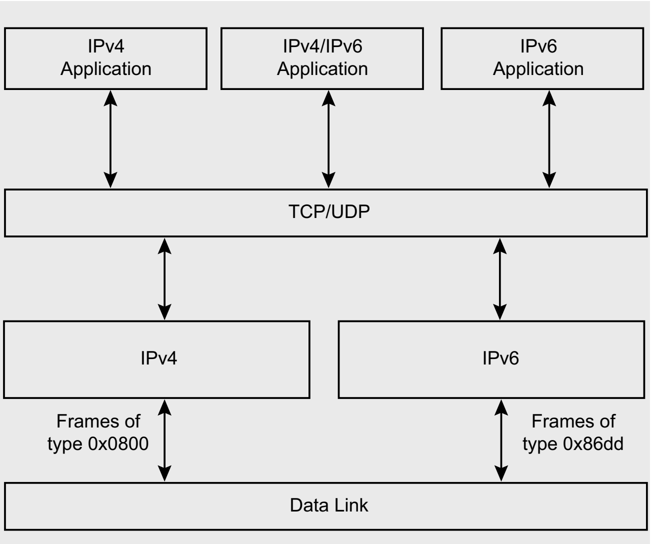


Figure 2. *IPv4 and IPv6 dual stack*

an IPv4-IPv6 dual stack environment. A node running both IPv4 and IPv6 is vulnerable to attacks targeting either or both protocols. To prevent insider attacks, each dual stack node must run both a personal IPv4 firewall and a personal IPv6 firewall, to be discussed in the sequel. Moreover, the addition of new code in a protocol stack to support IPv6 potentially adds new bugs and new software security vulnerabilities. In a dual stack environment, for the sake of simplicity network administrators may be mapping the IPv4 addresses to IPv6 addresses (in particular for the last byte of each address). This strategy makes, for an adversary, network scanning simpler.

Dual stack is the preferred transition technique because a server can utilize IPv6 to communicate with an IPv6 client while IPv4 can be employed to communicate with an IPv4 client. The technique is illustrated in Figure 2. The network layer contains both an IPv4 protocol entity and an IPv6 protocol entity. Ethernet frames of type 0x0800 are de-multiplexed towards the IPv4 protocol entity. Frames of type 0x86dd are de-multiplexed towards the IPv6 protocol entity.

Transport protocols, originally built for IPv4, may need to be revised, to run seamlessly over IPv6 (a task normally completed by the operating system vendor). For instance, when *User Datagram Protocol* (UDP) runs over IPv6, the checksum is mandatory, whereas it isn't over IPv4. The method used to compute the checksum for IPv6 has been changed.

To run seamlessly in IPv6, applications originally designed for IPv4 that manipulate IP addresses (for example, for logging purposes) need to be revised to support the new address format of IPv6 (a task normally performed by the maintainers of the applications).

Tunneling

Tunneling exists for two reasons. During the transition period, there will be IPv6 systems and subnets that will need to communicate together through IPv4-only partitions of the Internet. In such cases, IPv6 packets are encapsulated in IPv4 packets and sent using tunneling from IPv6 subnet to IPv6 subnet. Also, there will be IPv4-only systems and subnets, not yet upgraded to IPv6 that will need to communicate through IPv6-only portions of the Internet. In such cases, IPv4 packets are encapsulated in IPv6 packets and sent using tunneling from IPv4 subnet to IPv4 subnet. The downside of tunneling is the overhead that it creates. Overhead due to headers is doubled because each packet needs to be encapsulated into another packet. On the security side, the specific tunneling techniques have no built-in security mechanisms such as authentication, integrity protection and confidentiality. They are vulnerable to the traffic injection and traffic sniffing attacks.

Translation

Translation is helpful when an IPv6 node needs to communicate with an IPv4 node, or vice versa. Four aspects need translation: addresses, packets, error messages (i.e., ICMP) and DNS queries. The problem is challenging and has not been entirely solved. Insuring end-to-end security has been difficult to achieve and has not been obtained with solutions proposed so far, i.e., *Network Address Translation – Protocol Translation* (NAT-PT). Attacks such as reflection, pool depletion and application level gateway CPU attacks have been documented. There are translation techniques still under development. These may have vulnerabilities. Translation boxes are functionally similar to routers and share their vulnerabilities. Not all vulnerabilities of translation mechanisms are known at this time. It is best to consider security of translation techniques as an open problem. That being said, translation might be needed, for instance, between IPv6 proxy servers and IPv4 servers. The technique that seems to most suitable is Framework for IPv4/IPv6 Translation that is being drafted by the *Internet Engineering Task Force* (IETF). With this technique, there is no need to modify software in servers. A translation box bridges the IPv6 and IPv4 worlds. Application level translators, i.e., *Application Level Gateway* (ALG), apart from being functionally limited to one application may add new software vulnerabilities in their host system.

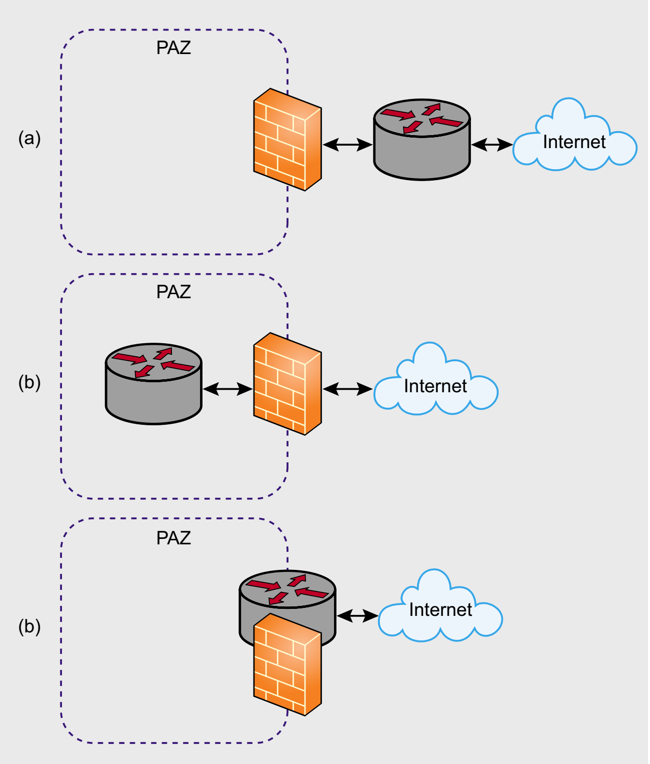


Figure 3. *Firewall-access router relative placement alternatives: (a) Internet-router-firewall-protected, (b) Internet-firewall-router protected and (c) Internet-edge protected*

Strengths and Weaknesses of the Architecture

The Departmental network architecture is examined according to known security risks.

Address Configuration

Dual stack operation has an impact on the network architecture. Each dual stack system must have an IPv6 address for each of its IPv6 interface. Addresses of servers in the PAZ must be globally routable. The addresses can be statically configured or auto configured. Static address configuration is done by human operators. There are two auto configuration options: stateful and stateless. Stateful auto configuration requires deployment of a DHCPv6 server. Upon request, the DHCPv6 server supplies addresses to nodes. It also keeps track of address leases. Leases eventually expire and addresses have to be granted again for new time intervals. Stateful auto configuration requires securing and maintaining a DHCPv6 server, i.e., using IPsec. Stateless auto configuration of an IPv6 address is achieved by combining the network prefix with the MAC address of the interface. Stateless auto configuration can be secured with IPsec, but given the small number of nodes in the PAZ, static address configuration is recommended. This means that the protocol elements for stateful and stateless auto configuration are not needed and should be disabled. They include the ND protocol, DAD and related ICMPv6 messages (e.g., NS, NA, *Router Solicitation* (RS) and RA).

Address Resolution

Address resolution consists of mapping IP addresses to hardware addresses. This function is essential for the operation of a network. It can be done using either permanent table entries, of IP address to hardware address mappings, or dynamically, using an address resolution protocol known as ARP in IPv4. In IPv6, the ND protocol is used for that purpose. Given the small number of IPv6 nodes in the PAZ, it is best to go with permanent table entries to avoid the vulnerabilities of ND. Alternatively, ND can be secured with IPsec.

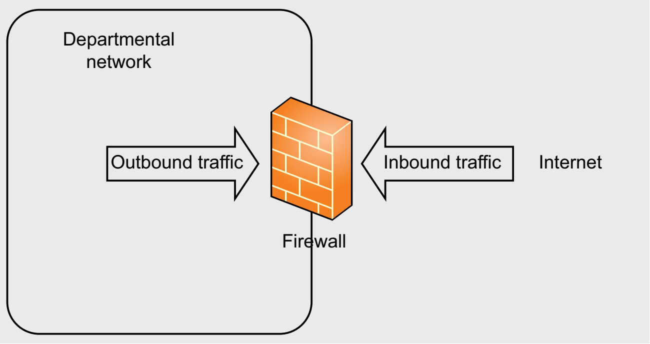


Figure 4. *Outbound and inbound traffic*

Name Service (DNS)

Dual stack operation requires DNS support for name resolution to both IPv4 address and IPv6 address. A name to IPv4 address biding is stored in a record of type *A* in a DNS. A name to IPv6 address binding is stored in a record of type *AAAA*. The records must be stored to favour resolution of *AAAA* records first. For each dual stack system, both records are required. Clients may formulate requests for either record of both of them. To prevent reconnaissance attacks, the dual stack DNS of the PAZ must contain entries only for public servers in the PAZ. Given the small number of IPv6 nodes in the PAZ, it is best to avoid dynamic updates, and their vulnerabilities, and operate with static DNS entries. Alternatively, dynamic DNS updates can be secured with IPsec. The use of DNSSec may also be considered.

Firewalls

A firewall can operate at three different network architecture levels, i.e., network, transport and application. At the network level, it does packet filtering. At the transport level, it performs TCP segment and UDP datagram filtering. At the application level, it does proxy functionalities. At both the transport and application levels, a firewall is expected to be independent of the IP version. The additional IPv6 firewall protection required above any current IPv4 protection is discussed hereafter. Aspects that are examined are firewall-access router relative placement, address filtering, ICMPv6 message filtering, validation of extension headers and filtering of tunneled packets.

Firewall Placement

The PAZ firewall must be placed as close as possible to the access router (the router connecting the PAZ to the Internet), to block the undesired traffic as near as

Table 1. *Edge firewall IPv6 address-based packet filtering*

Permitted traffic	
Outbound (i.e., egress filtering)	Inbound (i.e., ingress filteting)
Source address using the PAZ IPv6 address range	Destination address using the PAZ IPv6 address range
Blocked Traffic	
Outbound (i.e., egress filtering)	Inbound (i.e., ingress filtering)
Destination address using the PAZ IPv6 address range Destination nonexistent on the Internet Multicast destination address Destination address is IANA reserved Source address not using the PAZ IPv6 address range	Source address using the PAZ IPv6 address range Source address nonexistent on the Internet Source multicast address Source address is IANA reserved

possible from its source. There are three alternatives: Internet-router-firewall-protected, Internet-firewall-router protected and Internet-edge protected. The alternatives are depicted in Figure 3. Each alternative affects the definition of the firewall rules.

With the Internet-router-firewall-protected architecture, the router is outside the PAZ, between the firewall and the Internet. Assuming static address configuration and no need for multicast support beyond the PAZ, operation with this architecture requires firewall rules permitting interactions between the nodes in the PAZ and router. RSs from the PAZ and RAs from the router must be permitted, unless the router is statistically configured in the nodes in the PAZ. If the router runs a dynamic routing protocol, then the firewall must block the related packets (note that this may be hard to do if IPsec is used to secure the routing protocol, because of the concealment of the routing messages). The advantage of this alternative is that the firewall function and router function are assigned to two different machines. Hence, the load is balanced. The downsides are the need of two network elements and, because it is not behind the firewall, the router doesn't benefit from its protection. Moreover, additional configuration is required in the firewall, i.e., definition of rules, if control messages need to be exchanged between the router and nodes in the PAZ.

In the Internet-firewall-router protected architecture, the router is inside the PAZ, behind the firewall. As in the previous case, if the router runs a dynamic routing protocol, then the firewall must have rules blocking the related packets. Assuming static address configuration in the PAZ, generation of NA and NS messages should be blocked within the PAZ. Alternatively, routing may be static or done by the *Border Gateway Protocol* (BGP) (which messages are secured with MD5 signatures). With this alternative, the firewall and router functions are assigned to two different machines and the load is balanced. The router benefits from the protection of the firewall. The downside is that two network elements need to be maintained.

Table 2. *Edge firewall filtering of ICMPv6 messages*

	Rule	
ICMPv6 Message	Outbound	Inbound
Destination Unreachable (Type 1)	Block	Permit, if it is a reply to an IPv6 debugging packet
Packet Too Big (Type 2)	Permit if PAZ MTU smaller than ISP MTU	Permit for path MTU discovery
Time Exceeded (Type 3)	Permit	
Parameter Problem (Type 4)	Permit	
Echo Request (Type 128) and Echo Reply (Type 129)	Permit & rate control	Permit & rate control, but solely for PAZ IPv6 services
Listener Query (Type 130), Listener Report (Type 130), Listener Report v2 (Type 132) and Listener Done (Type 143)	Block	
Router Solicitation (Type 133) and Router Advertisement (Type 134)	Block (assuming static address and router configuration)	
Neighbour Solicitation (Type 135) and Neighbour Advertisement	Block	
Redirect (Type 137)	Block	
Router Renumbering (Type 138)	Block	
Node information query (Type 139) and reply (Type 140)	Block	
Inverse Neighbor Discovery Solicitation (Type 141) and Inverse Neighbor Discovery Advertisement (Type 142)	Block	
Home Agent Address Discovery Request (Type 144), Home Agent Address Discovery Reply (Type 145), Mobile Prefix Solicitation (Type 146) and Mobile Prefix Advertisement (Type 147)	Block	
Certificate Path Solicitation (Type 148) and Certificate Path Advertisement (Type 149)	Block	
Seamoby Experimental (Type 150)	Block	
Multicast Router Advertisement (Type 151), Multicast Router Solicitation (Type 152) and Multicast Router Termination (Type 153)	Block	

In the Internet-edge protected architecture, the router and firewall functions are done by the same device. A single network element is required. This is adapted to a small scale network. In a large scale network, the concentration of the routing and firewall functions may create too much load for a single device. The firewall must have rules blocking the RS and RA messages. It may have to permit routing messages, if the router needs to interact with other routers on the Internet. The router may be statistically configured in the nodes of the PAZ. Assuming that address auto configuration is not used, there is no need for RS and RA messages.

The Internet-edge protected model is the preferred firewall placement alternative for the Departmental network. The first two alternatives may be considered in future larger scale versions of the architecture.

Address Filtering

Each IPv6 packet contains a source address and a destination address. The source address indicates the origin of the packet, while the destination address points to the target. IPv6 address-based packet filtering rules are summarized Table 1. Outbound packets are from the PAZ, while inbound packets are from the Internet, see Figure 4. Outbound packets with source addresses using the PAZ IPv6 address range are permitted. Inbound packets with destination addresses using the PAZ IPv6 address range are permitted. Outbound packets with destination addresses using the PAZ IPv6 address range must be blocked. Inbound packets with source addresses using the PAZ IPv6 address range (packet spoofing indications) must be blocked. The RZ, OZ and PAZ firewalls must perform ingress filtering to prevent address spoofing attacks. It means that outbound packets with source addresses that do not belong to nodes in the RZ, OZ or PAZ should be blocked.

Bogons are packets to destinations or from sources that are nonexistent on the Internet. The firewalls must block bogons. Ranges of currently allocated IPv6 addresses, subject to updates, are available. There are also ranges of IPv6 addresses that must be blocked by firewalls for miscellaneous reasons.

Assuming that no applications in the PAZ require IPv6 multicast, packets with multicast IPv6 destination addresses (`ff00::/8`) must be blocked. Any packet with a source multicast address does not make sense and should be blocked. There is also a list of *Internet Assigned Number Authority* (IANA) addresses reserved for future use. They should never appear as source or destination addresses. Packets using theses addresses must be blocked.

