

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

CLOUD COMPUTING



CLOUD SECURITY
HACKING THE CLOUD.
DID SOMEONE SAY SWISS CHEESE?
A SECURE CLOUD?



Vol.7 No.05
Issue 05/2012(53) ISSN: 1733-7186

PLUS

TOOL TIME: SECURE DELETION
(IL)LEGAL: ZOMBIES AND ECONOMICS – WHY THE
LAW INHIBITS GOOD SECURITY BUSINESS CASES



eLearnSecurity
Forging security professionals

PENETRATION TESTING PROFESSIONAL v.2



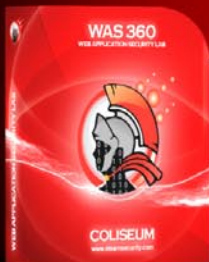
Online Penetration Testing Course



www.elearnsecurity.com

- ✓ 2400+ interactive slides
- ✓ 9 hours video training material
- ✓ 100% hands-on with Hera Labs
- ✓ Extremely in depth and thorough contents
- ✓ Leads to Hands-on ECPPT certification
- ✓ 3 Knowledge domains
- ✓ Web application penetration testing
- ✓ Network penetration testing
- ✓ System security and Exploit Development
- ✓ Lifetime access to course material

Now the most Hands-On course on Penetration Testing :



Coliseum Web Application Security Lab

- ✓ 14 real world vulnerable websites
- ✓ User-exclusive sand-boxed access to labs
- ✓ Multiplatform : PHP, MySQL, MS SQL Server
- ✓ Practice OWASP Top 10
- ✓ Web app analysis, XSS, SQLi, LFI/RFI, CSRF
- ✓ Get inline help if you get stuck



Hera Penetration Testing Virtual Lab

- ✓ VPN access from your own Attack box
- ✓ User-exclusive, non-shared access to labs
- ✓ Guided Exploitation Walkthrough
- ✓ Windows Servers, BSD, Linux, Firewalls, IDS's
- ✓ Different Labs with Different Network topologies
- ✓ On-demand: No Activation, No Expiration

www.elearnsecurity.com

HEY! TEACHER!

LEAVE THEM KIDS
ALONE!



THE MOST ADVANCED COURSE
ON PENETRATION TESTING

IS SELF-PACED!

WWW.ELEARNSECURITY.COM



HAKIN9 team

Editor in Chief: Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Managing Editor: Marta Jabłońska
marta.jablonska@hakin9.org

Editorial Advisory Board: Gurav Shah, Craig S. Wright,
Skyler Onken, Ivan Venclova, Mohsen Mostafa Jokar,
Mervyn Heng, Christopher Pedersen, Gary S. Milefsky,
Julian Evans, David Prokop

Proofreaders: Donald Iverson, Michael Munt, Elliott Bujan, Bob Folden, Steve Hodge, Jonathan Edwards, Steven Atcheson

Top Betatesters: Ivan Burke, John Webb, Nick Baronian, Felipe Martins, Alexandre Lacan, Rodrigo Rubira Branco

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


DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@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

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 all,

Spring finally! After long and cold winter I was looking for an inspiration. I was sitting in a park on a sunny day, enjoying the wonderful weather. Suddenly dark, grey clouds showed up on the sky. This when I thought "Let's make an issue about Cloud Computing". Few authors agreed with me and here is what we have for you First article by Gurav Shah – "Cloud Security". There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware – be it computing, storage or even networking. This introduces an additional layer – virtualization – that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist.

Next article by Gary s. Milefsky "Hacking the Cloud. Did someone say Swiss Chees?" What is the cloud? Is it the glorified internet? Is it an ISP who likes to run virtualized servers? Once we truly understand what Cloud Computing is, then let us look at the holes in the Cloud...I argue that yes, the cloud is like Swiss Cheese, loaded with holes and ripe for exploitation. By the way, who is responsible for compliance when it comes to 'moving' everything to the cloud – is it the Cloud Service provider or is it you, the company providing a service to end-customers/consumers? 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.'

Christopher Pedersen in an article "Do You Have The Correct Cloud? Cloud Privacy" talks about types of cloud and how to keep your information private.

We are starting to move to IPv6 and the cloud. Right now, the uptake is minimal at best with very few early adopters for all of the hype. The climate is changing. Soon, IP addresses will be on everything and even the concept of non-disclosure agreements and contracts designed to protect intellectual property will require that we consider the nature of the cloud and the Internet as a platform for contractual negotiation. Read in more in "Secure commerce in the Mist" by Craig S Wright.

We have a new section in our magazine. "Extra Articles". We present there articles which are not related to the main topic of the magazine, but are very valuable and interesting. Check them out!

Like in every issue at the beginning you will find short news from IT world and also we recommend Tool Time and (II)legal columns.

I wish you a very good reading!

Marta & Hakin9 Team

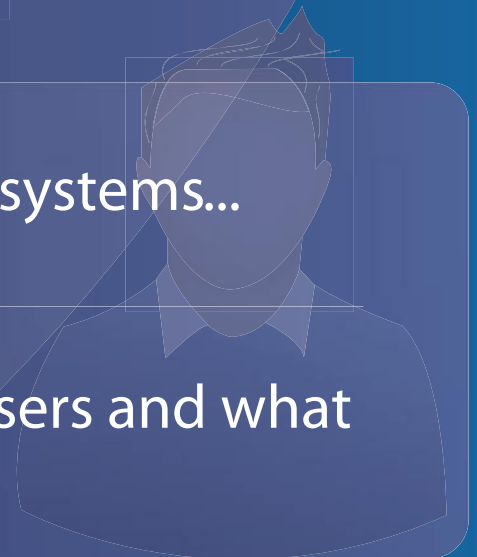
Be reactive...

- 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.

IN BRIEF

8 IN BRIEF

by Armando Romeo, *eLearnSecurity and ID Theft Protect*

As usual specialists from companies eLearn Security and ID Theft protect will share with us latest news from IT security world. Read it to up-date yourself.

BASICS

10 Cloud Security

by Gurav Shah

There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware – be it computing, storage or even networking.

18 Hacking the Cloud. Did someone say Swiss Cheese?

by Gary S. Milefsky

What is the cloud? Is it the glorified internet? Is it an ISP who likes to run virtualized servers? Once we truly understand what Cloud Computing is, then let us look at the holes in the Cloud...I argue that yes, the cloud is like Swiss Cheese, loaded with holes and ripe for exploitation. By the way, who is responsible for compliance when it comes to 'moving' everything to the cloud – is it the Cloud Service provider or is it you, the company providing a service to end-customers/consumers? 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.

24 A Secure Cloud?

by David Prokop

As IT professionals we can't look into our inboxes without seeing a new whitepaper or webcast related to the cloud. While usually helpful, rarely does the information address our favorite topic, security. In reality can a cloud based system protect your data? In short, yes. Security threats to a system based on cloud services are similar to a traditional data center the threats just manifest in a

different way. The two primary differences are that your organization will share infrastructure resources with other organizations. Second, your organization trusts the strength of the selected cloud vendor's security infrastructure, policies, and procedures. During the selection of your organizations cloud computing services look in depth at the following areas and ensure that your selected vendor has addressed each topic and meets your organizations security policies and regulatory requirements.

28 Do You Have The Correct Cloud? Cloud Privacy

by Christopher Pedersen

In both personal and business settings, clouding can be a great tool. But how do you know that when you upload your information into the cloud it is private? Can anyone just connect to your data-store and start perusing through your information? These are a few questions that we will discuss. If you don't know what the correct type of cloud is that you need, you may fail. The reason for this failure could primarily be a privacy issue. Yes, Privacy. The first question is, why are you using the cloud – business or personal? Most people don't use the right type of cloud. Are you launching applications, servers, or developing? Are you using the correct cloud type that also delivers the correct amount of privacy?

32 Secure commerce in the Mist

by Craig S. Wright

We are starting to move to IPv6 and the cloud. Right now, the uptake is minimal at best with very few early adopters for all of the hype. The climate is changing. Soon, IP addresses will be on everything and even the concept of non-disclosure agreements and contracts designed to protect intellectual property will require that we consider the nature of the cloud and the Internet as a platform for contractual negotiation.