Table 3. *Personal firewall filtering of ICMPv6 messages*

	Rule	
ICMPv6 Message	Outbound	Inbound
Echo Request (Type 128)	Permit	Block
Echo Reply (Type 129)	Block	Permit

Table 4. *IPv6 server-level traffic filtering*

Permitted traffic	
Outbound/Inbound	
Traffic the servers are listening on	
Blocked traffic	
Outbound (i.e., egress filtering)	Inbound (i.e., ingress filtering)
Packets with Routing Header type 0 (RH0) Packets with non well-formed extension headers Tunnelled packets Destination nonexistent on the Internet Destination address listed in Annex A Multicast destination address Destination address is IANA reserved	Source address is loopback interface Source address assigned to one of own interface Packets with Routing Header type 0 (RH0) Packets with non well-formed extension headers Tunnelled packets Source address nonexistent on the Internet Source address listed in Annex A Source multicast address Source address is IANA reserved

Filtering of ICMPv6 Messages

ICMPv6 is used to exchange error or condition reports between IPv6 peers. Recommendations for filtering ICMPv6 messages in firewalls in the Departmental network are summarized in Table 2.

Limiting the rate of ICMPv6 messages is recommended recommended, in particular the unauthenticated ones (e.g., using a token-bucket function). High rate of erroneous messages may be used by DoS attack or probing attack perpetrators (i.e., DoS attack to a multicast source). They may also result from errors in the formation of IP packets. ICMPv6 message origin authentication is possible using the Authentication Header or Encapsulating Security Payload Header of IPsec. ICMPv6 message confidentiality is possible using the Encapsulating Security Payload Header. They both mitigate the risks of the following attacks: source address spoofing, message redirection and message tampering. That being said, it is impossible to establish security associations with all possible sources of ICMPv6 messages. A site can expect to receive error and other messages from any location on the Internet. Malicious users may potentially use ICMPv6 messages for traversing firewalls, bypassing administrative inspection. It is possible to carry out a covert conversation using the payload of ICMPv6 error messages or tunnel inappropriate encapsulated

IP packets in ICMPv6 error messages. Deep packet inspection may ensure that the payload of ICMPv6 messages is associated with legitimate traffic.

Extension Headers and Tunneled Packet

Firewalls must verify that chains of extension headers are well formed and follow the rules of the IPv6 protocol. Note that at this time, not all firewalls have the capability to check all rules, particularly the ones that apply to several extension headers at the same time. Packets with unknown extension headers should be blocked. Firewalls must block any packet with a Routing Header type 0 to prevent the attack with the same name. Packets with a Router Alter option should be blocked. Packets with a Routing Header type 2 should also be blocked. The Routing Header 2 is used for mobility support, which is assumed to be not required in the Departmental network.

The tunneling transition technique is not used in the Departmental network. All IPv6 in IPv4 tunnelled traffic must be blocked.

Packet Fragmentation

IPv6 fragments destined to an internetworking device should be blocked. IPv6 requires link *Maximum Transmission Units* (MTUs) to be larger than or equal to 1280 bytes. There is no reason for an IPv6 fragment to be smaller than 1280 bytes (except for the last fragment of a sequence). Firewalls must block all fragments with less than 1280 bytes, except the last fragment in a sequence. All fragments should be delivered within 60 seconds, or be blocked. Fragmentation can be used to obfuscate the content of packets to IDSs and IPSs. The capabilities of IDSs and IPSs, to analyze IPv6 fragmented packets, need to be investigated.

Server Security

Server security already exists in IPv4 networks and is still required in IPv6 networks. Securing servers requires keeping their operating system up-to-date with patches, disabling non useful processes listening on TCP or UDP ports and disabling packet forwarding. Specifically regarding IPv6, server-level filtering of ICMPv6 messages must be exercised, using a personal firewall. Table 3 presents personal firewall ICMPv6 packet filtering rules recommended for IPv6 servers placed in the PAZ. With respect to edge firewall rules (Table 2), they differ regarding the handling of the Echo Request and Echo Reply messages. Solely the differences are listed in Table 3.

Even though packet filtering is done by edge firewalls, it is recommended to have packet filtering in personal firewalls (both outbound and inbound) to mitigate

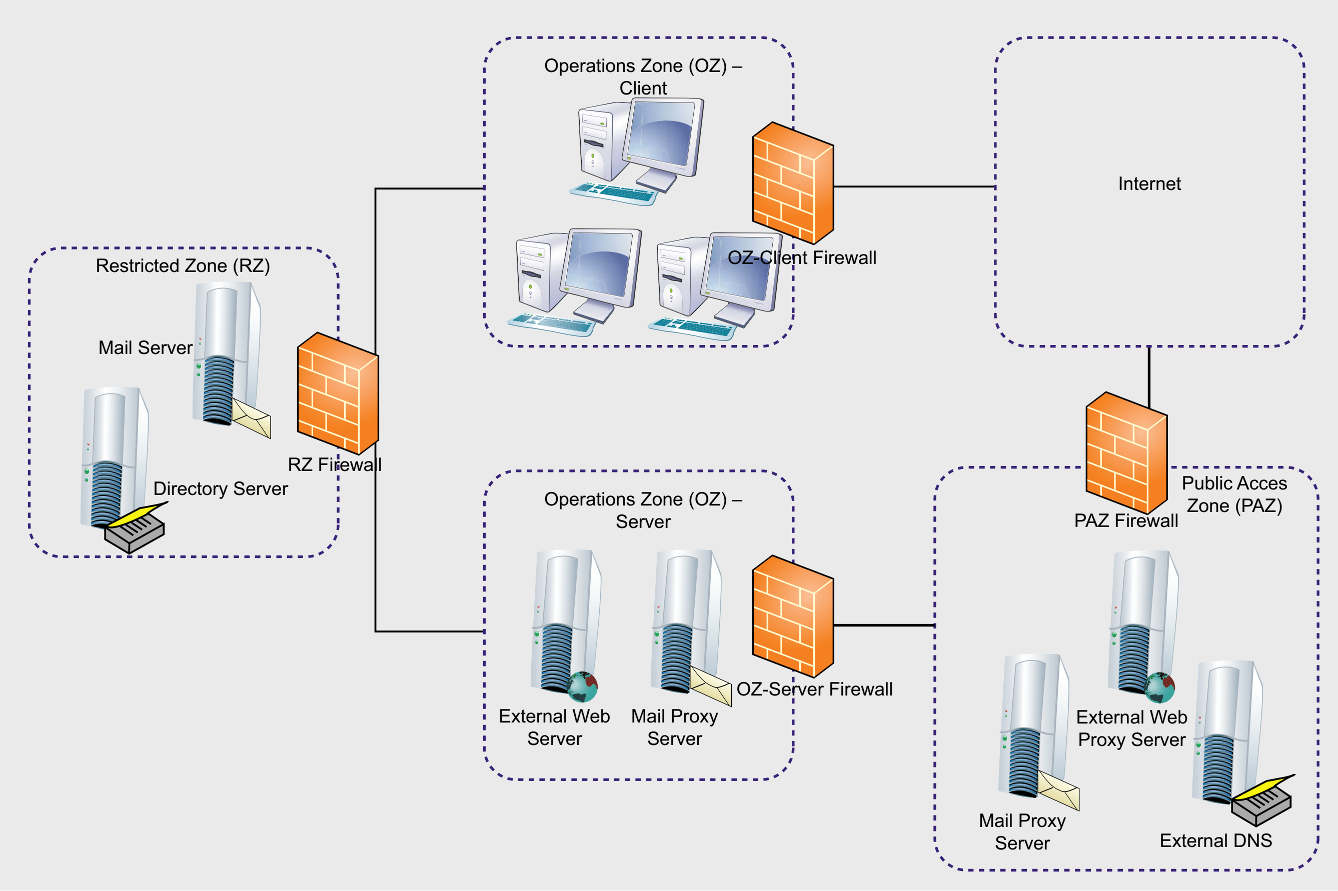


Figure 5. *Network architecture with separate client and server zones*

the Trojan horse threat. Server-level traffic filtering is summarized in Table 4. The servers accept all the traffic associated to the services that they are running, i.e., the TCP and UDP ports that are listening on. Bogons should be blocked. Packets with the Routing Header type 0 should be dropped. Not well formed packets, with respect to extension headers, should be rejected. Tunnelled packets should be blocked. There is no need for IPv6 tunneling in the Departmental network. Tunnels may create backdoors for adversaries. Some operating systems may create automatically IPv6 tunnels. It is best to verify that no tunnels are being created by the operating system. Packets in which the source address is the one of the loopback interfaces or belongs to one of its own interface must be blocked.

Zoning

Network security zones can be defined according to the principle of resource separation. Following this principle, a security zone must group together resources that are similar. In this context, similarity means equivalence in security attributes, potential vulnerabilities and degree of acceptable risk. The goal being that if a zone is compromised, the other zones will maintain their integrity.

The principle of resource separation dictates the division of client nodes and server nodes into different zones in the Departmental network. They are different with respect to their vulnerability to malware and the impact of such attacks. Malware and worms, in particular, propagate autonomously. Worms cause harm to network, such as consuming the bandwidth by increasing substantially the network traffic. They perform malicious actions such as deleting files, sending spam emails or installing backdoors. Client stations are at risk of malware infection through operations made by users such as reading emails, inserting USB memory sticks, downloading content from web sites, file sharing, instant messaging and peer-to-peer applications. Servers are at risk of malware infection through the Internet and exploitation of buffer overflows. Once successfully installed on a system, worms try to propagate and infect other systems, typically according to the following model: reconnaissance of available systems, scan for software vulnerabilities, attack new systems and spread again. Worm propagation can be mitigated with virus detection software running on nodes and an IPS at the edge of the network. An IDS may also be run to detect anomalously high traffic generated by worms. It is expected that worms will use more and more sophisticated propagation strategies. For instance, a worm may first infect IPv4 nodes, listen for IPv6 traffic to discover addresses of IPv6 nodes and exploit their vulnerabilities. Hence, it is best to separate IPv4 and IPv6 nodes.

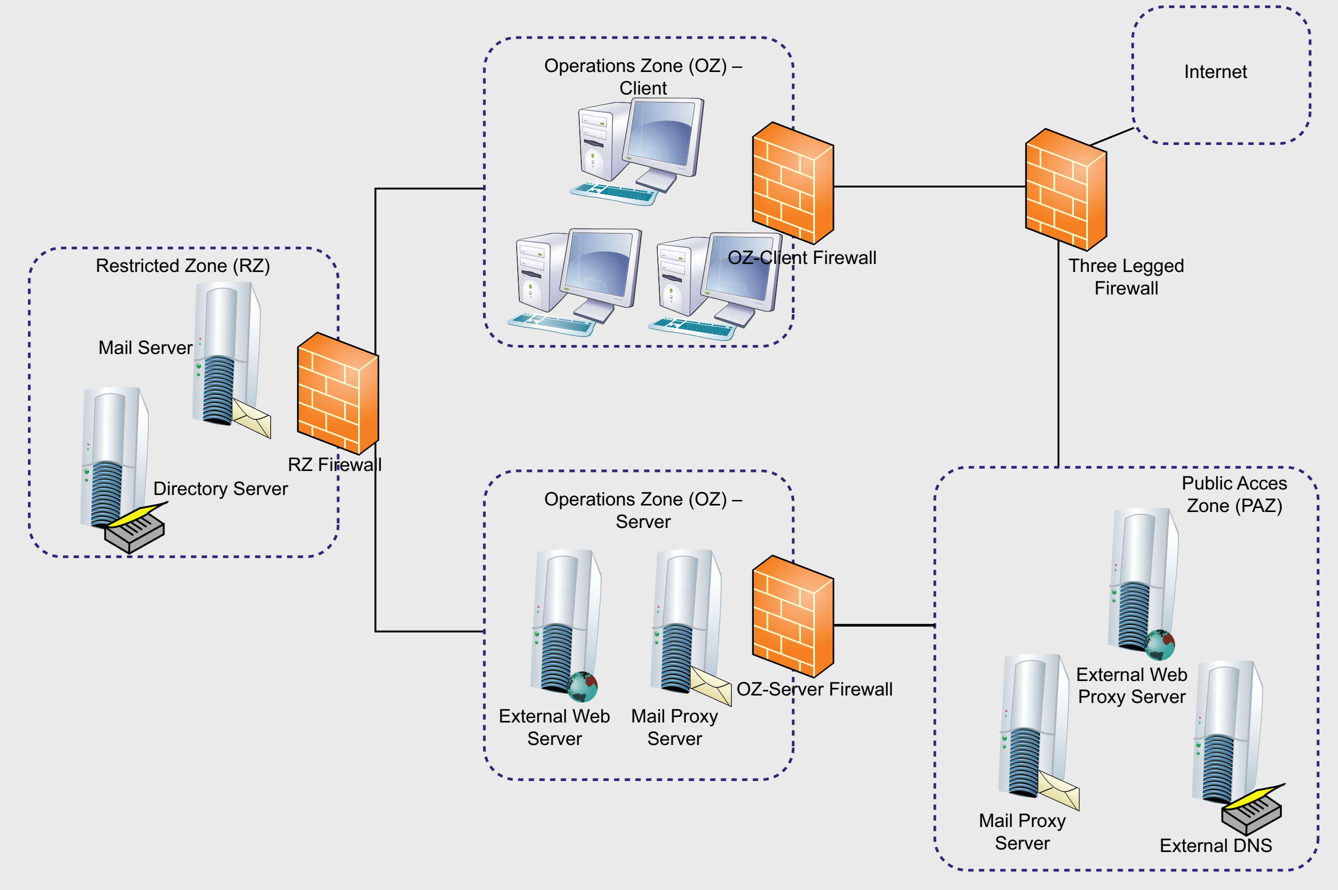


Figure 6. *Network architecture with a three-legged edge firewall*

Client workstations and servers do not have equivalent security attributes and degree of acceptable risk with respect to malware. Worms infect client stations more easily than servers, because of the higher number of propagation vehicles.

However, their impact is considerably higher on an infected server, than on an infected client station, because of the amount of data and number of users involved.

Besides, malware may be exploiting vulnerabilities of client stations then propagate to other nodes, including servers, on a local network. It is best to put in place a barrier to malware propagation between client stations and servers. Servers would be better protected against malware attacks.

In the Departmental network architecture pictured in Figure 1, client stations are placed together with a mail proxy server and an external web server in the same zone, i.e., the OZ.

This model is vulnerable to attacks by malware exploiting first vulnerabilities of client stations then vulnerabilities of servers. There is no barrier between these two classes of nodes. In case a worm attack on the client stations succeeds, network traffic may increase substantially within the OZ. The traffic between the PAZ and OZ and PAZ and RZ will not flow normally and affect the performance of the servers placed in the PAZ.

It is best to separate client stations and servers in different zones such that they don't have direct link access to each other and are isolated by a firewall. Figure 5 pictures a network architecture where the clients and servers are placed in different zones, don't see each other directly and are isolated by firewalls. All clients are placed in the OZ-Client. The OZ-Server contains solely servers.

An alternative design is pictured in Figure 6. A three-legged edge firewall bridges the Internet and both the PAZ and OZ-Client. The firewall has three interfaces. To be equivalent to Figure 5, the firewall must perform four-way filtering: Internet to PAZ, Internet to OZ-Client, OZ-Client to PAZ and PAZ to OZ-Client. The advantage of this version is that there is only one firewall box. The downsides are that the three legged firewall has complex filtering rules, is a single point of failure and must handle all the traffic.

Table 5. *Threats and mitigation*

Threat	Mitigation
Attacks enabled by a lack of IPv6 awareness	Deactivate IPv6 when not required Use a traffic analyzer to detect undesired IPv6 traffic Block all frames of type of type 0x86dd from a network where IP6 is not required (i.e., from the RZ and OZ)
Attacks due to auto configuration	Disable auto configuration, use static addresses and block related ICMPv6 messages or Secure ICMPv6 messages (ND and DAD) with IPsec and Edge firewall (ICMPv6 message filtering), personal firewall
Reconnaissance attack	Edge firewall (ICMPv6 message filtering), personal firewall, IPsec, DNSSec and SEND Use non standard and non obvious addresses
Router advertisement spoofing	Block RAs and use static routing tables and static IP addresses IPsec
Forged neighbour discovery message	Disable the ND protocol and use static IPv6 to hardware address tables Secure ND with IPsec or send SEND
Extension header attack	Edge firewall and personal firewall
Attack to multicast group	Block replies to ICMPv6 requests destined to multicast groups Multicast Security (MSEC) (if multicast groups are used)
Router redirect attack	Edge firewall and personal firewall
DHCPv6 spoofing	Disable DHCPv6 and use static addresses or use auto Secure DHCPv6 with IPsec
Worm attack	IDS, IPS, personal firewall, software maintenance, zoning and honeypot
DNS attack	Secure DNS updates (origin authentication) with IPsec or DNSSec Disable updates through the network and perform them manually
IPv6 address spoofing	Edge firewall and personal firewall (source address filtering) IPsec, SEND
Insider attack	Personal firewall
DoS and DDoS attack	Edge firewall and personal firewall (source address filtering, rate control ICMPv6 messages) Collaboration with ISP uRFP
Trojan horse	Personal firewall

Conclusion

The aspects of IPv6 that are at risk are auto configuration, dynamic routing, dynamic address resolution, name resolution, ICMPv6 messages, extension headers and addressing. There are conceptual tools available for hardening IPv6 networks, such as IPsec, firewalls, SEND, IPSs and IDSs.

Table 5 provides a summary of the threats and relate them to the mechanisms that can be used for their mitigation. For each case, the preferred mitigation for the Departmental network is underlined. The edge firewall and personal firewalls play an important role in the protection of the network.

The availability of IPv6 firewalls, IPSs, IDSs and implementations of SEND and the evaluation of their exact capabilities need to be clarified by further investigation. For instance, firewalls may be able to filter ICMPv6 packets, but may not have the capability to exercise rate control, verify consistency of reply and request messages and validate extension headers.

Acronyms

ALG	Application Level Gateway
ARP	Address Resolution Protocol
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSec	DNS Security
DoS	Denial of Service
DDoS	Distributed Denial of Service
DAD	Duplicate Address Detection
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPS	Intrusion Prevention System
IPsec	IP Security
ISP	Internet Service Provider
IT	Information Technology
MAC	Media Access Control
MSEC	Multicast Security
MTU	Maximum Transmission Unit
NA	Neighbour Advertisement
NAT-PT	Network Address Translation – Protocol Translation
ND	Neighbour Discovery
NS	Neighbour Solicitation
NTP	Network Time Protocol
OZ	Operations Zone
PAZ	Public Access Zone
RA	Router Advertisement
RS	Router Solicitation
RZ	Restricted Zone
SEND	Secure Neighbour Discovery
TCP	Transmission Control Protocol
uRFP	Unicast Reverse Path Forwarding
UDP	User Datagram Protocol

Dynamic configuration mechanisms of IPv6 facilitate the management of a network. If they cannot be secured properly, then it is best to disable them, because of the risks to the security they represent, and operate with static configuration. Static configuration makes sense particularly for small scale IPv6 networks.

The main recommendations are as follows:

- Test all relevant applications for compatibility with a dual IP stack.
- Structure the network into security zones grouping together resources that are equivalent in security attributes, potential vulnerabilities and degree of acceptable risk. Put client stations and servers in different zones, in accordance to the principle of resource separation. Avoid placing client stations on a path between proxies and their server.
- Disable all IPv6 protocol elements in the RZ and OZ. Use a traffic analyzer to insure that no IPv6 traffic is flowing in these zones.
- Deploy personal firewalls and an IPS for the mitigation of malware propagation. Maintain all systems up-to-date. Deploy an IDS for malware attack detection.
- Use static address configuration to avoid the risk associated with the use of auto configuration and ND (considering the small number of IPv6 nodes in the PAZ). Alternatively, secure DHCPv6, ND and DAD with IPsec.
- Use permanent hostname to Ethernet address resolution entries. Alternatively, secure ND with IPsec.
- Use static DNS entries to avoid the risk associated with dynamic DNS updates (considering the small number of IPv6 nodes in the PAZ). Alternatively, secure dynamic DNS updates with IPsec. Favour name resolution to IPv6 address in priority, i.e., the AAAA records.
- Use the Internet-edge protected edge firewall placement model in the Departmental network architecture. Considered the Internet-router-firewall-protected and Internet-firewall-router protected models for larger scale versions of the architecture.
- Deploy an IPv6 firewall which capabilities include IPv6 address-based packet filtering, ICMPv6 message filtering and well-formed packet validation (in particular the extension headers).
- Run a personal firewall on each server, for insider attack prevention and mitigation.
- Elaborate a reaction plan with the ISP to mitigate the impact of DoS and DDos attacks (the plan should contain at least contact information and a traceback procedure).

On the net

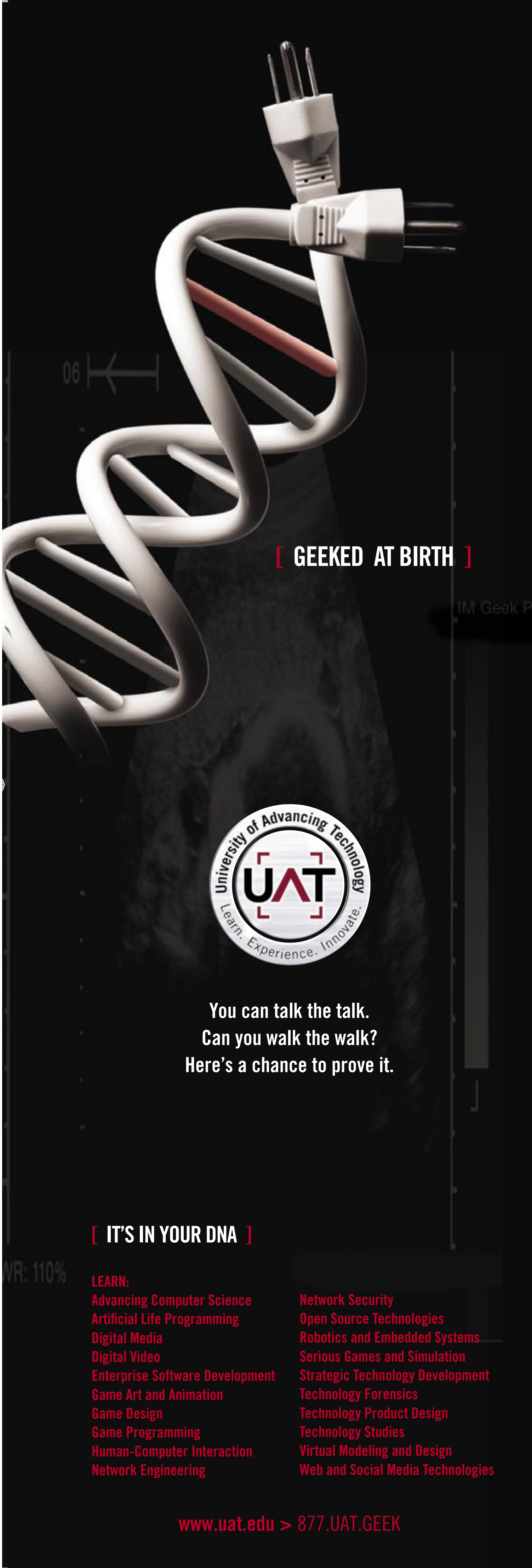
Visit the IETF web site (*www.ietf.org*) for all details about the IPv6 protocol and security.

Not all questions have been answered and further investigation is required to:

- Evaluate the performance and capabilities of implementations of IPsec.
- Evaluate the performance and capabilities of implementations of DNSSec and SEND.
- Evaluate the performance and reliability of dual IP systems versus mono IP systems. Quantify the exact amounts of additional resources required by a dual stack system (i.e., memory and CPU).
- Evaluate the security and performance of available translation transition techniques (that needs to be done before adopting one solution versus another, in case a translation transition technique is needed).
- Evaluate the capabilities and performance of IPv6 firewalls, including personal firewalls of servers, with respect to their ability to perform filtering of packets according to their address, ICMPv6 messages and extension headers.
- Investigate the capabilities of IDSs and IPSs to analyze fragmented IPv6 packets.

MICHEL BARBEAU

Michel Barbeau is a professor of Computer Science. He got a Bachelor, a Master's and a Ph.D., in Computer Science, from Universite de Sherbrooke, Canada ('85), for undergraduate studies, and Universite de Montreal, Canada ('87 & '91), for graduate studies. From '91 to '99, he was a professor at Universite de Sherbrooke, Canada. Since 2000, he works at Carleton University, Canada. He focuses his efforts on network and wireless security, vehicular communications, wireless access network management, ad hoc networks and RFID.



On Cyber Investigations

Case Study: A Targeted E-banking Fraud Part 1

As money migrates into the virtual world, the crime follows. This article presents a brief journey into the industry of cyber crime and the methodology of cyber investigation, disclosed through a real world case study.

What you will learn…

- a typical scenario for professional electronic banking robbery
- malicious technologies used and security vulnerabilities exploited in the real world, and their relevance to your own security fortress
- an outlook of the high-level layer of the process of cyber incidents investigation.

What you should know…

- basics of electronic banking technology
- basics of the modern threat landscape.

The author's main objective is to highlight the general approach and the particular techniques of a cyber investigation process.

The criminal case in question demonstrates a typical systematic approach to massive targeted e-money fraud. Due to this reason the article will also serve educational purposes to the professionals involved in cyber crime research and investigations.

Part 1 of the article (current) delivers a high-level outline of the incident, the investigation plan, and the investigation output.

Part 2 of the article will be focused on the specific expertise methods and instruments involved in the investigation process, as well as the technical details of the case.

A note on terminology

In the security industry, a number of memes related to reactive measures against cyber crime exist.

Incident response is a historical term, which basically refers to initial understanding of the attack context. Depending on the IR output, other business processes may come into action, such as a cyber investigation, a security auditing, or immediate defensive actions.

Forensics refers to the set of evidence extraction and preliminary analysis instruments and techniques, which guarantee the extracted data relevance to judicial processes in the first place, and the data collection thoroughness in the second place. Forensic science does not incorporate any apparatus for the comprehensive analysis of a criminal case.

Cyber investigation refers to the high-level process which incorporates and coordinates various specific processes, such as incident response, forensic investigation, malware analysis, vulnerability analysis, web site auditing, application security analysis and others, to provide a comprehensive understanding of the attack.

Case study

A money transfer provider (*The Victim*) had been suffering a mysterious finance fraud. Random individuals claimed and successfully cashed money transfers at local and foreign departments of the Victim; while their sender records in the Victim's central database were fine, there was nobody who actually supplied or dispatched those money.

Thus, the Victim was experiencing immediate financial losses at the rate of dozens to hundreds of fake money transfers per day, each transfer sized $3000 to $30000.

The Victim called for help as soon as they exhausted private measures, such as verifying the possibility of insider activity and attempting to recognize the fake transfers to block them. At the investigation start, the attack was still in progress (see Figure 2).

The Victim's Infrastructure

The Victim's dataflow as well as organizational topology was starlike. There was the central management entity, which also hosted the global payment information database and the website. The workstations in subsidiary offices relied upon the centralized database to cash the money transfers in and out. A money transfer request reimbursed by a sender's cash would be accepted by the operator at one subsidiary office, to be stored in the centralized database, to be cashed-out at another subsidiary office only to the claimant whose ID corresponded to the data which was provided by the sender. The payments data was stored and retrieved to and from the global database by operators via a commercial thin-client e-banking application.

The network communication channel between subsidiary offices and the central server was properly secured: authorization was required, the client's IP address was verified, and the traffic was strongly encrypted.

The attack scenario

Note: the scenario has been reconstructed from raw data only, such as network and server activity logs, malware grabbed from compromised computers, website backups and other data. Many assumptions had to me made due to the scarceness of evidence, and thus, every assertion within the scenario is somewhat of probabilistic nature (but no less than 80-90% probability).

It all started with a mass malware infection. A small Trojan was broadcasted by means of a standard drive-by attack or mass-mailing, to form a common botnet. One of the features of the Trojan was to detect the presence of e-banking systems on the compromised host.

At some point, the Victim's compromised hosts were noticed by the botmaster as specifically promising (Payment transfer systems attract cyber fraudsters like honey, because such systems have the major obstacle to low-risk cyber-robbery solved by design: that is, such systems allow easy and quick cashing out for unscreened individuals.) (i.e. by correlating the presence of professional e-banking software with the compromised computer's WHOIS data). A number of single payments were faked for the purpose of testing, which proved safe. Within the next few months, a targeted attack on the Victim was planned and executed.

The attackers' main objective was to compromise as many Victim's subsidiaries as possible, to perform a rapid distributed attack, to cash out as much money as possible before the Victim can undertake any

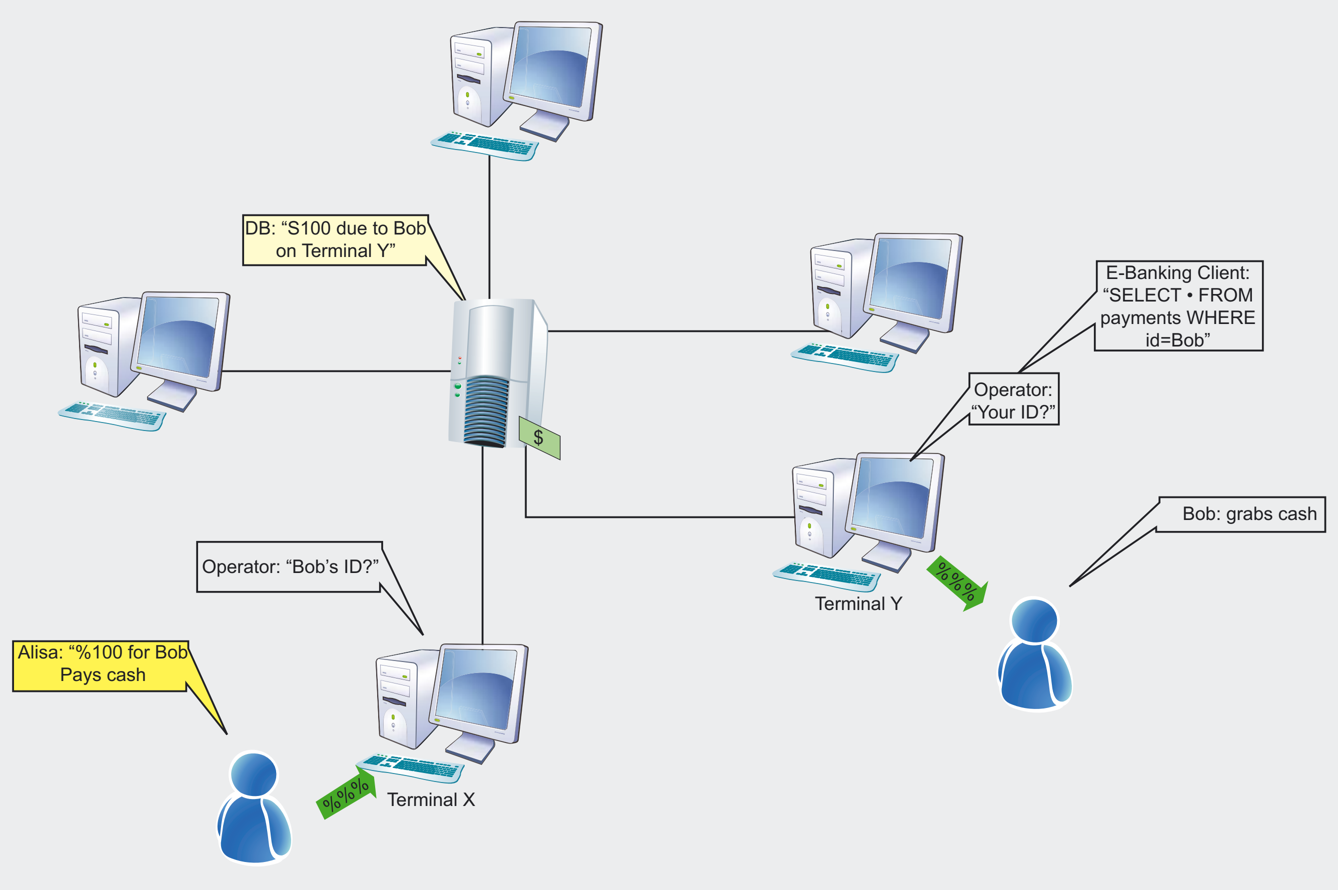

DB: "S100 due to Bob on Terminal Y"
E-Banking Client: "SELECT • FROM payments WHERE id=Bob"
$
Operator: "Your ID?"
Bob: grabs cash
%%%
Terminal Y
Operator: "Bob's ID?"
Alisa: "%100 for Bob Pays cash
%%%
Terminal X

Figure 1. *The Victim in normal operation*

defensive measures. How did they achieve this goal? The answer is that the Victim's central website was infected with malware. Because payment operators used to visit their personal accounts at the central website on the daily basis, the malware was planted on almost every operator's computer in a matter of days. And the malware of the attackers' choice was Zeus.

In order to infect the website, the attackers scanned it for vulnerabilities. They succeeded to find a script which allowed to upload custom files to the publicly accessible directory of the web server. A common web shell script was uploaded into that directory, which provided a custom control panel to the server when called from a browser. The server control panel functionality was then used to inject malicious Iframes into the website's HTML templates.