EXTRAARTICLES

36 Understanding Cyber Warfare and its Strategic Applications

by Skyler Onken

Simplicity is very important in every aspect of warfare. It is very difficult to coordinate such a large group of people to do a variety of tasks perfectly synchronized with each other. Every level of complexity adds an exponential amount of time that is needed to train and rehearse the coordinated effort. Because of this cyber assets should keep their tasks relatively straight forward when working within a combined arms mission. When follow on units will be relying upon the efforts of a non-kinetic cyber force, it

creates a large amount of “what-if” scenarios for that unit. Cyber assets should be given specific tasks as a form of fire support, not to be seen as a maneuvers element itself when in a combined arms environment.

42 Understanding the Crime Revolution

by Ivan Venclova

Our Internet Earth is currently too small to host all of our ideas because our space is defined by IPv4 address limitation. Asian companies, for example, can't park anywhere or build anything new because they are officially out of IP addresses. We have a sound solution, IPv6, and it is scheduled to take affect soon. Once it is in place our mega-technology-churches will create new neighborhoods full of buildings and parking lots and aggressively recruit members away from already existing networks by implementing seeker-friendly approach based on intensive market research and targeted advertising. This will be accomplished in order to re-pay their business loans, in the name of our personal desires and this will change our neighborhood crime ratings again.

48 Using Social Engineering to reconnaissance your victim

by Mohsen Mostafa Jokar

Social Engineering is a phase of hacking, That including the External reconnaissance. It is nontechnical approach to breaking a system of network. It is deceiving users of a system. with social engineering hacker convincing user to perform acts useful. Hacker cab be earn information about victim. Social engineering is a important phase because hacker can use it to attack the human element.

TOOL TIME

54 Secure deletion

by Mervyn Heng

The Internethas empowered us to do more with our electronic devices. We do everything from our taxes to shopping and sending private messages. Our devices become a hotbed of personal data that is of interest to malicious parties. Deletion of files and caching is insufficient in preventing harvesting of your information that resides on your devices. The solution is secure deletion or wiping to overwrite those files with random data to eliminate the chances of data recovery.

(IL)LEGAL

58 Zombies and Economics – Why the Law Inhibits Good Security Business Cases

by Drake

Considering information security as a standalone good or service that is demanded specifically by business leadership is incredibly misleading. A while ago, I was doing some academic research into cost models for information security. As part of this, I developed a panel of experts to bounce some ideas off, drawing on individuals with extensive bodies of security experience in banking, government, telecoms, and a number of other areas. One of the ideas that was discussed was that organisations don't, in fact “buy security”.

Learn
Web Application Security
with...



Coliseum

Virtual labs
100% practical hands on
training
by eLearnSecurity

FIND OUT
14 educational challenges

- ✓ Real world scenarios
- ✓ No set-up time
- ✓ Play on MS SQL Server
- ✓ Got stuck? We support!

OPENX AD SERVERS HACKED TO DISTRIBUTE MALWARE

Sophos researchers have identified several OpenX ad servers that have been compromised by malware. The malware is redirecting users to Web sites that push malware from exploit sites. iFrame attacks are common security issues for all browser types. In this instance OpenX ad servers were delivering a malicious JavaScript file called Troj/JSRedir-EF. The iFrame is added by the script which then loads the malicious content from a TDS, controlled by a group called BlackAdvertsPro.

Source: ID Theft Protect

ANONYMOUS HACKERS THREAT SECURITY COMPANY IMPERVA

Members of Anonymous have announced plans to target security firm Imperva Inc, which recently published a report claiming that the majority of Anonymous members have a very low to modest skill level. Anonymous has now taken exception with this announcement: *Although we do not see you as any form of threat we have concluded that your interest and views may become a mild nuisance in the future. Therefore you, yourself, will now become a target. You have angered the hive and the hive has spoken. Now you will feel the full fury of Anonymous... Imperva – expect us.*

Source: ID Theft Protect

INTERNET SCAMMERS TARGETING PINTEREST USERS

Scammers have launched a paid advertising campaign on Facebook targeting Pinterest users. The malicious advert uses social engineering techniques to lure Pinterest users to a website promoting Pinterest bots – it's a simple lure on "how to make money with Pinterest". The embedded URL in the ad takes users to a Web page that features a survey (nothing new here) which offers the user a Visa gift card and an e-mail address submission form for a possible subscriber. Pinterest isn't alone in being targeted in this way.

Source: ID Theft Protect

Ukraine Shuts Down Malware Exchange Website

Ukrainian police recently shut down the malware exchange Web site VX Heavens. VX Heavens billed itself as a vault for information, providing virus-writing tutorials as well as malicious code samples. The Web site had been running for many years. The Ukrainian

authorities didn't like what the owners were doing so confiscated their servers for forensic investigation. Creation and distribution of malware code is a major business for the underworld.

Source: ID Theft Protect

YAHOO! JOINS THE DNT CROWD A LITTLE LATE

Yahoo! is rolling out a Do Not Track (DNT) header feature across its entire operation. The tool will be implemented on its Right Media and Interclick properties. Yahoo! is a little behind the times with the DNT rollout though. Microsoft, Apple and Mozilla already implemented DNT sometime ago. Google also launched DNT inbuilt into Chrome last month (February). The DNT feature sends a HTTP header (DNT=1) to the ad networks (DAA) which means the user has initiated the DNT feature. The HTTP header approach requires no additional software – so no add-ons, cookies, extensions etc. For further information concerning the DNT story.

Source: ID Theft Protect

FLASHBACK

Another massive Mac virus has spawned – Flashback. It targets a vulnerability in the Mac version of Java and has already compromised as many as 600,000 Macs worldwide. This staggering number was first released by the Russian antivirus company Dr. Web and was later confirmed by Kaspersky. This is not the first time Flashback has come around; it initially was targeting Adobe weaknesses several months ago. Adobe quickly patched its vulnerability so the makers of Flashback started targeting a Java weakness. Apple and Oracle have now both released fixes to harden their software. Apple has also now released a removal tool to take care of the threat once infected.

Most security experts are frustrated with how Apple is handling these types of attacks. The vulnerability has been known about for months but Apple did not patch its side of the weakness until now. The only announcement from Apple is that they plan to make the next major version of OSX much more secure using features like XProtect and Gatekeeper. XProtect is an antivirus included with the OS that run as part of the OS; Gatekeeper involves a process in which developers register with Apple to be verified. A user can then allow their Mac to only install from verified developers and block everything else. The security experts will be watching as Macs security woes are only just beginning.

Source: Schuyler Dorsey – ELS

Master Boot Record Ransomware

Trend Micro has uncovered a new ransomware that goes after the master boot record of computers. Most ransomware encrypts files and demands money to have them unencrypted but this ransomware actually encrypts the master boot record. As soon as the infection takes hold, it automatically reboots the computer so it takes effect. The computer boots into a new screen with instructions on how to pay the makers of the virus so they may hand over the code to unencrypt your boot record in return.

Trend Micro stated that there have been almost 9,000 traces of ransomware just in the past thirty days and the United States remains the largest percentage of those.

Source: Schuyler Dorsey – ELS

MS12-020

A known vulnerability has existed in the RDP portion of Windows versions all the way up to Windows 7 since August when it was exploited by the Morto worm. Microsoft finally released the security patches in March which fixed the issue and stopped the threat of remote code execution. Just days after the security patch was released, a confirmed legitimate exploit was spotted in the wild. Researchers say it currently crashes or causes a denial-of-service condition (but does not initiate full remote code execution yet). Even though the current exploit does not grant code execution, the denial of service condition is the first step down that road. Customers of Windows products are advised to make sure their systems are patched as soon as possible to mitigate the threat of a worm down the road.

Source: Schuyler Dorsey – ELS

HP Switch Malware

HP has announced that customers who have purchased Procurve 5400 zl switches should be cautious with the compact flash cards shipped with them. Many of the compact flash cards may be infected with malware and use of it could result in the system being compromised. This pertains to the switches purchased after April 30th, 2011 with the serial numbers listed in their advisory. There are currently two fixes: customers can download a 'software purge' script from HP which will automatically remove all malicious items from the card (with no switch downtime) or they can request a hardware replacement of the Management Module. HP has yet to announce what malware is on the cards as well as where it originated.