Upon execution, the malicious Iframe instructed a visitor's browser to download an exploit from a random one-time website. The particular exploit version was chosen automatically by a malicious script, depending on the visitor's browser version information. The exploit then triggered remote code execution in the browser to download and execute a sample of the latest generation Zeus malware.

One of the most powerful capabilities of the Zeus enhanced with extra plugins is to provide support for custom remote desktop connection without kicking off the current user or messing with her input. This very feature was utilized by the attackers to get remote desktop access to the operator's computer while she was at work, to run the e-banking application on top of the operator's already authorized session (a technique known as session riding or session hijacking), and thus, to create fake money transfer records via the e-banking application, signed with the operator's digital signature and time-stamped with her normal working hours. The money transfer record contained ID information of a particular money mule. The central database server eagerly accepted the payment due record, since it was properly authorized and originated from a white-listed IP address.

In the meanwhile, a money mule approached a different subsidiary of the Victim (possibly even in other country) to claim the fake money transfer. The operator first checked the claimant's ID against the centralized database. If a valid money transfer was found designated to this person, she paid the amount of cash stated in the database record to the claimant. The claimant then disappeared.

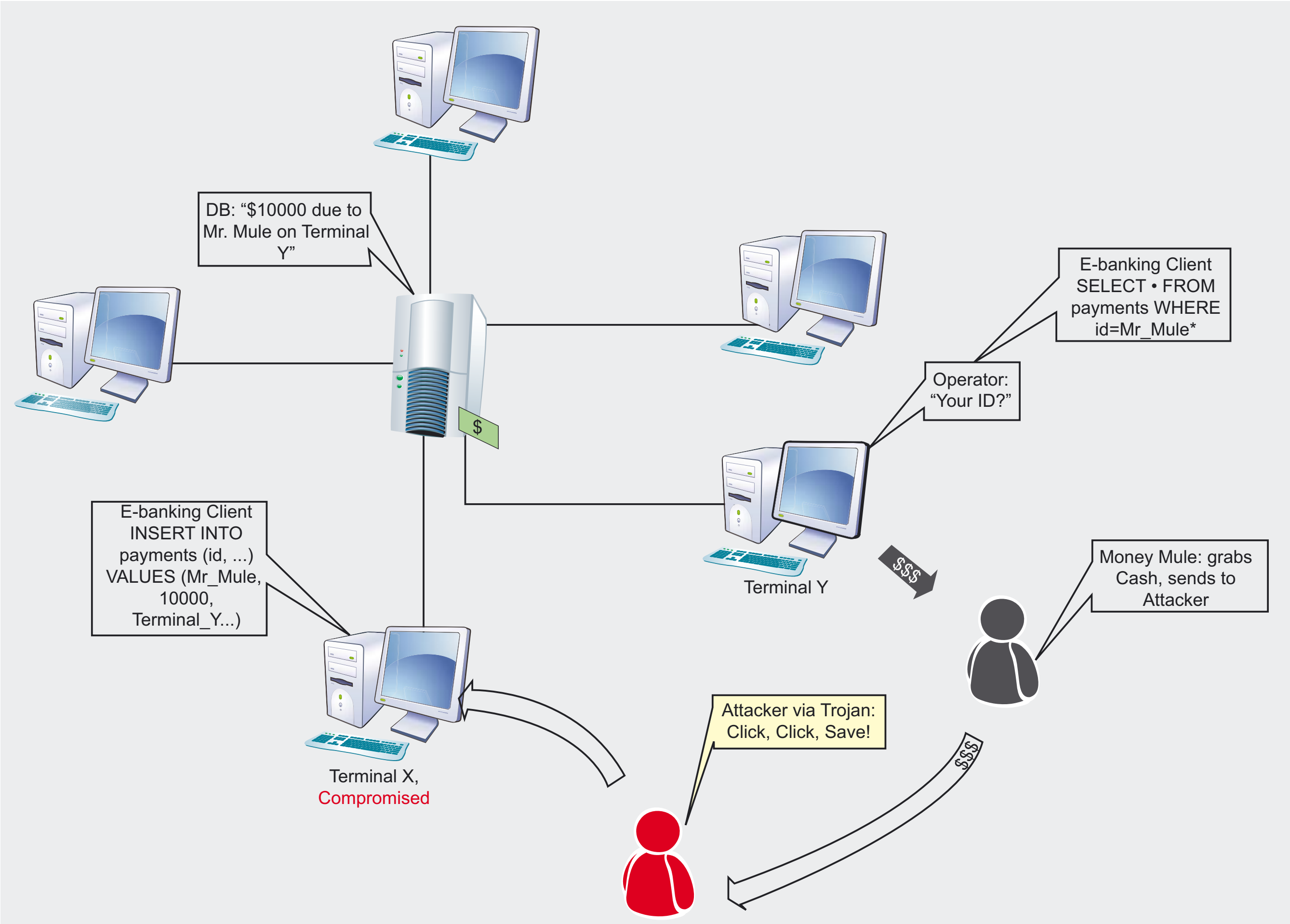

DB: "$10000 due to Mr. Mule on Terminal Y"
$
E-banking Client SELECT • FROM payments WHERE id=Mr_Mule*
Operator: "Your ID?"
Terminal Y
$$$
Money Mule: grabs Cash, sends to Attacker
E-banking Client INSERT INTO payments (id, ...) VALUES (Mr_Mule, 10000, Terminal_Y...)
Terminal X, Compromised
Attacker via Trojan: Click, Click, Save!
$$$

Figure 2. *The attack scheme*

As the Victim's central management entity became aware of the unfolding attack, they tried to distinguish and block the faked money transfers. Note that it is nearly impossible to tell a faked database record from a genuine one, as long as the stored record is complete with all the required information, authorization, and valid network connection logs. Luckily, in the described case, some of the faked transfers might be fingerprinted due to the flaw in the attackers' strategy, who used to send the same money mules to grab similarly (and considerably) sized pieces of cash from various cash-out departments of the Victim.

After a number of fake transfers were blocked, the attackers stopped their action almost immediately to avoid being caught red-handed, and started to cover up traces. After all, they still had the core control: the website file upload vulnerability, which might allow them to repeat the same attack after some time. Luckily for the Victim, the vulnerability was revealed during the investigation process.

As the reader might expect at this point, the output of the investigation was passed to the law enforcement entities, and the Victim's systems had to undergo major security refactoring.

The Investigation

The input to the investigation process was no more that the fact of mysterious fake money transfers. Nobody had any idea of how exactly were the money transfers faked. Luckily, the Victim have already performed the homework to explore the possibility of an insider attack, which proved false. So we could conclude from the very beginning, that fake money transfers were initiated by an external attacker. But how exactly?

- Was the central server compromised, to fake transaction records in the database, or to allow unauthorized connections from alien clients?
- Or, were the client computers compromised, to steal operator's credentials for a remote attack, or even to perform the attack directly from the compromised computer on behalf of the operator?

(From now on, please refer to Figure 3 for the visualization of the evaluation/action process).

In order to prioritize the choice of further expertise to save the precious time, it is important to properly estimate the probability of each possible scenario. Later, as expertise unfolds, the new information helps to re-evaluate the initial estimation, which allows to delay or to drop the unnecessary pieces of expertise.

In this case, obviously, the server compromise scenario is less probable, because organizations tend to underestimate client-side security of ordinary workstations (even those used for e-banking), by the side of the security of central servers. Note that the attacker will always target the weakest link, and we must follow his logic while performing the expertise.

A quick analysis of the central server network logs showed that the fake transactions were initiated by a considerable number of subsidiary offices workstations, recognized by their IP addresses. So the first step was to perform a forensic expertise of the compromised workstations. Again, after estimating

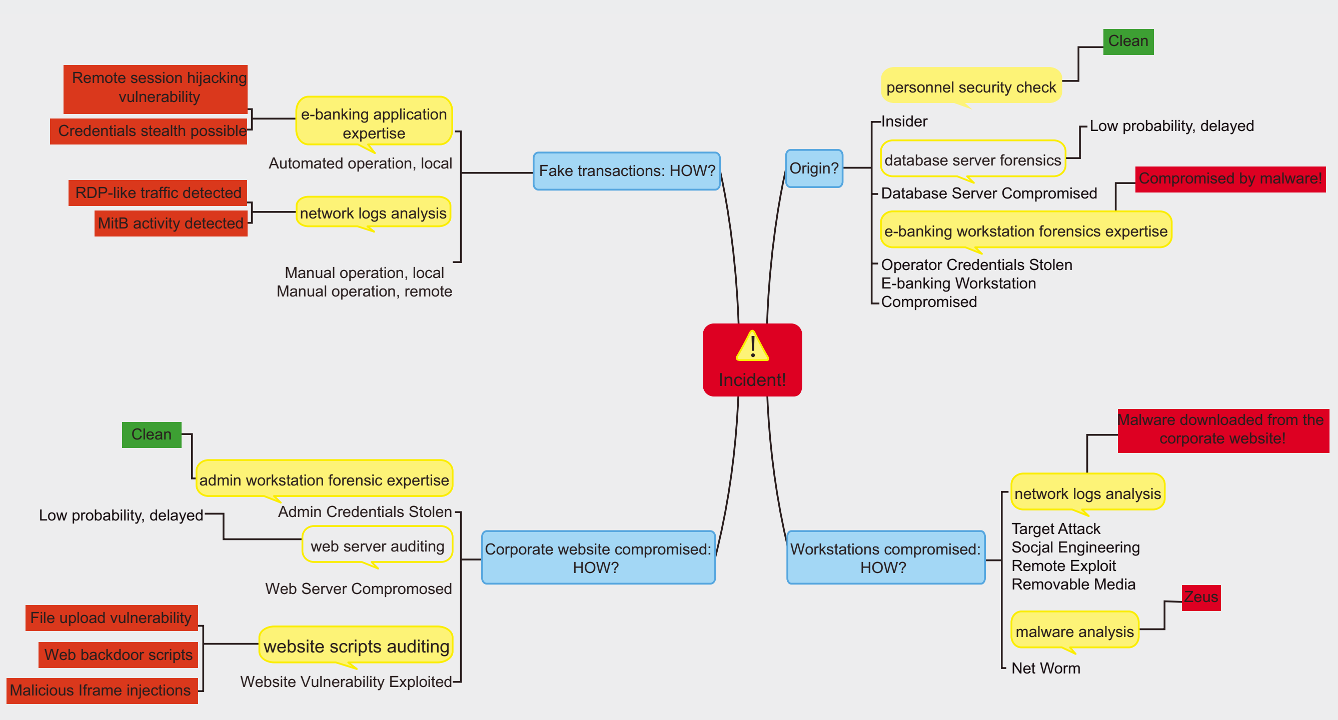

Remote session hijacking vulnerability
Credentials stealth possible
e-banking application expertise
Automated operation, local
RDP-like traffic detected
MitB activity detected
network logs analysis
Manual operation, local
Manual operation, remote
Fake transactions: HOW?
Origin?
Clean
personnel security check
Insider
Low probability, delayed
database server forensics
Compromised by malware!
Database Server Compromised
e-banking workstation forensics expertise
Operator Credentials Stolen
E-banking Workstation Compromised
Incident!
Clean
admin workstation forensic expertise
Admin Credentials Stolen
Low probability, delayed
web server auditing
Web Server Compromosed
File upload vulnerability
Web backdoor scripts
Malicious Iframe injections
website scripts auditing
Website Vulnerability Exploited
Corporate website compromised: HOW?
Workstations compromised: HOW?
Malware downloaded from the corporate website!
network logs analysis
Target Attack
Socjal Engineering
Remote Exploit
Removable Media
Zeus
malware analysis
Net Worm

Figure 3. *Evaluation/action mindmap, simplified*

the probability of various possible findings, we may find it surplus to perform a full forensic analysis of compromised computers. In this case, we started from looking for bodies or traces of malicious software, since it would be the most probable finding, and in case that it proved false, then only we proceeded to deeper analysis.

In this case, a deeper analysis turned low-priority, as soon as we've found that every compromised computer was infected with malware. Noteworthy, that every infected computer had an antivirus product installed, or in some cases, a few antivirus products. This new information was not enough to understand the attack, of course, but it was enough to define and prioritize the next steps, guided by the new questions:

- How were the clients infected with malware? Was it a targeted attack, or a web exploit, or a net worm, or a malicious Flash drive or a CD, planted on operators?
- How, if somehow, was the malware used to fake the money transfers? Was it a credentials stealth, or a session stealth, or anything else?

Two expertise processes have been considered equally necessary at this step: first, to perform the malware analysis, and second, to analyze the workstations networking logs. The workstations were based on standard editions of Microsoft Windows, so no internal logging was available, and in some cases, even proxy/router logs were unavailable or limited. In such cases, if the evidence is scarce, it is important to inter-correlate the tiniest pieces of information to understand the major pattern.

After performing malware analysis and network logs analysis, we learned the following:

- Every compromised computer was infected with the same version of Zeus Trojan.
- Every compromised computer have visited the same malicious website at some point before the attack, and have downloaded suspicious executable modules from them.
- The malicious websites were visited immediately after the browser homepage was visited (that is, the Victim's corporate website).
- Immediately after a client was compromised, it started to generate all kinds of suspicious traffic to malicious servers, compromised legitimate websites, and no-name VPS hosts.
- In some cases, network log records revealed a highly intensive, extended outgoing traffic accompanied by low incoming traffic – a pattern suggesting a remote desktop connection such as VNC or RDP.
- During the attack, in some cases, a text file was downloaded and saved to the compromised computer, containing details of payments to be faked (money mules IDs, amounts of money to fake, etc.)

It turned out that the Victim's corporate website was compromised to host malware, which allowed to infect many clients at once. However, the malware analysis output didn't shed any light to the technical details of faking the money transactions, because the Zeus Trojan is such a universal malware that would allow to implement many different attack scenarios.

The most promising and mysterious finding were the text files, containing details of the faked transactions. Basically, given that the operators were already screened by the Victim's own security service, this finding suggested only two opportunities: either the text files were parsed automatically by malware installed on the compromised computer to perform automated e-banking system transactions, or there was another person logged in to the same compromised computer, who extracted the payment information from the text files, to fake transfers by hands.

Luckily, a very tiny detail hidden in one of the network logs allowed us to resolve the last question immediately, which saved a lot of time on the expertise. That is, we've noticed that, a favicon.ico file was requested from the malicious web server immediately before the malicious text file request. This nuance testified that the malicious text file was requested by someone sitting at the browser, rather than it was downloaded by malware via a direct HTTP request. So, we were able to assume a high probability of the suggestion, that at least in number of cases the transactions were faked manually, by means of a remote desktop connection to compromised clients.

Still a number of questions remained.

- How did the attackers manage to compromise the corporate website, to plant an exploit on it? Did they break into the server, or did the find a hole in web scripts, or maybe stole the admin's FTP password?

Stealing web server administrator's password via a malware is an easy task, so we had to verify this high-probability scenario by means of auditing the administrator's computer. The administrator's computer showed no traces of malware, neither alive or deleted. So we performed the web scripts auditing, after considering them the most probable target for a server compromise. As the result, we've located a vulnerable script in the web site, subject to custom file upload, along with the uploaded malicious scripts which allowed to inject malware into website pages.

- Which scenarios of creating fake transactions would the e-banking application support? Because we had not enough evidence to assume the RDP connection was the only technology behind faking e-banking operation, we had to assume other scenarios to provide an effective advisory.

Auditing of the e-banking application revealed a vulnerability, which allowed to hijack an authorized session remotely, by stealing the session token. So, in some cases the attacker might perform fake transactions from his own computer, channeling the connection via malicious proxy installed on a legitimate Victim's workstation to bypass the e-banking server IP address verification. Apart from that vulnerability, we've found that the e-banking application allowed easy stealing of the user's key files – again, the attacker might use them to impersonate a legitimate operator remotely.

Note the dual link between the probability evaluation and the expertise: every piece of expertise provides new information, which allows to refine the vision, to plan the further expertise.

Lessons Learnt

- On attacker's way of thinking. An attacker builds his way to the goal step by step, on each step locating and exploiting the easiest targets throughout the victim's infrastructure. Thus, a non-comprehensive security equals to no security.
- On the doubtful value of security solutions. We've seen a number of top-rated antivirus products installed on compromised hosts along with the powerful – and still very common – malicious tools. We've also seen IPS solutions guarding the network, while the attacker gets straight inside via a client-side vulnerability. Thus, security should rely on system design rather than on any kind of *solutions*.
- On the easy-going trend about the attackers' approach. The attackers are building highly professional attacks upon common malware (Zeus), which is easy to buy on the black market. Moreover, rarely do they bother with studying the e-banking applications internals, or even with stealing credentials, but they rather set up a remote desktop connection to impersonate the already authorized operator, and to perform the job via the same comfortable visual interface, that the operator uses. Cyber crime looks easy – even the big cyber crime, and this is the alarm.
- On the expertise coverage. It is important to explore every system that could have been possibly involved in the attack. In this case, if we've missed even a single malicious script on the web server, then the attackers would easily replicate the same attack after some time.
- On web security. Web site security matters, more than one would estimate for a regular corporate site. Compromising the corporate site might lead to compromising the organization partners or clients, all at once, which can be leveraged to compromise the organization in a variety of ways.

Cyberhunting

If we analyze why the attackers are going so easy about massive cyber crime, this is because they succeed more often than they are caught. Basically, prosecuting cyber criminals beyond their virtual identities is the task for the law enforcement; but, in case that a virtual identity is shadowed thoroughly (i.e. via a distributed anonimization network/botnet), it is nearly impossible to solve that task by means of passive analysis.

So we are going to lose on points, unless we adopt a more aggressive technology for investigating cyber crimes. As an example, a virtual criminal can be easily identified in person, if s/he is baited or socially engineered out of the Tor for just a moment. The important thing to understand is that, any ethical or legal limitations being applied to the cyber investigation process, are only limiting the investigators and serve no other purpose, since the criminals operate beyond those limitations by their nature.

ALISA SHEVCHENKO

Alisa Shevchenko alisa@esagelab.com
CEO, eSage Lab www.esagelab.com
Specially for www.nobunkum.org

Cloud Computing Legal Framework and Privacy

The internet does not belong to one country or region. Therefore, international collaboration is a key area of focus and we need to continue to work with partners around the globe in support of our cybersecurity goals.
Howard A. Schmidt

What you will learn…

- Legal Framework of the cloud
- Safe Harbor isn't safe
- Death of Privacy Rights

What you should know…

- Cloud Computing basics

Cloud Computing is not a brand new term or concept. Since the days that you started to use AOL Webmail, MSN Hotmail, Yahoo, or Gmail you have been using Cloud Computing. If you use Facebook, Twitter, online data storage, Google Apps, many photo sites, etc. then you are using Cloud Computing.

Simply stated Cloud Computing is using others' computer systems, hardware, and software to do things on your system. The data is yours but others take care of the server(s) and application(s).

According to the *National Institute of Standards* (NIST), Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics

- *On-demand self-service*. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and portable digital assistant).
- *Resource pooling*. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- *Rapid elasticity*. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- *Measured Service*. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled,

and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

- *Cloud Software as a Service* (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Cloud Platform as a Service* (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service* (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

- *Private cloud*. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- *Public cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

For additional technical information please refer to the *National Institute of Standards* (NIST) *http://www.nist.gov/itl/cloud/index.cfm* or the Cloud Computing Alliance *https://cloudsecurityalliance.org/*.

Corporations do this too and that is where things get really dicey. Data centers which are facilities that house computers, etc. can be anywhere in the world. There is not one universal data security and privacy regulation that all countries in the world have agreed to follow.

There is no such thing as the Internet Police. You have to be proactive and not reactive in protecting your individual data. Use my motto: *I like you but I do not trust you*.

According to the Cloud Security Alliance in a March 2010 report, the 7 security threats posed by cloud computing are:

- *Abuse and Nefarious Use of Cloud Computing* – The ease of the registration process for services over the cloud opens up the cloud environment to abuse by spammers, malicious code authors, and other criminal elements.
  <u>Solution:</u> strengthen security of the registration process.
- *Insecure Application Programming Interfaces* – Cloud computing providers expose a set of software interfaces that customers use to manage and interact with cloud services. These interfaces can be hacked by unauthorized users.
  <u>Solution:</u> beef up authentication and access control to weed out unauthorized users.
- *Malicious Insiders* – The threat posed by a malicious insider is not unique to cloud computing. However, the threat is amplified by the convergence of IT services and customers under a single cloud environment and a lack of visibility into the hiring standards and practices of cloud employees.
  <u>Solution:</u> enforce strict supply chain management security and conduct comprehensive background check of cloud employees.
- *Shared Technology Vulnerabilities* – Cloud computing providers deliver services by sharing infrastructure. This opens up the entire system to security breaches.
  <u>Solution:</u> implement a defense-in-depth strategy that includes computer, storage, and network security enforcement and monitoring.

- *Data Loss/Leakage* – The destruction or loss of data, whether accidental or intentional, poses a grave risk to any network, but the risk increases in the cloud environment due to the number of interactions.
  Solution: encrypt data in transit and implement strong data backup and retention strategies.
- *Account, Service, and Traffic Hijacking* – Account, service, and traffic hijacking, such as phishing, fraud, and exploitation of software vulnerabilities, pose risks to any computer system. If attackers gain access to a cloud environment, they can eavesdrop on cloud users, manipulate data, return false information, and redirect users to illegitimate sites.
  Solution: use strong authentication techniques and unauthorized activity monitoring.
- *Unknown Risk Profile* – The benefit of cloud computing, reducing the costs of maintaining computer hardware and software, also creates a risk of losing track of the security ramifications of cloud deployments. *Security by obscurity may be low effort, but it can result in unknown exposures*, the report warns.
  Solution: maintain detailed information about who is sharing the cloud infrastructure, as well as network intrusion logs, redirection attempts, and other security logs.

On April 12 and 13, 2011, I spoke to Dr. Ann Cavoukian, Ph.D. the Information & Privacy Commissioner, Ontario, Canada (*www.privacybydesign.ca*) and her staff. The Commissioner reiterated what she had stated in the Clouds panel discussion she led in 2010 (Reboot event):

The Cloud has become Big Business, and it is growing bigger all the time. For organizations, the economics of scale and logistics are compelling: they can outsource their entire IT department and expertise to "The Grid" in order to focus on core competencies and to adapt and innovate with the times. For individual users and consumers: the Cloud represents convenient "free" services, available anytime, anywhere, from any device.

But there are persistent questions and concerns about what can go wrong when vital data is stored on a server in the sky and under the control of someone else. Jurisdictional and legal considerations are paramount – which laws apply? Accountability concerns follow closely behind – how to assure the confidentiality, integrity and availability of „outsourced" data? Cloud discussions tend to be oriented towards businesses, enterprises, organizations, and governments as Cloud customers and users... but what about the interests of individuals? The „death" of privacy is largely about the loss of control by individuals over their personal data, and of poor information management handling practices by others. Robust transparency and accountability measures, strong and effective safeguards, rigorous data minimization practices, and empowered individuals can all be achieved together when universal Privacy by Design principles are applied to Cloud data systems in a thoroughgoing and proactive manner. Legal parameters and remedies are important, but technology building blocks, standards, and other privacy-enhancing features can and must be built directly into Cloud architectures and operations. The opacity and doubts surrounding Cloud computing can be dispelled by highest standards of leadership, verifiable methods and measurable results. Applied Privacy by Design can help bridge legal differences across jurisdictions, and assure the needed trust among all stakeholders in this most innovative of economic paradigms.

Here are a few examples of the privacy issues that have been in the news lately:

Impersonation

Carbon Thieves Force European Union to Improve Security, Close Spot Market
www.bloomberg.com
January 21st, 2011

The European Union, whose decision to suspend registries halted the region's spot carbon-emissions market following the theft of permits, said it won't lift restrictions until member states step up identification checks. It suspended most operations at Europe's 30 registries for greenhouse-gas emissions on Jan. 19 after a Czech trader reviewing his $9 million account found *nothing was there*. The EU estimates permits worth as many as 29 million Euros may be missing. *At minimum they need to have second authorization in place, such as electronic certificates or ID cards*, said Simone Ruiz, European policy director of the Geneva-based IETA.

Data Protection

Two Arrested in iPad Security Breach
The Wall Street Journal,
January 19th, 2011

Two computer hackers have been arrested for allegedly using a security breach of AT&T Inc.'s servers to gather email addresses and other personal information of about 120,000 users of Apple Inc.'s iPad, including corporate chiefs, U.S. government officials and Hollywood moguls. They have each been charged with conspiracy to access a computer without authorization and fraud in connection with personal information. AT&T acknowledged in June that a flaw in its website made it possible for iPad users' email addresses to be revealed and said it had fixed the problem.

SEC Fines Three for Failing to Protect Customer Data
www.informationweek.com
April 11th, 2011

The *US Securities and Exchange Commission* (SEC) have fined former employees of broker-dealer Gunn Allen Financial for failing to adequately protect customer data. The company was liquidated in November 2010; the SEC maintains that Gunn Allen former president Frederick O. Kraus and former national sales manager David C. Levine broke privacy rules when Kraus authorized Levine to take information about 16,000 clients with him to his new job; the data were transferred on a thumb drive. Kraus and Levine were fined US $20,000 each. Former chief compliance officer Mark A. Ellis was fined US $15,000 for failing *to ensure that the firm's policies and procedures were reasonably designed to safeguard confidential customer information*. The case is the first in which

people have been fined solely for violating the SEC's Safeguard Rule, or Regulation S-P, which requires financial advisers and institutions under SEC jurisdiction to protect customer data and give customers the opportunity to opt out of having their information shared with unaffiliated third parties.

Senator Calls for Investigation into Epsilon Breach
www.gcn.com
April 7th, 2011

US Senator Richard Blumenthal (D-Connecticut), has asked the Attorney General's office to investigate the Epsilon data security breach. The email provider sends 40 billion messages a year on behalf of its clients; Epsilon says that about 50 clients were impacted by the breach, meaning the names and email addresses of individuals who have agreed to receive messages from those companies were compromised. Senator Blumenthal asked Attorney General Eric Holder to look into the possibility of civil or criminal liability for the breach. He also asked Epsilon to provide more information about the incident.

Data Availability

High Hotmail email access issue now resolved
www.windowsteamblog.com
January 3rd, 2011

Beginning on December 30th we had an issue with Windows Live Hotmail that impacted 17,355 accounts. Customers impacted temporarily lost the contents of their mailbox through the course of mailbox load balancing between servers. We identified the root cause and restored mail to the impacted accounts as of yesterday evening, January 2nd. As with all incidents like this, we will fully investigate the cause and will take steps to prevent this from happening again. We're very sorry for the inconvenience this may have caused to you, our customers and partners.

Data Deletion

Missile data found on hard drives
www.news.bbc.co.uk
May 17th, 2009

Sensitive information for shooting down intercontinental missiles as well as bank details and NHS records was found on old computers, researchers say. Of the 300 hard disks bought randomly at computer fairs and an online auction site, 34% still held personal data. Researchers from BT and the University of Glamorgan bought disks from the UK, America, Germany, France and Australia. The information was enough to expose individuals and firms to fraud and identity theft, said the researchers. Professor Andrew Blyth said: *It's not rocket science -we used standard tools to analyse the data*.

Privilege Role

Admin Who Kept San Francisco Network Passwords Found Guilty
www.pcworld.com
April 28th, 2010

The San Francisco network administrator, who refused to hand over passwords to his boss, was found guilty of one felony count of denying computer services, a jury found.

Although the city's network continued to run, San Francisco went 12 days without administrative control of the Fiber WAN, and that constituted a denial of service – illegal under state law.

Database admin steals 2.3M consumer records at Fidelity National subsidiary
Computer World
July 3rd, 2007

A senior database administrator at a subsidiary of Fidelity National Information Services, Inc. who was responsible for defining and enforcing data access rights at the company instead took data belonging to about 2.3 million consumers and sold it to a data broker. The broker in turn sold a sunset of the data to other marketing companies. The stolen data included names, addresses, birth dates, bank account and credit card information, the company said in a statement.

Denial of Service

Bot herders hide master control channel in Google cloud
By Dan Goodin
www.theregister.co.uk
Oct 15th, 2009

Cyber criminals' love affair with cloud computing just got steamier with the discovery that Google's App Engine was tapped to act as the master control channel that feeds commands to large networks of infected computers. The custom application was used to relay download commands to PCs that had already been infected and made part of a botnet, said Jose Nazario, the manager of security research at Arbor Networks. Google shut down the rogue app shortly after being notified of it.... Researchers from Symantec found a Facebook account pumping commands to zombie drones. And in August, Nazario found several Twitter accounts that were doing much the same thing.

Logs

The Athens Affair
By Vassilis Prevelakis, Diomidis Spinellis
IEEE Specturm
July 2007

Just as we cannot now know for certain who was behind the Athens affair or what their motives were, we can only speculate about various approaches that the intruders may have followed to carry out their attack. That's because key material has been lost or was never collected. For instance, in July 2005, while the investigation was taking place, Vodafone upgraded two of the three servers used for accessing the exchange management system. This upgrade wiped out the access logs and, contrary to company policy, no backups were retained. We still have a long way to go before privacy is anywhere close to being somewhat secure and unfortunately few organizations are taking proactive steps to protect sensitive information when they store it in the cloud.

IBM Study

A Cloud Computing study done by IBM in 2010 asked Chief Information Officers if they were doing anything to:

(a) Ensure the privacy rights of customers, consumers and employees are protected.
(b) Ensure the safe sharing of confidential information.

They were asked what steps are taken to protect sensitive data. There responses were:

- None (44%)
- Legal or indemnification agreement (32%)
- Informal self-assessment (8%)
- Training of end-users before deployment (6%)
- Vetting and evaluation by the security team (6%)
- Vetting and evaluation by outside auditor (2%)

There was either 0% or 1% differential when answering in regards to (a) or (b).

The lack of activity seeking to protect data in the cloud was shocking especially when many companies state that they should be trusted because they are listed on the Safe Harbor Privacy list. Let's take a look at what that list means, if anything.

Legal Considerations

Legal issues are highly complex and daunting. This is just a brief introduction and Cloud Computing demands the attention of corporate legal counsel. Electronic Discovery (eDiscovery) will be a challenge. The key is where does the *Electronic Stored Information* (ESI) reside? When the ESI was stored on your in-premise servers you had complete control: retention policies, backup practices, data restoration, data destruction, etc. where all under your control. With Cloud Computing, the game has changed. Many of these areas are under the control of data centers around the world which follow different guidance then you may be accustomed. What if is virtualized over many countries? What insurance to you get to protection you from these new risks or do you self-insurance and if so how do you predict your risk exposure?

Let's look at some of the legal regulations and issues.

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22

"ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act") by extending government restrictions on wiretaps beyond telephone calls to apply to electronic data transmissions. "The PATRIOT Act also clarified and updated ECPA in light of modern technologies, and in several respects

it eased restrictions on law enforcement access to stored communications." U.S. Dept. of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, § III.A.

The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically." http://it.ojp.gov/default.aspx?area=privacy&page=1285

Some examples of individual data that can be obtained via subpoena include:

- Gmail accounts
- Facebook records
- Twitter
- Cell phone records
- GPS data
- Other cloud-based storage

Twitter's policy is to notify users before releasing personal information; however, most Internet companies are not required to provide users with any notice, and law enforcement officials can even demand that requests be sealed from targets of investigation. *http://support.twitter.com/entries/41949-guidelines-for-law-enforcement*.

Google's privacy policy, like Facebook's, alerts customers that it will comply *with valid legal processes seeking account information* but is silent on whether it will try to notify targets of an investigation. According to a New York Times article (*http://www.nytimes.com/2011/01/10/technology/10privacy.html?pagewanted=1&_r=3&partner=rss&emc=rss*) Google had over 4,200 requests from law enforcement agencies the first half of 2010 alone!

In an April 6, 2011 meeting on Capitol Hill, The United States Justice Department stated that it is satisfied with the ECPA as it currently stands and stated that consumers are protected more if the Government has easy access to records. *http://www.informationweek.com/news/security/privacy/229401192*.

Microsoft, Qwest and others members of the *Digital Due Process* (DDP) coalition disagree. They believe, as I do, that the current laws are not keeping up with technology *http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163*. Two recent 6th Court of Appeals decisions agree with DDP, of which, one is listed below.

Even the *American Civil Liberties Union* (ACLU) has created proposals designed to simplify, clarify, and strengthen the ECPA *http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa*:

1. *Robustly Protect All Personal Electronic Information*. Current loopholes in our privacy laws need to be closed to protect electronic information without regard to its age, whether it is *content* or *transactional* in nature, or whether an online service provider has access to it to deliver services.
2. *Safeguard Location Information*. The law should require government officials to obtain a warrant based on probable cause before allowing access to location information transmitted through cell phones, which 82% of Americans own.
3. *Institute Appropriate Oversight and Reporting Requirements*. To ensure adequate oversight by Congress and adequate transparency to the public, existing reporting requirements for wiretap orders must be extended to all types of law enforcement surveillance requests.
4. *Require a Suppression Remedy.* If a law enforcement official obtains non-electronic information illegally, that information usually can't be used in a court of law. The same rule, however, doesn't apply to illegally-obtained electronic information. Such a rule only encourages government overreaching and must be changed to require a judge to bar the use of such unlawfully obtained information in court proceedings.
5. *Craft Reasonable Exceptions*. Currently ECPA sometimes allows access to the content of communications without a true emergency, without informed consent and without prompt notice to the subject. ECPA must be amended on each of these fronts if electronic records are to receive the protections Americans need.