Source: Schuyler Dorsey – ELS

Android SMS Malware

Researchers at NQ Mobile and North Carolina State University have discovered a new Android malware circulating that is completely controlled by SMS called TigerBot. Once installed, it does not create an icon but registers itself as a legitimate application on the device and waits for SMS instructions. According to NQ, "Upon receiving a new SMS message, TigerBot will check whether the message is a specific bot command. If so it will prevent this message from being seen by the users and then execute the command accordingly". Commands that TigerBot accepts include recording of surrounding sounds, recording of phone calls, reporting of GPS coordinates and changing of network settings. Experts advise that as usual, users only download applications from legitimate sources such as Google Play.

Source: Schuyler Dorsey – ELS

MAC OS X LITTLE SNITCH DEFINES WHO YOU CAN TRUST

If you use a Mac and you want to manage and control the flow of data that leaves your computer, then I suggest you might want to use Little Snitch. Tech geeks will know about this clever privacy tool, but the masses of my readers aren't technical. So, I thought I would explain further why you should download and install Little Snitch. Little Snitch allows you more control than a system firewall – in affect it allows you to have control by intercepting unwanted connection attempts, allowing you to have control on how to proceed. It informs you whenever any program attempts to establish an outgoing connection. You choose to allow or deny the connection, or define a rule to handle future connection attempts.

Source: ID Theft Protect

IPHONE BLACKBERRY AND ANDROID MOTION SENSOR EXPLOIT

A team of researchers have devised an experimental Android-based Trojan called TapLogger that can manipulate the mobile onboard motion and orientation sensors to crack stored passwords. Motion and orientation sensors can also utilise the vibration sensor of a mobile device, which could then activate a Trojan to capture keyboard inputs using a malicious keylogger.

Source: ID Theft Protect

Cloud Security

With the increasing use of Web and web application, Cloud Computing has become news. Every application wants to be on the Cloud. The increasing rise of data over the Cloud has also attracted hackers from around the world towards the Cloud. With the increasing use of Cloud Computing the need for Cloud Security is also rapidly growing.

What you will learn...

- Basic knowledge on Cloud Security
- Different aspect of Cloud Security from the service providers

What you should know...

- Brief information on Cloud Computing
-

This paper tries to explain the different aspect of Cloud Security from the service providers as well as end user point of view. This paper will also try to address the current cloud security concerns raised.

Before we head off to Cloud Security, let us first understand the basics of what Cloud Computing is.

What is Cloud Computing?

Cloud computing is the delivery of providing various computing products as services. Shared resources, software, infrastructure, information and data is provided as a paid service to the end customer over the web. Cloud computing provides these various services without requiring cloud users to know the location and other details of the computing infrastructure. Every user accesses data on the cloud through a version of the browser developed for various devices.

Service models

Cloud computing providers offer their services according to three fundamental models:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

Infrastructure as a service (IaaS)

Infrastructure as a Service is a provision model in which an organization outsources the equipment used

to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Platform as a service (PaaS)

Platform as a Service is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Software as a service (SaaS)

Software as a Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Deployment Models

There are 4 different ways in which Cloud can be deployed and various services of the cloud can be used:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud

Private Cloud

Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall.

Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their customers within the corporation.

Marketing media that uses the words private cloud is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's *Elastic Compute Cloud (EC2)* or *Simple Storage Service (S3)*.

Public Cloud

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The term public cloud arose to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud

computing technologies, such as virtualization. A private cloud is managed by the organization it serves. A third model, the hybrid cloud is maintained by both internal and external providers.

Examples of public clouds include *Amazon Elastic Compute Cloud (EC2)*, IBM's *Blue Cloud*, *Sun Cloud*, *Google AppEngine* and *Windows Azure Services Platform*.

Hybrid Cloud

A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms.

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 Simple Storage Service (Amazon S3)* for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without

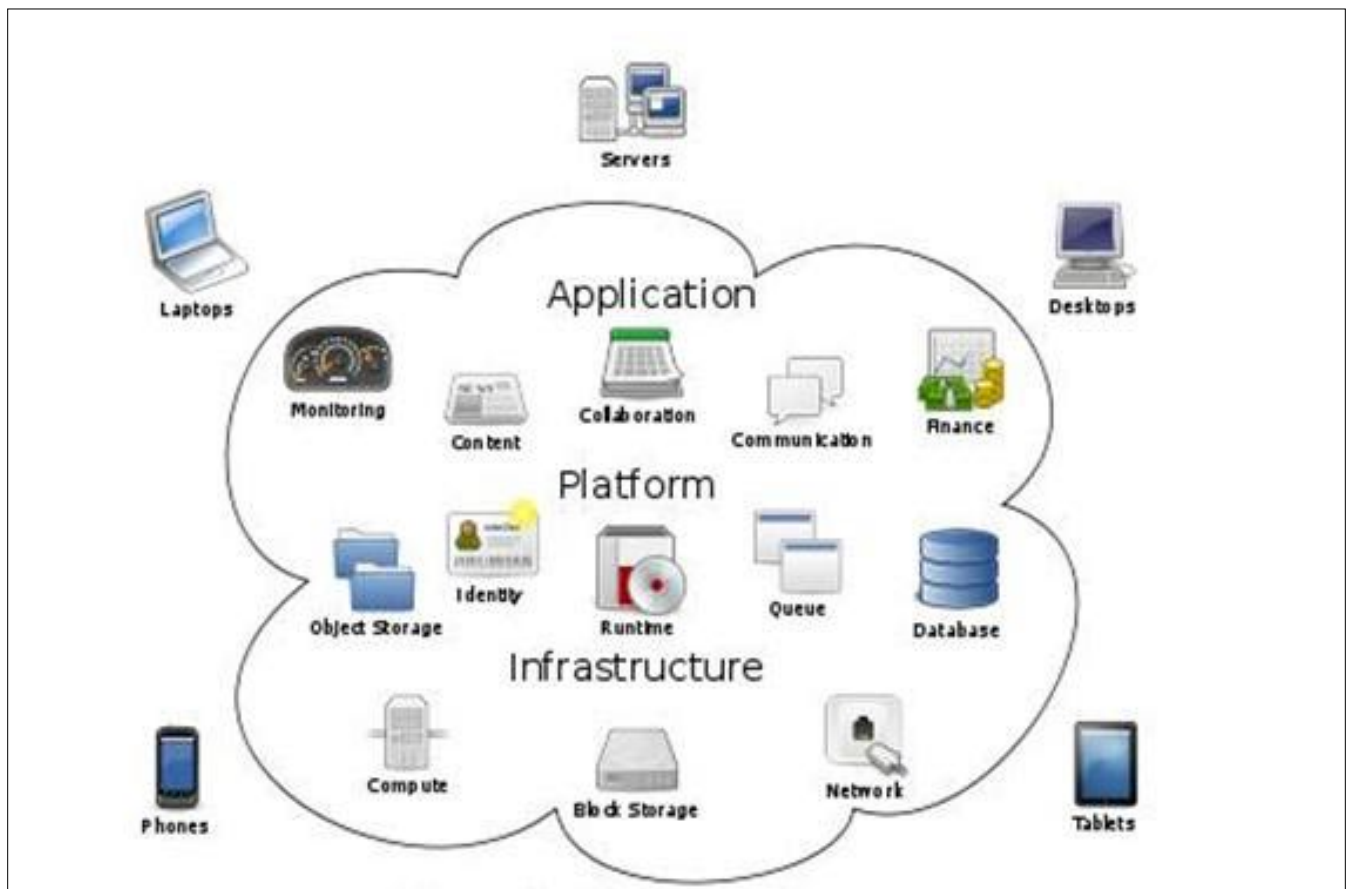


Figure 1. A view of Cloud Computing

exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid cloud is also referred to as hybrid IT.

Community Cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

Cloud Computing Security

There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS

and underlying hardware – be it computing, storage or even networking. This introduces an additional layer – virtualization – that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or *hypervisor*. While these concerns are largely theoretical, they do exist.