United States Fourth Amendment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

In December, 2010, the 6th Circuit Court of Appeals ruled that the Fourth Amendment protects an individual's e-mail communications that are stored on a third party's server against unreasonable search and seizure. The effect of the ruling is that the 180 day distinction made in ECPA no longer holds – emails are protected regardless of the amount of time they are stored or archived.

The court reasoned that phone calls and letters are protected by the Fourth Amendment, and because email is also a communications medium, it would *defy common sense to afford e-mails lesser Fourth Amendment Protection*.

It's unknown whether the 6th circuit ruling will be appealed, and if so, what the outcome will be. Nevertheless, until we know the answers to these questions, to protect yourself from liability email production should be made only in response to a search warrant and advice of counsel.

Safe Harbor

Many Cloud Computing companies such as Google state that they adhere to the U.S./EU/Swiss Safe Harbor Privacy principles and list that fact as one of the reason why individuals and companies should trust them that they are following best business data privacy practices.

„Google adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce's Safe Harbor Program.

Google regularly reviews its compliance with this Privacy Policy. When we receive formal written complaints, it is Google's policy to contact the complaining user regarding his or her concerns. We will cooperate with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between Google and an individual." *http://www.google.com/privacy/privacy-policy.html*

But what is this policy and who is the certification authority? Is there a requirement for an organization to have a third party security auditor validate the security posture of the joining or reaffirming member organization? According to the website, *http://www.export.gov/index.asp*, an organization can join and certify them self! They pay a fee, fill out the necessary paperwork and no one is held accountable to whether the joining or reaffirming organization is actually applying solid security principles. Without outside Government Security Auditors or independent third party security auditors validating the security posture of the organization, I would not rely on an organization's statement that they themselves certify that they are in compliance with best business data privacy practices.

„Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. Organizations generally not subject to FTC jurisdiction include certain financial institutions, (such as banks, investment houses, credit unions, and savings & loan institutions), telecommunication common carriers, labor associations, non-profit organizations, agricultural co-operatives, and meat processing facilities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances. If you are uncertain as to whether your organization falls under the jurisdiction of either the FTC or DoT, as certain exceptions to general ineligibility do exist, be sure to contact those agencies for more information.

I was surprised to find out the Department of Commerce makes no representation as to the whether the organizations listed on the above mentioned website are actually doing anything beyond paying a fee and filling out paperwork that says they take privacy seriously.

In maintaining the list, the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.

U.S.-EU Safe Harbor

"The European Commission's Directive on Data Protection went into effect in October 1998, and would prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) „adequacy" standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The EU, however, relies on comprehensive legislation that requires, among other things, the creation of independent government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. organizations to engage in a range of trans-Atlantic transactions.

In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a „safe harbor" framework. The U.S.-EU Safe Harbor Framework, which was approved by the EU in 2000, is an important way for U.S. organizations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU member state authorities under EU member state privacy laws. Self-certifying to the U.S.-EU Safe Harbor Framework will *ensure that EU organizations know that your organization provides „adequate" privacy protection, as defined by the Directive.*

The decision by U.S. organizations to enter the U.S.-EU Safe Harbor program is entirely voluntary. Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the U.S.-EU Safe Harbor Framework's requirements, which includes elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the Safe Harbor Privacy Principles.

According to the U.S.-EU Safe Harbor program and organization can develop its own self-regulation and in my opinion that is no regulation at all!

To qualify for the U.S.-EU Safe Harbor program, an organization can (1) join a self-regulatory privacy program that adheres to the U.S.-EU Safe Harbor Framework's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the U.S.-EU Safe Harbor Framework."

U.S.-Swiss Safe Harbor

"The Swiss Federal Act on Data Protection went into effect in July 1993, and important modifications in January 2008. The Act would prohibit the transfer of personal data to countries that do not meet Switzerland's "adequacy" standard for privacy protection. While the United States and Switzerland share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by Switzerland. In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Act, the U.S. Department of Commerce in consultation with the Federal Data Protection and Information Commissioner of Switzerland developed a „safe harbor" framework and this website to provide the information an organization should need to evaluate – and then join – the U.S.-Swiss Safe Harbor program.

Please note that the form used for self-certifying compliance with the U.S.-Swiss Safe Harbor Framework is identical to that used for self-certifying compliance with the U.S.-EU Safe Harbor Framework; nevertheless, an organization is not required to self-certify to one of the Safe Harbor Frameworks in order to self-certify to the other. Organizations should also note that when they select "Switzerland" as a country from which they receive personal data, they are self-certifying compliance with the U.S.-Swiss Safe Harbor Framework. It is critically important that an organization read the U.S.-Swiss Safe Harbor Privacy Principles, 15 FAQs, and enforcement documents before submitting a self-certification form.

According to the U.S.-Swiss Safe Harbor certification submission requirements as long as your processing fee has been received and the paperwork is complete the organization gets added to the U.S.-Swiss Safe Harbor List on the website!

Upon receipt of your organization's self-certification submission and corresponding processing fee, the submission will be reviewed for completeness. If and when the submission is deemed complete, it will be posted to the U.S.-Swiss Safe Harbor List, available on this website."

European Union (EU) Data Protection

Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC (Official Journal L 181 of 04.07.2001).

This Decision sets out standard contractual clauses to ensure an adequate level of protection of personal data transferred from the EU to third countries. The Decision requires Member States to recognise that companies or bodies which use these standard clauses in contracts relating to the transfer of personal data to third countries ensure an „adequate level of protection" of the data.

The European Union agrees that there needs to be better legislation. European leaders want worldwide legislation on data protection to improve the security of cloud computing *http://www.security-technologynews.com/news/eu-leaders-want-cloud-computing-security-regulations.html*.

German Data Protection Authority

The German Data Protection Authority recently issued a legal opinion on cloud computing which categorized clouds outside the EU as per se unlawful even if the EU has issued an adequacy decision in favor of the foreign country in question, unless the German rules on data processing are applied and the EU approved model contract for controller-processor data transfers (Directive 95/46/EC, applicable to all 27 Member States as well as Norway, Iceland and Liechtenstein) are used. This legal opinion determined that the safe harbor certification held by the U.S. is not sufficient to protect data stored in the cloud *https://www.datenschutzzentrum.de/presse/20100618-cloud-computing.htm*. (You can use *http://www.online-translator.com/* to translate the German version to another language of your choice.)

There are many more legal concerns in the cloud for instance:

Additional References:

- *http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf*
- *http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf*
- *http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf*
- *https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf*
- *https://cloudsecurityalliance.org/csaguide.pdf*
- *https://cloudsecurityalliance.org/guidance/CSA%20Cloud%20Controls%20Matrix%20(CCM)*
- *http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment*
- *http://iac.dtic.mil/iatac/download/Vol13_No2.pdf*
- *http://www.privacybydesign.ca/content/uploads/2010/07/pbd-NEC-cloud.pdf*
- *http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf*
- *http://www.clouddir.com/*

- Patriot Act
- UK Regulation of Investigatory Powers Act
- Stored Communications Act (part of ECPA)
- National Security Letters (may not even know of investigation)
- HIPPA (*health-related information*)
- *Gramm–Leach–Bliley Act* (GLBA) (financial services industry)
- *Federal Trade Commission* (FTC) and state privacy laws
- *International Traffic in Arms Regulations* (ITAR)
- *Export Administration Regulations* (EAR)
- Fair Credit Reporting Act
- Privacy Act (for federal agencies)

Since United States and international privacy laws vary by country whose laws will be followed when data centers cross international boundaries? Whose responsibility will it be to:

(a) Conduct due diligence?
(b) Restrict access, use, and disclosure of personal information?
(c) Establish technical safeguards?
(d) Establish organizational safeguards?
(e) Establish administrative safeguards?
(f) Create and execute legally binding contracts with cloud-computing providers?
(g) Notify individuals of a data breach?
(h) Notify the proper agencies of a data breach?
(i) Notify the proper sector-specific privacy laws and regulations in each country?
(j) Notify individual's that their data will be outsourced to another company?

Conclusion

Whether you like Cloud Computing or not it is here to stay. Security and privacy issues need to be addressed before moving to the cloud. The legal framework needs to be expanded and updated to encompass today's and tomorrow's technologies. An agreed upon unified international legal framework needs to be designed and adopted.

- Visit sites like *www.privacybydesign.ca*, *www.privacyassociation.org* and *www.cloudsecurityalliance.org*.
- Have Dr. Ann Cavoukian come and speak to your company or organization on privacy.
- Have your security professionals join the International Association of Privacy Professionals (IAPP) and become certified. The IAPP offers four credentials: CIPP, CIPP/G, CIPP/C and CIPP/IT. Each designation is designed to demonstrate mastery of a principles-based framework and knowledge base in information privacy in a legal or practical specialization.
- Have your security professionals obtain the only industry *Certificate of Cloud Security Knowledge* (CCSK) from the Cloud Computing Alliance.
- Collaborate with others in the industry both locally and internal
- Get your legal counsel involved.

As Howard A. Schmidt, a Special Assistant to the U.S. President and the Cybersecurity Coordinator for the U.S. federal government stated in Issue Number 13 Infosecurity Professional Magazine *The internet does not belong to one country or region. Therefore, international collaboration is a key area of focus and we need to continue to work with partners around the globe in support of our cybersecurity goals.*

REBECCA WYNN

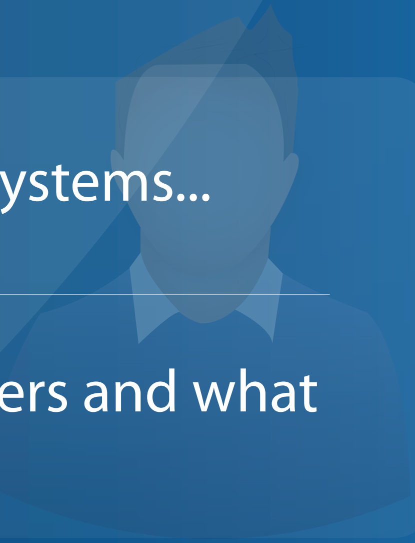
Rebecca Wynn, MBA, CISSP, LPT, CIWSA, NSA/CNSS NSTISSI 4011-4016 is a Principal Security Engineer with NCI Information Systems, Inc. She has been on the Editorial Advisory Board for Hakin9 Practical Protection IT Security Magazine since 2008.

idtheft
protect

Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...

Be proactive...



- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...

ID Theft Protect provides information on threats from a user perspective.

Visit: **http://id-theftprotect.com**

Cloud Security: Is the Sky Falling Already?

Is It Raining Cats and Dogs or Have We Found a Silver Lining in Cloud Computing?

Everyone seems to be jumping into the Cloud with both feet and many before they have realized that there may not be a silver lining with their public or private cloud.

What you will learn…

- Attack Methods against These Devices
- System Hardening and Defense Methods
- Current Tools for Defending These Devices

What you should know…

- Your Cell Phone and/or PDA Operating System
- Common Vulnerabilities and Exposures (CVEs)
- How to Install a Task Manager and Firewall

Just take a look at the competitive nature of streaming video on demand, offered by NetFlix through the Cloud or Amazon or large cable TV operators like Comcast and others. Some of these vendors seem to be sending out TCP resets on their end-user customers to kill the smooth streaming of a video, over their internet service, because it comes from another video service provider. I'm sure there will be law suits flying soon, when users get upset about their movies hanging, restarting or playing at a lower quality than they expect. So there's already a battle taking place in the Cloud.

Knowing that Cloud computing relies upon 'elasticity' and lots of virtual machine computing power, you might ask yourself if there will be another battle taking place – that between Cyber criminals, Cyber terrorists and Cloud Service providers. Most folks I talk with in IT think it's a great idea to do outsourcing – their PCI audit, for example, if they are a retailer, vs doing a self-assessment (which I recommend), their accounting package in the *cloud* at *QuickBooksOnline.com*, remote *cloud-based* storage for backups and the list goes on and on. So what's really happening here?

First, let's level set things – does anyone know what the *Cloud* really is? How does it differ from the *Web* or the *Internet* and why is it so important? Once we have a grasp of what the Cloud is, then we can better understand why I've predicted that it will become, this year, a Hacker Haven and a Malware Magnet. With this understanding, we will be able to make intelligent judgments about whether this ecosystem is one in which we will shift portions of risk for our own organizations and how to ensure the risk is as minimal as possible.

When it comes to regulatory compliance, if your cloud provider is not SAS-70 audited regularly (most are NOT) then don't expect them to be responsible for your compliance posture. If there is a breach in the cloud, the bottom line is that it's your responsibility, if you are using Cloud Computing to host servers or services used for your outward facing business or if you store confidential customer records *in the cloud.* I would argue that it increases your risk and there can be no shift of blame for a successful *Cloud* attack and breach of confidential data stored in the Cloud. You are ultimately responsible. So before you make the move, let's get a better understanding of what the Cloud is and then you can decide if it is worth the move.

Cloud Computing is *the concept of offloading data storage, software applications and computing resources to one or more remote locations using various internet protocols*. The big problem with the Cloud is that you shift risk and lose control to gain flexibility, availability and the cost savings of shared, remote resources. This, of course, opens the doors wide open for hackers, cyber criminals, cyber terrorists and their favorite tools – new *zero day* malware. I'll give you some ideas on how to deal with this problem later in this article.

For a more in depth understanding of Cloud Computing, read my last article from Hakin9 Magazine on *Securing the*

Cloud where I use the definition provided by my friends at the National Institute of Standards and Technology (*NIST.gov*), as it is the best, most comprehensive. According to NIST, Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

For those who don't want to go digging up my last article, let me just summarize, that Cloud computing provides:

- *On-demand self-service*. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- *Resource pooling*. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- *Rapid elasticity*. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- *Measured Service*. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Through three service models:

- *Cloud Software as a Service* (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Cloud Platform as a Service* (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service* (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

With Four Deployment Models:

- *Private cloud*. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- *Public cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Private Clouds – A Silver Lining?

Before you consider moving to the Cloud and take advantage of this *silver lining* of elasticity, on-demand services, and so on, you need to consider staying on a Private Cloud vs a Public Cloud to maintain control, unless of course you are outward facing and want to provide services, like NetFlix, to your customers.

If you can choose a Private Cloud over a Public Cloud, it gives you more control over the security posture and your own business model. It could be your silver lining as you make the shift to Cloud Computing. Remember, if there is ever a data breach it's your fault unless you get a third party SLA agreement spelling out responsibility during a cyber breach. I doubt you can get an SLA from a third party without them protecting themselves from liability of a breach in your Cloud. If you can do this, please let us know – share your story with Hakin9 magazine so others can learn from your successes.

Public Clouds – Raining Cats and Dogs?

Just like signing up with a web-host service provider, you'll still need to take a close look at the *service level agreement* (SLA) of your Cloud Computing service provider in the following eight important areas:

1. Confidentiality
2. Availability
3. Integrity
4. Reporting
5. Alerting
6. Compliance
7. Policies
8. Quality of Service

If you can get some level of guarantees in these eight areas that meet your own internal self-assessment requirements for best practices in providing *uptime* or *access* and the quality you expect, you'll be better positioned to make the right decision on which Cloud Computing service provider is best for you.

Risks in Cloud Computing

After getting a basic understand of Cloud Computing, you'll realize that there is a major risk that needs to be managed. To do so, we must understand the Risk Formula. This formula is an *immutable law* – you need to consider all exploiter opportunities, vulnerabilities and the devices – network assets and related database servers – where the Cloud service might be weak. Here's the formula to use:

```
Risk = Threats x Vulnerabilities x Assets
```

Threats

In the case of Cloud Computing, the threats we should be worrying about are:

Malicious insiders with access to the virtual machines, servers and services that are hosting the Cloud service. Without proper physical/logical/network security and strong policies that include background screening of individuals, you may have someone gaining access to your Cloud service who holds the 'keys to the castle' and also has an agenda of theft and greed.

Virtual Computing Exploits are new forms of malware (botnets, viruses, worms, spyware, Trojans, zombies, etc.) that take advantage of Hypervisor flaws and other holes in the VM host operating system.

Application Layer Exploits are traditional attacks against known holes. These known holes are called CVEs and I explain what they are below.