Cloud Security Dimensions

Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices. While cloud security concerns can be grouped into any number of dimensions these dimensions have been aggregated into three general areas:

- Security and Privacy
- Compliance
- Legal and Contractual Issues.

Security and Privacy

In order to ensure that data is secure and that data privacy is maintained, cloud providers attend to the following areas:

Data protection

To be considered protected, data from one customer must be properly segregated from that of another; it

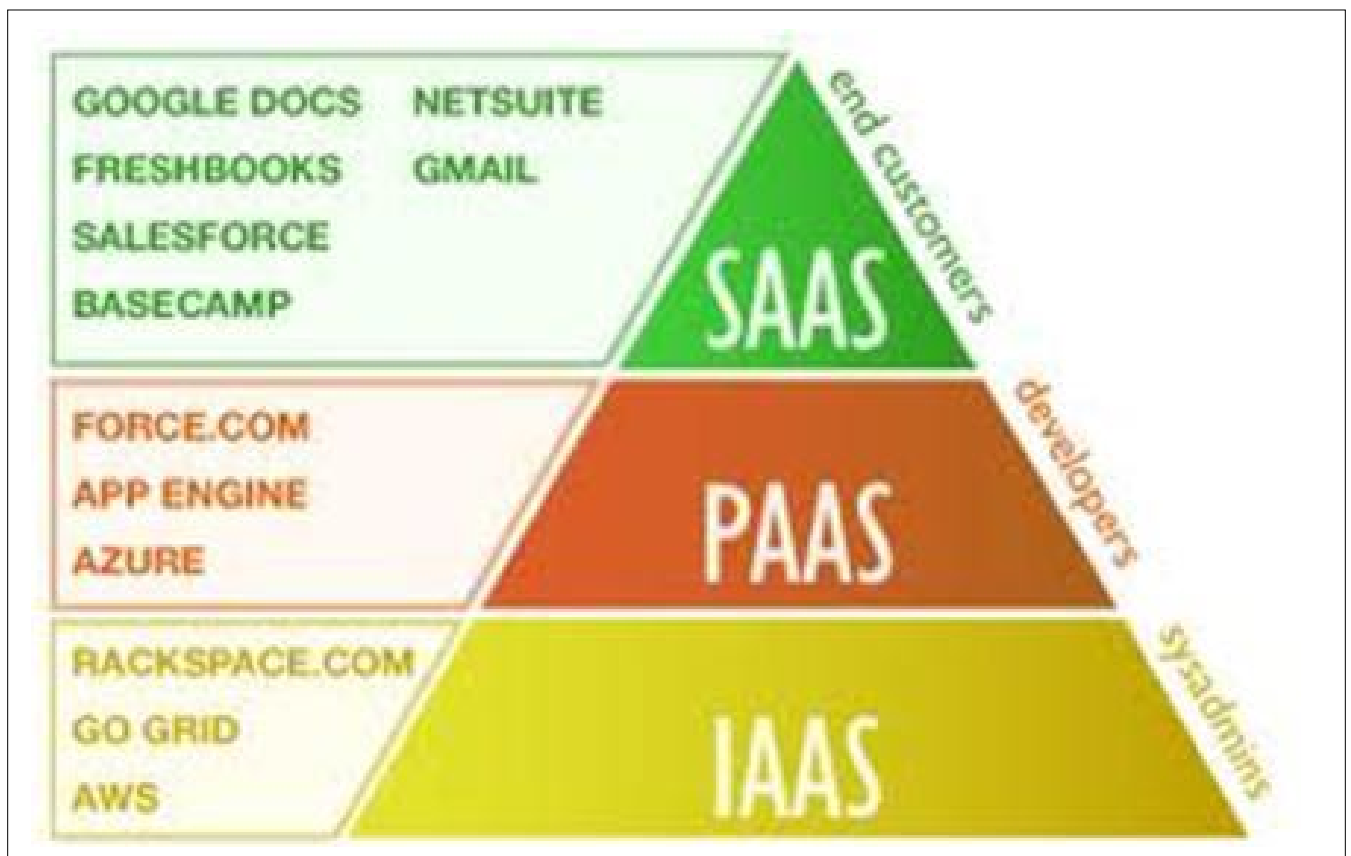


Figure 2. Tree structure of SaaS PaaS and IaaS model

must be stored securely when at rest and it must be able to move securely from one location to another. Cloud providers have systems in place to prevent data leaks or access by third parties. Proper separation of duties should ensure that auditing or monitoring cannot be defeated, even by privileged users at the cloud provider.

Physical Control

Physical control of the Private Cloud equipment is more secure than having the equipment off site and under someone else's control. Having the ability to visually inspect the data links and access ports is required in order to ensure data links are not compromised.

Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.

Physical and personnel security

Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.

Availability

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

Application security

Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

Privacy

Finally, providers ensure that all critical data are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Legal issues

In addition, providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country

Compliance

Numerous regulations pertain to the storage and use of data. Many of these regulations require regular reporting and audit trails. Cloud providers must enable their customers to comply appropriately with these regulations.

Business continuity and data recovery

Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered. These plans are shared with and reviewed by their customers.

Logs and audit trails

In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation

Unique compliance requirements

In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements. Using a cloud service provider can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.

Legal and contractual issues

Aside from the security and compliance issues enumerated above, cloud providers and their customers will negotiate terms around liability, intellectual property and end-of-service.

Public records

Legal issues may also include records-keeping requirements in the public sector, where many agencies are required by law to retain and make available electronic records in a specific fashion. This may be determined by legislation, or law may require agencies to conform to the rules and practices set by a records-keeping agency. Public agencies using cloud computing and storage must take these concerns into account.

Top 7 Threats to Cloud

Abuse and Nefarious Use of Cloud Computing Description

By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to

conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Impact

Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

Remediation

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Service models affected

- IaaS
- PaaS

Insecure Interfaces and APIs

Description

Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

Impact

While most providers strive to ensure security is well integrated into their service models, it is critical for

consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

Service models affected

- IaaS
- PaaS
- SaaS

Malicious Insiders

Description

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.

To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary – ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

Impact

The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

Service models affected

- IaaS
- PaaS
- SaaS

Shared Technology Issues

Description

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Impact

Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

Remediation

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.

- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

Service models affected

- IaaS

Data Loss or Leakage

Description

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

Impact

Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

Remediation

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

Service model affected

- IaaS
- PaaS
- SaaS

Account or Service Hijacking

Description

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Impact

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Service model affected

- IaaS
- PaaS
- SaaS

Unknown Risk Profile

Description

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns – complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications. Versions of software, code updates, security practices, vulnerability profiles, intrusion

References

- Wikipedia
- Search Cloud Computing
- Cloud Security Alliance

attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

Impact

When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

Remediation

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

Service Model affected

- IaaS
- PaaS
- SaaS

GAURAV SHAH

Senior Consultant – Righthshore Security Testing Team – Center of Excellence

Gaurav Shah has been working into the field of Information Security for the past 6 and a half years. He has an experience in Vulnerability Assessment and Penetration Testing of web applications, web services and Networks, as well as in building Threat Models for various Software architectures. Gaurav is certified in CCNA, CEH and Certified Vulnerability Assessor.

gaurav.a.shah@capgemini.com



ADVTOOLS SARL

SECURITY EXPERTS iPhone & iPad

- iOS security trainings
- iOS applications pentests
- Audits of mobile management systems (MDM)

Contact: info@advtools.com - Tél.: +41 22 301 91 00 - www.advtools.com

Hack in Paris 18-20 June, 2012

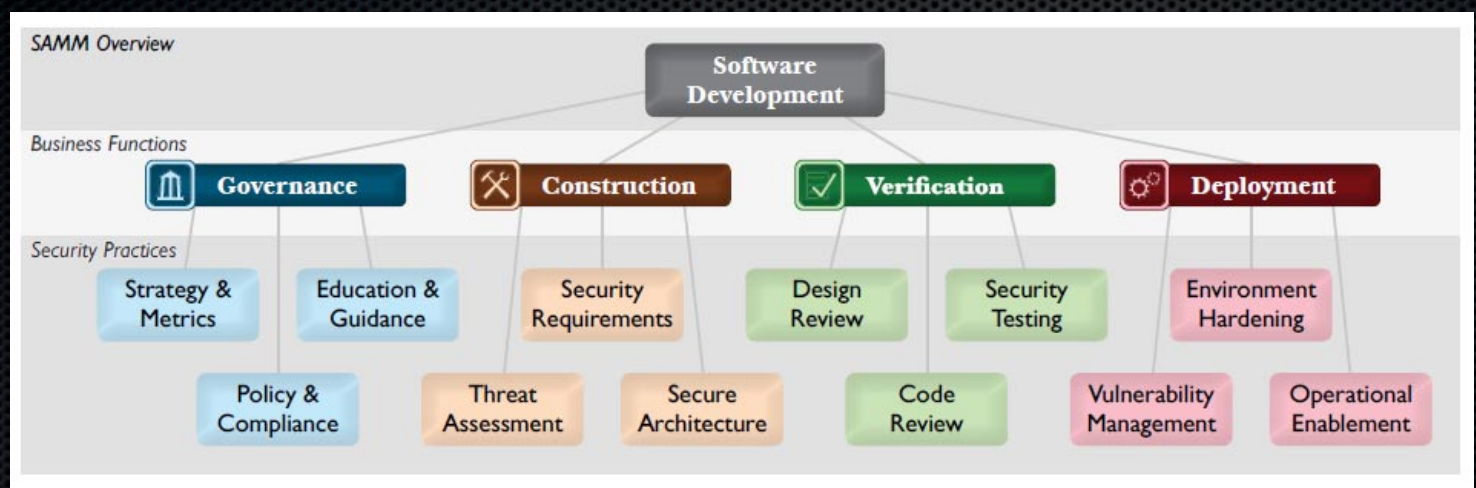
Training "iOS Applications Attack and Defense" Win an iPad!

www.hackinparis.com



OWASP Foundation

"We help protect critical infrastructure one byte at a time"



- 140+ Checklists, tools & guidance
- 150 Local chapters
- 20,000 builders, breakers and defenders
- Citations: NSA, DHS, PCI, NIST, FFIEC, CSA, CIS, DISA, ENISA and more..

Learn More: <http://www.owasp.org>

Hacking the Cloud

Did someone say Swiss Cheese?

I can't believe how much hype there is out there in regards to Cloud Computing. Every company that can add the word "Cloud" to their product or service offering seems to be doing so – Cloud Backups, Cloud-based Anti-virus, Cloud-based Management of Your Firewall, the list goes on and on....

What you will learn...

- The Basics of Cloud Computing
- Holes in the Cloud (like Swiss Cheese)
- Hacking and Hardening the Cloud

What you should know...

- What is a CVE®
- What is a Virtual Machine
- Vulnerability Management

But let's get real, shall we? What is the cloud? Is it the glorified internet? Is it an ISP who likes to run virtualized servers? Once we truly understand what Cloud Computing is, then let us look at the holes in the Cloud... I argue that yes, the cloud is like Swiss Cheese, loaded with holes and ripe for exploitation.

By the way, who is responsible for compliance when it comes to *moving* everything to the cloud – is it the Cloud Service provider or is it you, the company providing a service to end-customers/consumers? 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.

Defining "the Cloud"

I would like to summarize what the Cloud is based on the definition from my friends at the National Institute of Standards and Technology (*NIST.gov*). Accordingly, 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

See Figure 1

1. *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.
2. *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).
3. *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.
4. *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.

5. *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

See Figure 2

1. *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.
2. *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

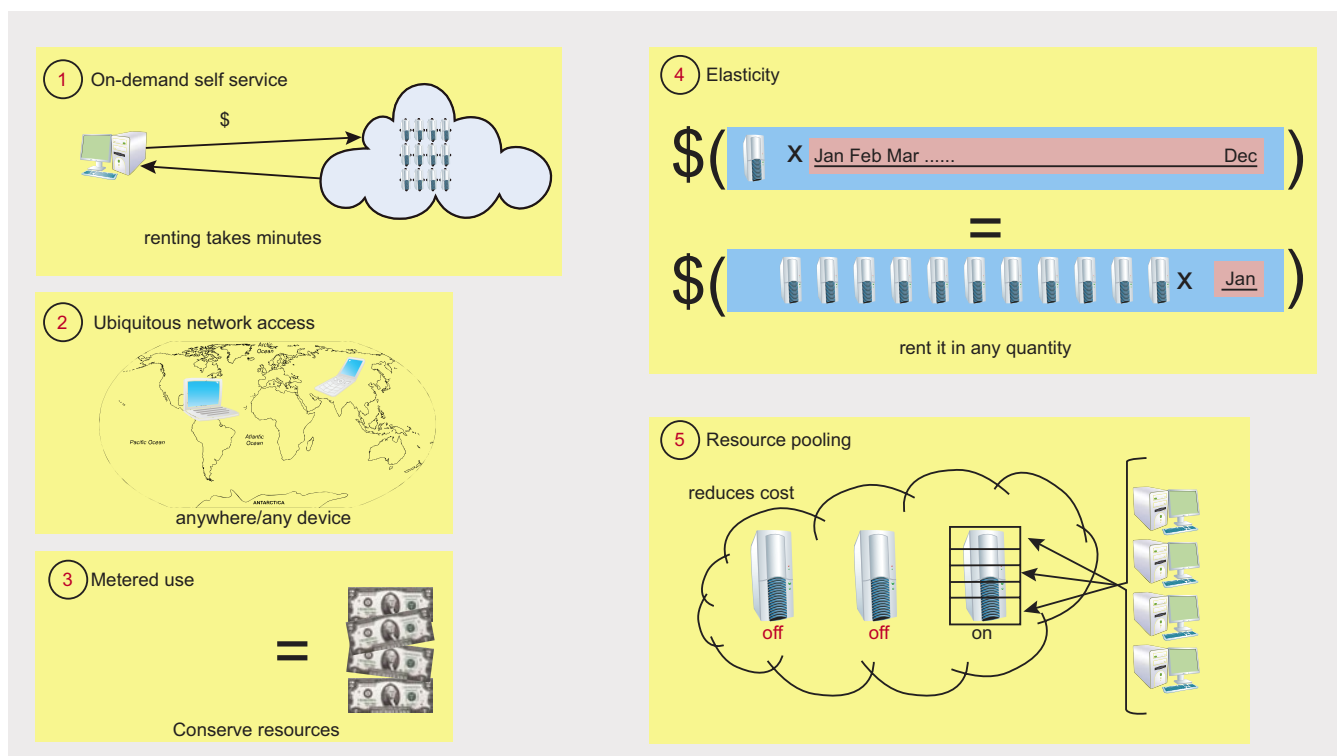


Figure 1. Essential Characteristics of the Cloud (Source: NIST.gov)