Some Example Threats to Cloud Computing

Because Cloud Computing is taking off, it's opened the door to new and innovative exploits. Here are some of the latest ways cyber criminals and cyber terrorists are exploiting the Cloud:

Cloud Abuse

Cloud Infrastructure as a Service (IaaS) providers are open to abuse through weak, insecure registration processes, where anyone with a valid credit card can register to immediately begin using cloud services. Anyone can obtain an anonymous funded Debit/Credit card by going to a local mall or over the internet and funding the card. Then, by abusing the anonymity of the registrations, cyber criminals can host old and new *zero-day* malware exploits. Cloud providers need to provide strict and validated registration processes. In addition they should be able to blacklist abusers, tracking remote ISP, router, IP address, MAC address and other information to *fingerprint* the criminals and block their abuse.

Exploiting Cloud APIs and Virtual Machine (VM) Vulnerabilities

Some of the top Public Cloud providers also offer application programmer interfaces (APIs), written from a *trust* perspective, not a paranoid security model. Without strong encryption, validation, authentication and access control, these APIs will be exploited to gain access or control over critical *admin* Cloud functions. With VMs taking off, there are more and more Common Vulnerabilities and Exposures that require detection, analysis, review, reporting and remediation. This means you have to work with your VM provider – for example, Microsoft or VMware – to make sure they are writing SECURITY FIXES not just more patches that open more holes.

Account Hijacking

Some of the more serious cyber criminals will use numerous methods such as traditional Phishing attacks and more sophisticated combinations of Malware exploits through social engineering ie, knowing Jane is in the payroll department, sending an email to her…. *Jane, here's the spreadsheet I promised you….see attached PAYROLL.xls* where *PAYROLL.xls* is a custom malware attack that installs keyloggers watching for Jane's access to *QuickBooksOnline.com* to gain access to her credentials on this Cloud service. It's important to train your employees to be more cautious about opening email attachments. In addition, it's strongly recommended to run a HIPS engine like Threatfire or Prevx in conjunction with sophisticated firewalls like Comodo or ZoneAlarm, which should catch and block the keylogging and data leakage. I'm also a proponent of three factor authentication. If you can't get that far, go for at least two factor as required access to your Private Cloud service or by your employees to those that provide you with Public Cloud services.

Vulnerabilities

Common Vulnerabilities and Exposures (CVEs – see *http://nvd.nist.gov* and *http://cve.mitre.org*) in popular applications such as web-servers, database-servers, file-sharing servers, etc. that can be exploited remotely. These holes are commonly known and documented by the software companies that make these applications, but usually, only after they have been exploited and this information has been shared with MITRE's CVE program and the NVD. If you find yourself or your Cloud Service provider to be running any flavors of these vulnerable applications, you'll need to audit these systems for these flaws and harden them.

Assets

In the Cloud Computing environment, your assets at risk start at the core – the storage media that houses your confidential data, customer records, transactional data and any other information that could cause a *personally identifyable information* (PII) breach. Working your way out from the core, you have the physical location where this information is stored. If it's in a Public Cloud, you have no control over this storage process so you must add a layers of encryption to protect the data. If there are malicious insiders or cyber criminals hacking your vulnerabilities, maybe you've encrypted the information at the 'abstracted' storage layer and in the transport that would make it difficult for these folks to steal the PII. So, *Encryption of data* is so crucial to protection against exploitation. In addition, you always want to know what real or virtual devices are running or connected to your Public and/or Private Clouds. You should also have intrusion defense solutions in place to defend against unwarranted access or virtual machines running that are attempting to steal data through cross-virtual-machine exploits. *Hardening your VM assets* in the Cloud is as important as it is in your corporate LAN.

Proactively Hardening Your Cloud

Make sure you or your service provider reads and follows the recommendations by NIST on hardening your virtual machine environments. This document, published in January, 2011 can be found here: *http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf* and visit their Cloud Computing Collaborative, here: *http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/* as well as the Cloud Security Alliance: *https://cloudsecurityalliance.org/* where you will find their guidelines, which are complementary to the NIST guide: *https://cloudsecurityalliance.org/csaguide.pdf* and finally, another Cloud Security group with some higher level and simple documents you might want to share with your executives, while considering moving to the cloud: *http://cloudsecurity.org/*.

Conclusion

Cloud Computing has many benefits but like all paradigm shifts, it opens up new doors and new possibilities for both increased rewards and risks. If you are certain that the benefits far outweight the risks, make sure you can back it up with an enforceable agreement from your Cloud Computing service provider and run a Private Cloud whenever you have this option.

No matter how strong the SLA with your Cloud provider, it's always up to you to document the proper steps at securing your data in the Cloud and complying with regulations, no matter who you trust. The Cloud Computing provider is an extension of your own IT service offerings to your own organization, so do not hand over the keys to the castle without knowing who you've given them to and how they will guard your most critical and confidential assets, when you've moved the data into the Cloud. If you do it right, you'll find the silver lining – a strong value proposition that provides you with the low *Total Cost of Ownership* (TCO) you've been looking for and a high *Return on Investment* (ROI), otherwise, get ready for your Cloud to begin raining cats and dogs.

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a regular contributor to Hakin9 Magazine and a frequent contributor to NetworkWorld, CIO Magazine, SearchCIO and others. He is also a frequent speaker at network security events and trade shows throughout the globe. He is the founder and Chief Technology Officer (CTO) of NetClarity, Inc, where he can be found at http://www.netclarity.net. He is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org and a CISSP®. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), serves on the advisory board of MITRE on the CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (http://www.NAISG.org).

An analysis of the cloud security threat

The cloud is very much the talk of the IT media town these days. Client side computational resources are still in demand but IT vendors and businesses are looking to the cloud in the hope that third-party companies will manage the network infrastructure (including overload requirements whereby the company has to pay for additional hosting services) and data/network security.

Did you know?
The cloud security market by 2015 will be worth $1.5bn dollars, Forrester Research, 2010

The basic idea behind cloud computing is that unlike traditional computing where the software and data are locally contained, cloud computing does away with client-based software and data. This means end users don't have to be concerned with how to setup a system and application configuration for example. Computer resources will be dedicated to managing Internet bandwidth, browsing and an operating system. Cloud computing in essence will radically alter the way computers and the Internet will be used in the future.

This has to some point already happened with *MSN Hotmail and Google Mail* (Gmail) for example. Both these services are available from any computer anywhere in the world where there is an Internet connection and the emails that are received are stored on email services (not servers) in the cloud.

The cloud computing models

IaaS (*Infrastructure-as-a-Service*) – this in effect means the business purchases the infrastructure, own the software and purchase the power (including dynamic scaling and policy-based services) that is needed. In other words it runs identical to a virtual server, with the only difference being that the business would run the virtual server on a virtual disk. Amazon web services are a good example here.

PaaS (*Platform-as-a-Service*) – the provider provides the cloud computing resource and platform. With PaaS, businesses will develop the software applications they want. These types of services provide the end-to-end system development life cycle (SDLC) i.e. website portals; easier administration; automatic update; patch management and gateway software. GoogleApps and Windows Azure Platform are examples here.

SaaS (*Software-as-a-Service*) – this model (closely related to ASP and on demand computing software) provides everything. The service (well known providers include MS CRM and *SafeForce.com*) is provided through a web portal for example and the service is usually free from anywhere. Yahoo! Mail, Hotmail, Google Search. Google Docs or Microsoft Office Web is examples here.

The International Data Corporation (IDC) says that *The proliferation of devices, compliance, improved systems performance, online commerce and increased replication to secondary or backup sites is contributing to an annual doubling of the amount of information transmitted over the Internet*. The actual cost of dealing with this amount of data is something companies are yet to fully address. Currently, companies only look at the cost savings measures and bottom line. It might change once the global economy is out of its current slump.

Enterprise and SME cloud advantages and threats

Businesses are starting to realize that simply by tapping into the cloud they can gain very fast access to high-end business applications, improved mobility and dramatically improve their infrastructure resources and performance all at very little cost. So just how safe is enterprise cloud computing?

For those of you who use SaaS and PaaS, you will know how robust your systems are – and providers of these services were first to point out that the security in the cloud is tighter than in most enterprises. Cloud infrastructure sees multi-tenancy (usually via an external third-party) between hardware, applications and resources so it's easy to see that businesses and enterprises place a huge amount of trust the external cloud provider.

Did you know?
Two thirds of firms have security fears of cloud computing claims YouGov survey, on behalf of Kaspersky Lab, April 19th, 2011.

So it's easy to see that SaaS and PaaS are still fallible to data breaches which end up costing far more than the savings made by moving the network into the cloud. It's important then to have the right SLA in place which protects the business and its customers. You will also need to make sure you conduct a security audit of the in the cloud vendor to establish their security status.

Different countries have different requirements and controls placed on access, so it's easy to forget that the data must reside in a physical location i.e. remote server. Then there is user access. Access control and data management are one of the top security concerns, because insider attacks are a huge risk – think tailgating and someone inserting a USB to copy data or insert a logic bomb onto a server. Users have to have entrusted and approved access to the cloud at all times.

In a virtualized cloud computing environment, for instance, a hacker might use a process or transaction to gain access to the hypervisor that governs the different virtual instances of a cloud-based server. Such access could give the hacker extensive (and, certainly, unauthorized) access and capabilities that could lead to service interruptions or data security breaches.

Data breaches are the main concern for businesses moving into the cloud. The next section will detail some high profile cloud-based data breaches from the past 12 months. This will provide some idea as to the threats and costs facing business including loss of customers and brand damage.

Some high profile cloud-based data breaches

Google Gaia cyberattack: Google was attacked by hackers this time last year. The Google shared security system called *Gaia* (not many people knew what this was as its name was only mentioned once in public) was breached by hackers. Gaia controls the log-in process for Google's applications and as such provides SSO (*Single Sign On*) to Google's applications. This really does expose the flaws of the cloud, chiefly systems and processes. Why did Google insist on providing an SSO? Probably has something to do with there being no alternatives other than users having many different logins, so the users bear the burden of security. As we know this is open to exploitation. The weakest link in any security will always be the people.

Google like most organizations involved in the cloud, will need to invest or internally develop a better SSO system, one that is rigorously tested against internal and external threats. Strong, multi-factor authentications must also be improved and consideration must be given to the use of federated log-in systems. This will lead to a need for users to log-into fewer stronger Web sites than weaker ones. Adopting a strong authentication, and identity federation is a must have for enterprise and SMEs.

Google isn't alone here –in fact the next two high profile cloud-based data breaches with Gawker and Microsoft clearly highlight the need to better collaboration between the cloud vendors. Similar to the AV industry in the way they exchange malware feeds to help with improved global dynamic detection, the cloud vendors could start sharing relevant security information (and applying universal security standards) in the same way. The really big question isn't whether your cloud vendor can provide better security, but whether they actually will.

Did you know?

According to the Poneman Institute and IDC, only 23% of the cloud customers require proof of compliance from their vendors. 62% of executives don't trust their ability to protect their data in the cloud. Most interesting of all was that only 20% of businesses regularly involve the security team in the cloud decision-making process.

Gawker news sites: Gawker was compromised back in December of last year. The Gawker encompasses a set of news sites which include Gizmodo, Lifehacker, Kotaku, io9 or Jezebel. Over 1.3 million passwords were stolen and uploaded via a torrent file (the file size was a staggering 500MB). Also posted, were Gawker's source code and internal employee conversations which was a major data breach. The disclosure of this authentication information led to a viral effect with increased spam attacks, for example, on Twitter being attributed to the breach.

Did you know?

The Gawker servers were running outdated kernel versions. This would have left Gawker seriously vulnerable to exploitation. A group calling itself *Gnosis* was behind the attack.

The passwords were encrypted in the torrent but the encryption schema Gawker used was outdated and very easily cracked. The data breach included usernames and passwords which meant users had to change these on all sites that used Gawker. Some of the Gawker partner web sites were forcing users to change their passwords i.e. LinkedIn was one such web site which sent out an email asking the user to reset their password.

Storing this level of data in the cloud and not having the appropriate security protocols (i.e. encryption) in place would have adverse effects on the Gawker brand and those companies that use its services and those companies that might advertise their products and services. Brand damage isn't quantifiable so it will take a brave person to say what the actual damage.

This example of a cloud data breach clearly highlights that users need to be more proactive when it comes to usernames and passwords. Changing them regularly across multiple sites is important but with the increase in use of SSO, it's becoming easier for hackers to exploit one website and then have access to a handful of other websites that accept SSO i.e. Facebook, Google, Yahoo! And so on. Users should be encouraged to use encryption volumes and store passwords in a password manager (with the password file being stored on an encrypted volume for added protection). Web sites should encrypt all their data at source with the highest levels of data encryption (AES) and allow users the option to automatically encrypt their profile data after they have exited a session.

Microsoft BPOS: Last December the Microsoft *Business Productivity Online Suite* (BPOS) Standard suite service was hacked by cybercriminals. This is a cloud-based service run entirely by Redmond. The issue affected a number of Microsoft customers who were being hosted on the BPOS. The BPOS was accessed and company data was downloaded. The data breach occurred in Microsoft data centers in North America, Europe and Asia. The issue was resolved within two hours of being discovered, Microsoft said in a statement. However, during this time *a very small number* of illegitimate downloads occurred.

Did you know?

BPOS includes Exchange Online, SharePoint Online, Office Communications Online and Office Live Meeting. In October of last year, Microsoft outlined the next version of BPOS, called Office 365, intended to be a full-fledged option to Google Apps and other cloud-based suites. Office 365 combines the collaboration and communication elements of BPOS with Office Web Apps and, alternatively, even with Office 2010.

Microsoft stated at the time that due to a configuration issues, offline Address Book information for the BPOS standard customer could be downloaded by other customers of the service, in a very specific circumstance. It wasn't made clear what that *very specific circumstance* was though.

Did you know?

This Offline Address Book contains an organization's business contact information for employees. It is stored on a server hosted by Microsoft as part of Exchange Online but can be downloaded for offline access. It doesn't contain Outlook personal contacts, e-mail, documents or other types of information, Microsoft stressed.

Epsilon: Earlier in March Epsilon an email marketing company experienced a data breach. Epsilon put millions of customer of such notable companies as Best Buy, Ethan Allen, Walgreens, Target and a host of banks vulnerable to a potential onslaught of spam and phishing attacks. Cyber criminals breached the Epsilon servers. The time taken to alert the affected companies of the data breach meant that the hackers were able to send out phishing emails masquerading as the companies mentioned above. Customers were informed about the breach after the phishing emails had been distributed.

Epsilon isn't the only marketing firm that has left its clients' customers in a vulnerable position this year (2011). Unanimis, an advertising company, was hacked in February of this year (2011), and malicious advertisements ended up on prominent websites as a result. The multi-tenant environment of cloud services means that a breach into one system can give hackers access to multiple systems across a multi-customer environment. The Epsilon breach reignites concerns about the security within this environment.

Cloud security lessons

First, insider threats are real for our own organizations and they are real for cloud providers. There are multiple ways to protect ourselves from internal threats, but one of the foundational elements is to limit and monitor all privileged access as well as baseline and investigate abnormal behavior.

Another lesson is that when assets are concentrated, the damage from an individual incident can be greater. In other words, the same type of incident can cause more damage.

We face this in our own data centers with the shift to virtualization platforms where multiple workloads are now dependent on the integrity and separation provided by the virtualization platform underneath. Public cloud-based services providers face the same problem on an even greater scale. That means the level of due care we require from the provider meet must be higher.

One approach is monitoring (as discussed above). Another would be to limit the scope of administrative access for any given employee. Another would be to put a tight process around how and why administrators are granted administrative access. Nothing new here, it's just the impact of a lapse is magnified. And the issue isn't just Google, it relates to any cloud-based services provider.

The Clouds Control Matrix (CCM)

The Cloud Controls Matrix (CCM) provides fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, and NIST, and will augment or provide internal control direction for SAS 70 attestations provided by cloud providers.

As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry.

The CSA CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardize security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

Source: https://cloudsecurityalliance.org/cm.html.

Non-financial in the cloud data security

So what about employing better security standards for non-financial data like email addresses? There doesn't appear to be a PCI equivalent outside of the financial industry. This will be needed sooner rather than later. Email addresses are much less sensitive than financial information but they can lead to obvious fraud through phishing.

Some organizations will no doubt feel that email addresses is sensitive information and is therefore too sensitive to outsource to a third-party. In the current economic climate it's all about setting a business apart from the rest and a business can offer enhanced security then this will lead to improved customer relationships.