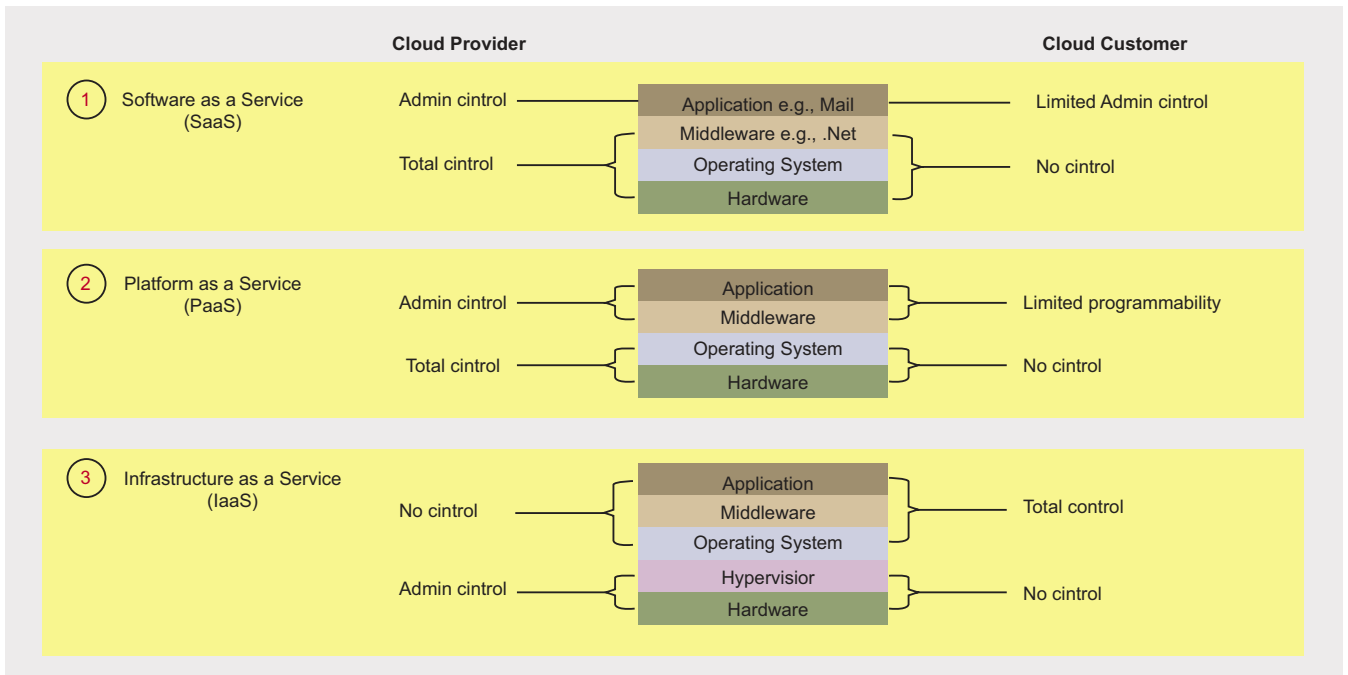


Figure 2. Service Models of the Cloud (Source: NIST.gov)

deployed applications and possibly application hosting environment configurations.

3. **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).

- the organization or a third party and may exist on premise or off premise.
2. **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.
3. **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.
4. **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).

Deployment Models

See Figure 3

1. **Private cloud.** The cloud infrastructure is operated solely for an organization. It may be managed by

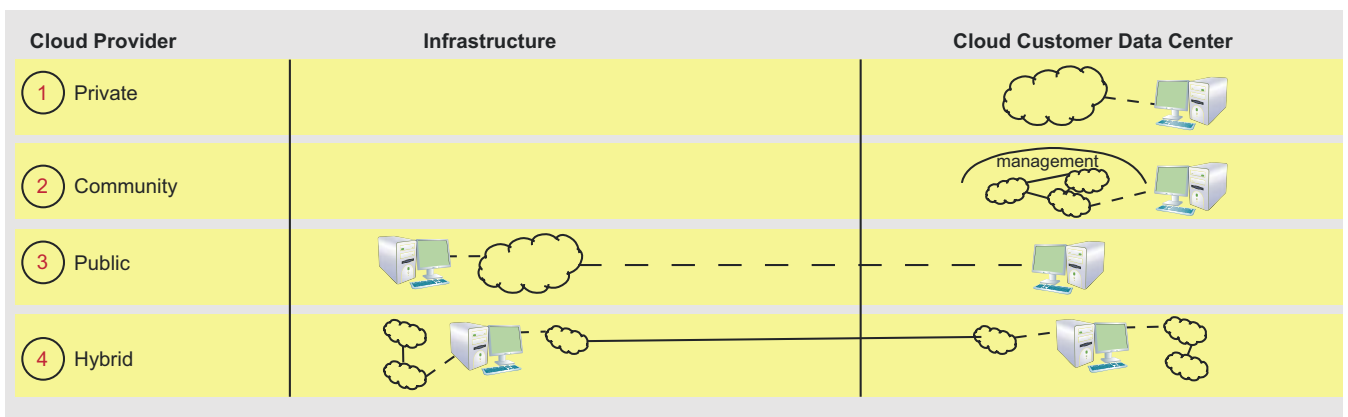


Figure 3. Deployment Models of the Cloud (Source: NIST.gov)

Security Risks in the Cloud

I've found the following areas of risk that you can address by ensuring you are completely satisfied with the *service level agreement* (SLA) of your Cloud Computing service provider:

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 identifiable 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/wiki-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 outweigh 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, you have a Cloud with as many holes as Swiss Cheese.



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>).



CODENAME: SAMURAI SKILLS COURSE



<< Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , any where)
- Our Course is Totally Different from Other Courses (new Techniques)

We have Real World Hacking/Penetration Testing Lab with Over 20 Real Target

A Secure Cloud?

As IT professionals we can't look into our inboxes without seeing a new whitepaper or webcast related to the cloud. While usually helpful, rarely does the information address our favorite topic, security. In reality can a cloud based system protect your data? In short, yes.

What you will learn...

- What is in the cloud
- Securing your services

What you should know...

- Basics on Cloud Security

Security threats to a system based on cloud services are similar to a traditional data center the threats just manifest in a different way. The two primary differences are that your organization will share infrastructure resources with other organizations. Second, your organization trusts the strength of the selected cloud vendor's security infrastructure, policies, and procedures. During the selection of your organizations cloud computing services look in depth at the following areas and ensure that your selected vendor has addressed each topic and meets your organizations security policies and regulatory requirements.

What's in the Cloud?

In nature the cloud comes in a shapes and sizes. In the IT world, cloud architecture can be broken into operational or deployment models that provide cost-effective computing resources all of which is accessible over the internet. Cloud computing offers an organization several advantages or characteristics including:

- On-demand deployment of an organization's IT environment or applications.
- Decrease infrastructure hardware cost by pooling resources.
- Ability to balance system resources up or down to meet user demand also called *Rapid Elasticity*.

- Broad Network Access is the ability to access an organization's applications from any location with Internet accessibility.
- The capability to monitor metered cloud resource (e.g., network, server, storage, and software) usage, or measure service, to scale resource to adjust for need or cost.

Cloud computing consist of public, community, private, and hybrid operational models. Within a Private cloud, services and infrastructure are owned and managed by a single entity and therefore responsible for managing their own security. One of the benefits of a private cloud is that it provides greater control over resources usage, unlike public cloud resources. Cloud bursting is the result of an organization's private cloud running out resources and leverages public cloud resources, sometimes on a temporary basis, to ensure system or service availability. Organization's utilizing clouds based on the community model share a common need (i.e., compliance, application, security posture, etc.) By sharing the resources of the common need cost of the resource is reduced. Public cloud model provides a wide range of cloud computing services to the general public that are charged based on resources usage. The public cloud model offers both application and infrastructure resources which can only be accessed via Internet. Access may be accomplished through cloud carrier or a dedicated *virtual private network* (VPN). The

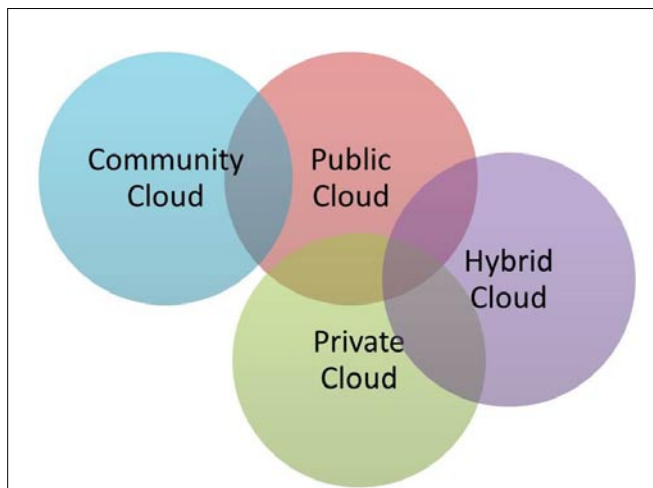


Figure 1. Cloud Model Relationship

common services from vendors such as *Amazon Elastic Compute Cloud* (Amazon EC2), Google, and Microsoft offer cloud services such as SaaS, IaaS, and PaaS.

SaaS (*Software as a Service*) allows an organization or IT department to purchase and almost immediately utilize an application developed by an outside organization. The software application, supporting infrastructure and platform management, including security, is addressed by other groups. This removes the need for an organization to install software on an organization owned asset and storage thus simplifying or completely eliminating maintenance and support of the application. While SaaS offers quick application deployment solution the application is still vulnerable to DDoS attacks or privilege escalation due to a misconfigured platform or device. Applications should be architected to mitigate an interruption in the service.

IaaS (*Infrastructure as a Service*) providers stand up the physical and virtual environments including servers, storage devices, and network devices plus cabling, HVAC and power. Although the services may be accessed remotely, your organization is left responsible for installing, patching and maintaining the operating systems and applications. Depending on your IT staff skill level and availability this could become an issue

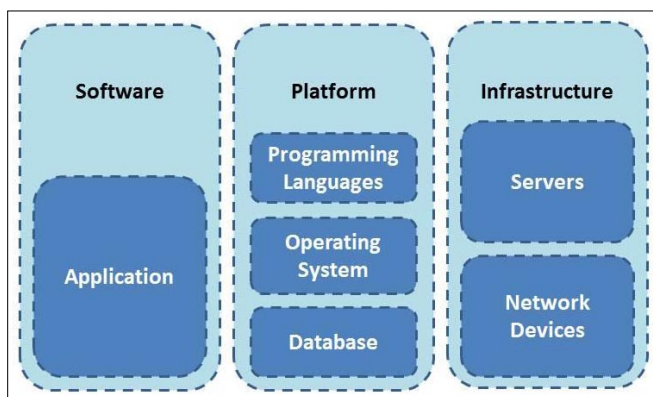


Figure 2. SaaS Customer Responsibilities

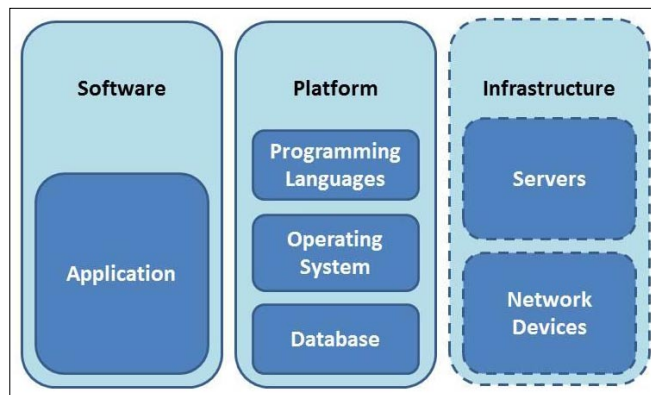


Figure 3. IaaS Customer Responsibilities

depending on the size of your organization's cloud environment. IaaS implementations are vulnerable to poorly coded or misconfigured applications and also vulnerable to weaknesses existing in the network or virtual infrastructure. Regular penetration testing and auditing should take place to identify issues.

Typically PaaS (*Platform as a Service*) implementations include operating system, multiple programming languages, database, and web server. Your organization is responsible for the installation, patching and maintenance of your application on each platform. The benefit a PaaS solution is that it offers your organization's developers an environment to develop and test applications on-demand. PaaS maintains the same security flaws as an IaaS solution with the addition of improper use of the existing PaaS APIs. A proper SDLC (*Software Development Life Cycle*) should be in place.

A hybrid model is a combination of two or more of the models previously discussed. A hybrid model can be used to address political, technology or security related hurdles. In situations where data collected from public cloud hosted applications is deemed to be too sensitive to be stored on public cloud resources it is then stored within databases hosted in an organization's private cloud or standalone server and storage solution.

The above text provides a primer on what cloud computing services is, the technology is depends upon

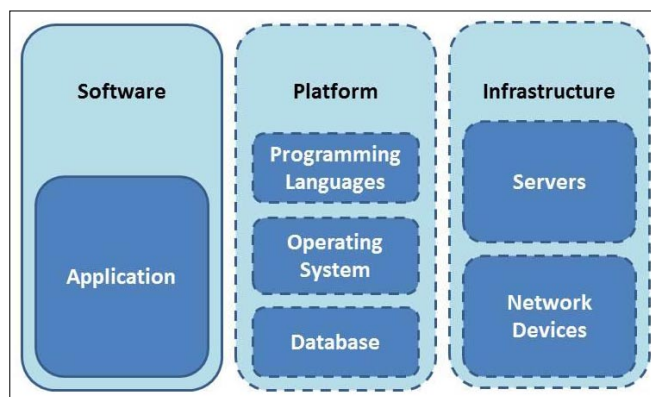


Figure 4. PaaS Customer Responsibilities

and the levels service that are available. Now it's time to dig deeper into the security which can be applied to each model and service.

Securing your services

Because security threats manifest differently in a cloud environment verses a traditional IT infrastructure you may have several approaches to address potential threats. You can no longer rely on the premise firewall being the outer crust of your infrastructure and there may multiple entry and exit points. Vendors are moving towards a multitier trust model and security vendors are focusing their products to address a cloud environment as whole. Implementing security needs to be integrated early into the planning process. Early integration allows for your organization to identify potential vulnerabilities and because the environment is based on virtualization technology you are face with an ever changing perimeter boundary.

Traditionally products have been purchased to address problems identified as a result of a failed control during compliance audit. In the cloud install security products in piecemeal fashion could open and expose an unidentified vulnerability.

The best security measure that you can implement is to always know and understand what is running in your environment.

Identity Management

Cloud environments normally support a large community of users. Even when employing security best practices, such as least privilege, the permission levels will range dramatically depending on a particular users function.

Does your cloud service provider supply and support the ability to manage all aspects of the full ID lifecycle management of both privileged and end users? Also, does your solution prevent the creation and use of multiple accounts for a single user? If not, one option is to leverage a third party trust solution. Although implementing a vendor proprietary solution looks to be the path of least resistance opt for standard connectors. Currently, there is a push for providers to increase support of XACML-compliant entitlement management. If you are bridging multiple cloud instantiations implement a federated identity management solution where authenticated ID's can be shared between various applications, systems, and sites alleviating the need to vet new ID requests. Ensure that all ID's meet your organization password management and complexity policy and passwords are stored in an encrypted format along with the encrypted transmission of passwords between systems and applications. Identity Management has a key role in a virtualized cloud environment as it helps meet the compliance and regulatory requirements.

Access Management

In the case of access control, leverage a cloud based a SAML 2.0 supported single sign-on solution. The solution should incorporate at minimum two-factor authentication to all applications and systems. Privileged access to both the system and application should be encrypted using a VPN based connection. If VPN access is unavailable use a secure network protocol such as IPSEC, SSH, and SSL. All privileged access should logged and retained in an audit trail for troubleshooting or forensic activities.

Logging

As with traditional security infrastructures logging is a necessity. The same log sources need to be factored into your cloud logging solution including; system logs and network intrusion/prevention devices logs, deception network applications, unified threat management solutions, and once again your identity and access management solution. Database logging addresses changes to data but falls short when it comes to who is reading your data. Depending on your log review and retention policies there will be an associated cost as storage and application space could consume significant resources. At minimum ensure that your logging solution captures the following events:

- Failed login attempts
- Privileged access attempts
- Privileged activities
- Access attempts to sensitive data
- Access attempts to audit trail data
- Start and stop of services or applications
- System shutdown or start up

Each event should contain at minimum:

- UserID
- Date and Timestamp
- Event description
- Event source
- Event success and failure

Note

Due to storage limitations it may not be feasible to retain all successful events, but it is the successful events that need to be watched the closest.

Depending on your logging solution or provider, ensure that your logs are separated from your system and protected. Keep a backup copy and retain your logs as specified by your organization's retention policy.

Data Security

Data loss or leakage is a primary concern of IT managers across the globe. Due to the various paths

data could become compromised it is imperative that your data protection solution address both internal and external threats. Over time your cloud design will change to meet new business or regulatory needs. As your design changes strengthen your data protection starting at the hardware layer.