Cloud security accountability

Businesses are lured into the cloud mainly due to the cost savings, but there isn't really any clarity when it comes to balancing the financial argument with the obvious security risks. The CIO (CFO's want things on the cheap, they are also concerned about the risk) of a major enterprise who wants to preserve his job status might well not want the exposure of moving data beyond the corporate firewall and into the cloud.

Risk management and understanding of the business security concerns is crucial in this decision making process. Most businesses currently realize that the technology is still in its infancy at the moment so at

this stage it's unlikely that organizations will precede en mass to the cloud right now. Cloud insiders claim that it may take 10 years before businesses move their infrastructure to the cloud. Security is one key element and over time this will move into the executive boardroom in time. The economic climate will see to that as will organizational necessity.

Did you know?
Cloud computing will surge to $150bn dollars by 2013, Gartner report, 2010.

There is a range of divergent views on the implications of implementing an in-the-cloud infrastructure. Some experts claim the cloud will drive the change while others believe the CIO/CTO will disappear in time as on-demand computing will lead to more cost-effective IT and the demise of the CTO as we know it today. To be fair right now no one really knows. Experts can only guess what the future will hold.

Is cloud computing just hype?

Suppliers are pushing the in-the-cloud and there are some that claim this is pure hype. Vendors do appear to be selling everything these days as *cloud computing* and there hasn't really been technological advances in this area to suggest otherwise. Some commentators have claimed that cloud developments are *at best spurious*.

There are no doubt some business executives who will be looking at moving away from Microsoft Exchange server and placing their corporate email in the hands of a company like Google. When (rather than if) this happens, corporate will then be interested in security, ease of use, uptime and SLAs. Corporate decision leaders (i.e. CFOs) will then find it easier to develop a winning business case for the move into the cloud and working with external cloud-hosted systems such as Google Apps.

The simple conclusion is that, while all senior executives will have a say on the likely business impact of cloud computing, one person will have to be responsible for an organization's strategic approach – and that is likely to be the CIO. Some businesses will see the advantages of constantly evolving user experience and providing a wider availability of services around limitless storage. So what about a hybrid cloud?

Did you know?
A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as **Amazon's Elastic Compute Cloud (EC2) for general computing but store customer data within its own data center.

Did you know?
**22nd April update: Scores of well known websites went offline on 21st April because of problems with Amazon's web hosting service (EC2). Foursquare, Reddit and Quora were among the sites that went offline. It isn't clear what caused the outage, however some have suspected a cyber attack due mainly to the fact it wouldn't mirror the Wikileaks website. At time of writing EC2 is still offline.

Source: http://searchcloudcomputing.techtarget.com.

Final thoughts

For now most businesses will be reticent to move to the cloud (they may move some of their operations into the cloud) especially given the breaches highlighted in this feature. No one cloud vendor can currently give a total guarantee to the security of data. Wouldn't it be great to be able to have the control rather than rely on a third-party? This is why a hybrid solution could potentially inevitably win the day for CIO/CTOs and their executive board members.

JULIAN EVANS
Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect. IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.

Experts on Cloud

Antivirus in the Cloud: fad or future?

by Malcolm Tuck, UK Managing Director, Kaspersky Lab

Although identified by Gartner as a top ten IT strategy for 2011, cloud technology has yet to realise its full potential in corporate IT departments – the promise of increased flexibility and scalability provided by the cloud is offset by ongoing concerns about the security of corporate data. So it is ironic that the cloud represents one of the most exciting and promising new channels for the development and use of anti-malware software.

A good fit for IT security

Cloud computing is an effective method for performing a number of IT security tasks associated with protecting users. First of all, cloud computing allows parallel data processing, i.e. it is ideal for tasks which can be divided into several parts and processed simultaneously, thus getting quicker results. This is crucial for current antivirus products.

In order to analyse a suspicious program it must be checked against lists of malicious and security software as quickly as possible. If this does not yield results, it must be compared to the signatures of known threats, its code must be scanned for dangerous instructions and its behaviour must be examined in an emulator.

All of this research can be performed in parallel. Some processes can even be divided into even smaller parts, for example, database searches. Cloud analysis has a great advantage over analysis performed on a local machine as it allows all of the required detection technologies to be used, having first distributed them between several computers for analysis, thus providing faster and more qualitative research. Additionally, cloud data processing is ideal for reducing the load on a local machine. This task – reduction of resource usage – is important for antivirus developers.

Data processing using cloud services also contributes to the accumulation of extremely valuable information. This feature is also important in combating IT threats. The harvested information is necessary for the immediate neutralisation of all known threats, as well as for the detailed analysis of new malicious programs and the development of antivirus solutions.

There must be a continuous exchange of data between the cloud and the numerous local machines running security products. Local computers provide information about current threats which are analysed and neutralised using the cloud's enhanced computing power, providing a continuous stream of information. Should a new threat appear on just one local machine, protection can be developed immediately and delivered to the other computers connected to the cloud. The bigger the cloud in terms of the number of local machines connected to it, the higher the security level.

Making the right antivirus decision

Antivirus products should incorporate all of the above-mentioned advantages of cloud computing: rapid, deep, parallel data processing, reduction of load on local computers and constant accumulation of valuable information about IT threats.

MALCOLM TUCK

Malcolm joined Kaspersky Lab as Managing Director of their UK Operations as of Aug 2008.

Malcolm has lead IT products and services based organizations through various stages of growth, from initial establishment to regional deployments in Europe and Asia Pacific. This has enabled him to gain valuable experience in identifying what is required to enable a fast paced business to be successful, attract the right personnel and build long term client/partner relationships that are outcomes orientated.

Starting his career as an Avionic Engineer in the Royal Air Force, Malcolm moved to New Zealand and into Information Technologies with IBM in 1990, he then moved to the role of General Manager of Services for Sun Microsystems ISO in New Zealand then on become Chief Executive Officer for a Systems Integration and Development company RHE & Associates in Asia Pacific. Establishing RHE's operations in Perth, Melbourne, Sydney, Auckland and Wellington, before returning back to the UK in 2005 taking up a role as Alliances Director, EMEA for Symantec.

Malcolm is a member of the Australian Business Chamber of Commerce and the Institute of Directors and is married with two children and enjoys classic car restoration, travelling and golf.

Information about malicious programs, spam, phishing resources and other threats, as well as safe programs, should be processed and accumulated in the cloud. This information allows antivirus solutions to provide full control over suspicious programs on users' computers without impeding the operation of a user's safe software. Suspicious programs should be checked against a list of malicious and trusted software. A scanning system based on digital imprints is a much faster method than signature-based scanning.

The use of information from the cloud, in addition to detection results from local machines, should minimise the number of false positives. The response time to new threats should then decrease because the cloud service immediately receives information about any newly emerging threats, analyses it quickly, develops the necessary protection tools and delivers them to users' computers.

Many IT departments still approach the cloud with caution. By recognising the part it can play in an IT security strategy, they can benefit from highly effective parallel computing and instantaneous data exchange, and the subsequently enhanced quality of protection.

Cloud Computing Standards: The Great Debate

Justin Pirie, Director of Communities and Content for Mimecast

Recent research conducted by Mimecast has found that a large proportion of businesses are now using some form of cloud service, with a further 30 percent planning on adopting more cloud services in the future. Fashionable new architectures within the technology industry are not unusual. However, even allowing for a certain amount of bandwagon jumping, this rate of cloud adoption has been considerable.

The *cloud* itself is a competent and established business tool that solves a range of security issues and drives efficiency. However once one delves deeper into the world of cloud computing, one finds that there are some issues that still need resolving. One problem is that as more organisations turn to the cloud, the need for an effective set of industry standards is becoming ever more pressing.

There is a clear divide between those who argue for implementation of cloud standards and those who argue against. At the heart of this debate is a clear need to balance the benefits of having a standard with the call fora sustained pace of innovation.

The argument against cloud computing standards relies on the premise that standards just aren't necessary. In this sense, industry wide uniformity and standardisation is seen as something which wouldstifle innovation and distract focus from more specific problems.

According to this train of thought, different providers need to be free to evolve solutions that best fitdistinctive domain and customer needs.

The alternative *one voice, one system* argument sees the lack of standards in the cloud industry as a serious problem. With the industry being void of anycommonly accepted standards, vendors have nothing to hold them to account and as a result potential and existing customers have little objective information on which to base their buying decisions. A lack of homogeneity can cause a range of issues. For instance a deficiency of inter-cloud standards means that if people want to move data around, or use multiple clouds,the lack of fluency between vendors creates a communication barrier which is near impossible to overcome. Surely companies should be able to move their data to whichever cloud provider they want to work with without being tied in for the foreseeable future?

Another issue is that there is considerable confusion around the term *cloud* itself. Among vendors there is a definite trend of *cloud washing* whereby less scrupulous companies re-label their products as cloud computing too readily, overselling the benefits and obscuring the technical deficiencies of what they have to offer.

This *cloud washing* is in some areas leading to a mistrust of cloud. Furthermore, with the market becoming increasingly crowded and no clear standards in placeit is hard for customers to tell the difference between a cloud vendor with a properly architected delivery infrastructure and one that has patched it together and is merely using cloud as a *badge*. All of this makes it increasingly difficult for customers to navigate their way through the maze of cloud services on offer and, of course, it is the customer who should be the priority throughout these discussions.

Moving forwards, there are a range of bodies that are pursing some form of resolution to the standardisation debate. However for these organisations to have a genuine impact on the industry, companies and individuals need to rally behind them and actively support their calls for universal standards.

The first standard that needs to be tackled is security. It's the number one customer concern about transferring data to the cloud and needs to be addressed as soon as possible. The reality is that this concern is mirrored by vendors who are similarly wary of any potential security breaches and, as a result in most cases go to extreme lengths to protect their customers' data. In factone cloud security firm recently estimated that cloud vendors spend 20 times more on security than an end user organisation would. Security breaches would inevitably mean the reputation of a company falling into disrepute and in worst cases mark the end of their business altogether.

Moreover, the creators of any new cloud based technology do not want to see their project fail for obvious reasons. It is those vendors that do not apply strict standards to their business that need to be called into question. An industry standard is the only way to manage this and good vendors would welcome one because they have nothing to fear from rules of best practice.

The second standard that needs to be tackled is the *Cloud Data Lifecycle*. In previous years, when a customer bought software they installed it directly on their premises. Therefore if the vendor went away they could keep running the software until they found an alternative. With an increasing number of people flocking to the cloud, how can a customer ensure they continue to have access to their dataif the vendor goes out of business? It is for this reason that we need Data Lifecycle standards because currently the onus is on the customer to check the financial health of their provider.

The good news for cloud users is that there is light at the end of the tunnel. The issue of standards is no longer being sidelined but instead being addressed on a large number of platforms with contributions from some of the industry's top decision-makers and influencers.

For most, if not all conversations, it is simply a question of when, not if, cloud standards are established. However while the debate continues, customers will need to ensure that they are aware of the dangers and pitfalls associated, albeit rarely, with adopting a cloud service. Carrying out their own due diligence and research to ensure that their chosen technology is robust, properly architected and secure will remain an essential practice until that time.

JUSTIN PIRIE BIOGRAPHY

Justin is a leading SaaS and Cloud specialist- he authors the influential "This Week in SaaS", blog and runs the largest SaaS community in the world, with over 28,000 members. Justin has been in IT over ten years, gravitating towards SaaS over the last five. This last year he's been consulting to companies large and small, helping them create successful SaaS products and strategy, and before that he was an officer at Endeavors Technology, the inventors of Application Virtualisation.
Job title: Cloud Strategist
Mobile: 0789 475 5178
Email: jpirie@mimecast.com

Cloud Security: Whose responsibility is it anyway?

by Rik Ferguson, Director of Security Research & Communications, Trend Micro EMEA

While commercial pressures to move IT resources to the cloud mount, security still remains the number one stumbling block in the adoption of cloud services by businesses, particularly in the area of public cloud infrastructure.

According to research last year by IDG Research Services, while nearly half of large companies had enterprise applications or business processes running in the cloud or planned to begin migration in the next year, two thirds did not have a cloud security strategy. Companies appear to be putting their head in the sand when it comes to data governance in the cloud – with research from Gartner indicating that 40% of virtualisation projects take place without the involvement of the security team.

With targeted attacks by cybercriminals on cloud providers on the rise, the industry has been making moves to address cloud security provision, including the forming of the Cloud Security Alliance and the signing of the Cloud Security Manifesto. Standards are being agreed and guidelines drawn up, and corporates are increasingly looking for greater disclosure from their cloud partners.

But could it be that traditional attempts to secure cloud computing have been focused on the wrong area? By throwing all the responsibility on cloud security vendors, the issues don't actually go away – they just become someone else's issues. The real problem for corporates looking to benefit from the cloud is around data governance – it's the corporate's responsibility to look after their own data and it's ultimately their problem if sensitive data gets into the public domain.

It's an issue that has been and will continue to be highlighted time and again, as sensitive data falls into the wrong hands. If you don't know what security measures have been put in place by your cloud hosting partner then it's impossible to say this will not happen. Companies have attempted to protect themselves by mandating standards, and conducting audits, but while there are people involved in the process, there's always the danger that data could be leaked from the inside.

The obvious answer is to encrypt all the data that a corporate hands over for hosting to a cloud service provider. The challenge then becomes about access management, authenticating the identity and integrity of cloud servers as they attempt to get at the data.

What's the problem?

When resources move to the cloud, the traditional segmentation that exists within a corporate environment disappears as services are grouped together in order to gain the efficiencies from sharing hardware resources. Highly sensitive data that would have been locked away in a secure environment now sits on the same box as less sensitive data that might only have been password protected.

This new myriad of services introduces new risks to the enterprise. The castle walls that previously existed between different departments like finance, personnel and marketing have disappeared, and these are essential for governance and compliance. The separation of duties that had been tied down and is mandated in standards like the PCI Data Security Standards and Sarbanes-Oxley is all thrown up into the air again in the cloud.

Secondly, previously external facing systems are now linked up to systems which would normally be internal. This means your corporate website is now running alongside your payroll system on effectively the same physical server – you'd never have done that historically but in the new world you do. And looking a little wider, where different companies are sharing cloud infrastructure, data from one company is sitting alongside data from another.

Finally, taking this into the public cloud space, with a consumer service like Amazon EC2, the implications of pooling all this data are huge. In a sense, you are putting it all on a plate for the cybercriminals, because once they are inside this environment, they have access to all the data, untraceable to the source. And they don't have to break through the firewall, they can just sign up and become a customer and attack it from the inside.

Encrypting sensitive data not only protects it from other customers but also from rogue administrators trying to access it from within the cloud service provider. But the actual encryption is not the problem – standard AES Encryption is a mature technology that's been deployed successfully for many years. What you find is that as soon as you solve the data encryption challenge, you come onto another challenge around access management.

Who goes there?

The challenge of authenticating servers is not straightforward like user authentication. If you think about encryption for a laptop, as someone turns the laptop on, you would ask them to enter a pass phrase and that would unlock the disk and allow the operating system to boot up.

The trouble in the cloud computing world is everything's much more dynamic. Overnight, you've only got one web server, then in the morning when people start coming in, you want to spin up another three or four to deal with the load. User intervention is also a problem. When a user is on their laptop. they've got an interface, and you can collect data from them. But when a machine's spinning up out of a cloud in the data centre or in the public cloud, there isn't a natural thing to get hold of.

So what you need is a system that checks for two things – identity and integrity. First of all, is this really your machine, rather than someone else pretending to be your machine? Secondly, you need to know about the integrity of the system – is there a firewall in place, are the anti-virus signatures up to date, when did you last check that there wasn't a piece of data-stealing malware on the machine that is going to steal the data as soon as you unlock it?

If you check those two items before you release the keys to the box, then you can be pretty sure that you're protecting the data. Introducing a key server brings the added advantage of achieving separation of duties. Either the cloud service provider is looking after your servers and the security vendor is looking after your key, or you bring the keys back in house leaving only encrypted data in the hands of your outsourcer.

So whose responsibility it is to secure data in the cloud? Ultimately, enterprises will pay for it because it's their data that needs to be protected and their responsibility. But there are a lot of smaller businesses looking for the benefits of cloud deployment, and they'll just look to the service providers, who in turn can offer it as a value-added service.

The service providers really like the concept too because if a piece of sensitive data ends up in the public domain, they don't want it coming back to them, with a company claiming they must have leaked it. The provider can say that even if they had leaked the data, there's no way it could have come from them because it's encrypted and they don't have access to the encryption keys.

Trend Micro recently presented at Infosecurity Europe 2011.

VISIT US AND FIND OUT MORE
SWISS CYBER STORM 3
12 - 15 MAY 2011
FH RAPPERSWIL (CH)
WWW.SWISSCYBERSTORM.COM
BYTE ME!