Standards such as PCI DSS, HIPAA, and Sarbanes-Oxley, etc., require that organizations protect their data at rest. Unlike the previous section a traditional approach cannot be applied to cloud based data storage. Data in a cloud environment is no longer physically isolated in a data center. One of the benefits of cloud computing is also a security risk in that storage of your hosted data may also be provisioned and de-provisioned frequently leaving remnants of your data behind or another customer's data on your allocated storage. Being the customer, unless you specifically added data cleansing to your hosting agreement, you are left to trust your provider to scrub the disks properly. If your data was stored unencrypted there is a potential risk for data loss. Whether your data is encrypted or not, it should be at minimum, logically partitioned away from consumer applications. If your data is to be encrypted, understand its limitations in that the data content may not be readable but the data can be moved or modified. In determining what data you need and should encrypt look for the following data locations and types.

- Data at Rest includes files stored on servers and removable media
- Data in Process includes real time transactional data such as data processed in a database
- Data in Transit focuses on network protocols and data passing over wired and wifi networks.

Although your organization's data in the cloud has been encrypted, the cloud does not distinguish between sensitive data and common data so by default anyone with access to the virtual system or its storage has to access your sensitive data revealing a fundamental flaw, the lack of data integrity in cloud computing. Another flaw with encryption in the cloud is key management and what is considered a secure location to store the encryption keys. If possible, store the keys outside of your cloud environment. In selecting a key management solution ensure that the product is capable of encrypting various data types and manages the keys throughout their full lifecycle.

As cloud services is still in its infancy using the hybrid model might be a possible approach allowing you to store your data your organization's private cloud or data center while hosting your applications in a public cloud. Once the protection profiles have been determined for your hybrid solution and minimum key strength policies are in place you need to encrypt for both data

at rest and in transit. By using well-established secure network protocols to encrypt your data in transit and FIPS compliant encryption algorithms to protect you can have some assurance your data is safe. Regularly verify the integrity your organization's data being stored through the use of checksums. If a data corruption is detected you will most likely need to restore from a known source.

Application Security

In cloud computing who is responsible for your organization's application security? Ultimately, you are. Create a website risk management plan that will heighten awareness and will protect valuable corporate and customer data from attackers. Application security is core to deploying the components of your internet presence. When implementing SaaS applications you lose visibility into the environment to prevent malicious actions. If able employ a third party application to monitor your SaaS applications. When developing an application for the cloud the same SLDC would apply that your organization employs for internal application development.

Vulnerability Management

When implementing IaaS or PaaS services your organization should have a Vulnerability Management plan. Similar to a traditional infrastructure patches will need to be tested and applications and operating systems will need to be hardened and tested for configuration changes. If your environment contains an Intrusion Detection System (IDS) you will need to routinely update the signature files. To minimize exposure to virus propagation, install antivirus software on all systems. The AV program should be able to isolate or remove malicious software.

Create or maintain a vulnerability scanning plan. At minimum the systems should be scanned every 30 days to ensure all patches are being applied regularly.

Conclusion

The benefits of cloud computing is clear, so is the need to improve security for cloud implementations. Like any new technology, cloud computing security will mature. By applying the similar methods and mindset taken in traditional system development your organization can manage access controls, see the activity occurring on your systems, and keep your data secure.

DAVID PROKOP

Do You Have The Correct Cloud?

Cloud Privacy

In both personal and business settings, clouding can be a great tool. But how do you know that when you upload your information into the cloud it is private?

What you will learn...

- What type of cloud is for you.
- How to keep your information private.
- What not to do when clouding.

What you should know...

- Different Authentication methods.
 - How to determine data center resources.
-

Can anyone just connect to your data-store and start perusing through your information? These are a few questions that we will discuss. If you don't know what the correct type of cloud is that you need, you may fail. The reason for this failure could primarily be a privacy issue. Yes, Privacy.

The first question is, why are you using the cloud – business or personal? Most people don't use the right type of cloud. Are you launching applications, servers, or developing? Are you using the correct cloud type that also delivers the correct amount of privacy?

Clouding is a newer technology, no one has set any pure standards, and all the big names are trying to become the top tier cloud service that sets these standards. Amazon EC cloud service has begun to set the standard for the way people perceive the cloud. Ubuntu has almost everyone beat when it comes to developing solutions and free access to clouding. But the giants are waking up! Microsoft, Apple, Oracle, and Citrix, to name a few, want a piece of the action as well. With that in mind every company is claiming that they have the best technology and the best privacy. But no one can ever have the claim of the *best* privacy. Privacy is an untamed beast in this world. It's like saying a Mini Cooper is faster than a Ferrari. It's never going to happen.

What you can do is to find the correct cloud which delivers the proper security for its intended use. A

correct clouding experience can make your business a success greater than your competition or put your life at ease when backing up your family photos. We are going to go through many of the popular clouds and look at what their purposes are and how private they are.

Clouds in a public domain are potentially great and potentially disastrous. Most users don't know what type of cloud it is they need and will usually go with the cheapest and easiest service they can find. Cheaper is not always better. Creating a private cloud can be helpful as well. If you know that it is going to cost you a lot running on a public cloud service, it may be cheaper for you to run everything in house. By doing this you can convert many, if not all, of your servers to the cloud. This brings cost down and allows the business to flow. This is often a good business solution. Businesses are moving to clouds because they get the redundancy they need to keep their business alive. They are also moving because they want to use all available resources in their data centers.

For example, you have an SQL server and a few Application servers connected to each other, some of the Application servers don't get used a lot because they are low taxing applications. However, because of the configuration they need these applications need to be installed on separate servers. Add in a modeling application that needs more resources to run properly

and you have a real problem and a possible server failure. This is when clouding makes a difference. If all of these machines are clouded together, they can grab just the resources they need allowing other applications that need more resources to use them. This makes everything faster, more reliable, and avoids possible disaster.

Now, as far as what type of cloud fits what service type we will look at the chart below. Note some have dual service types. When they are being built or reviewed they should be made for that single service: Table 1.

There are many differences in each service, which is why keeping things running on the proper cloud type can keep your information private. The following table explains these different types (Table 2).

If you are using the right service you can protect your information the right way. Not using the proper service can lead to a weak link in your security. This weak link can expose everyone's data. This is why some professionals think that clouding is less secure than a dedicated server. They are right; If the cloud is not being used correctly it is less secure. If you are using the cloud correctly it will be more secure.

If you have multiple types of services going to the cloud, such as virtualization, and development, there are many different authentication types you now have to defend against. This allows many different angles that an attacker can take. Unless you have a huge security budget and can set forth on every authentication type connecting to your cloud, you're going to run into crossover and one service is going to be the weak link, and that's the one that the attacker is going to take. Just like with any application or device, you have too much going on or you are not using it properly it can destroy your infrastructure and security makeup.

I know many out there that are reading this are saying: My cloud is safe and I have people connecting to it using services that you say it's not designed for. Right now you're not getting hit a lot by attackers. The cloud is basically getting off the ground and many attackers aren't really interested in cloud hacking yet since a lot of companies and people are going back and forth because they aren't sure yet. Once everyone starts getting moved over to the cloud and it takes off you will see more and more attacks happen, making privacy and security a number one concern.

There isn't a lot of information out there when it comes to clouding and privacy. One who creates something in the clouding world can be a pioneer and set standards if they try hard enough. Since clouding is so new to the information world it is easy to get lost. Just remember that choosing the right cloud can



HAKIN9

Join our
Exclusive and Pro club
and get:

- HAKIN9 **Hakin9 one year subscription**
- HAKIN9 **Full page advertisement in Hakin9 every month!**
- HAKIN9 **Information about your company send to over 100,000 Hakin9 readers!**

More information at
en@hakin9.org

BASICS

Listing 1. Types of clouds and services

Name:	Authentication:	Service Type:	Special Service:	Authentication Rating
Ubuntu, Canonical	- LDAP Authentication - Hash Key	- Developing - Data / Backup	- 12.04 Any Web Service over Me (AWESOME)	Using a hash key makes for a very good connection and usually secure. Hash Keys are very sensitive and are difficult to spoof.
VMware	- Based of the machine build	- Virtualization	- ESX	- Smart Cards or Hash Keys are a plus. Smart Cards give the two out of three challenges. - Passphrases are not a good idea. Passphrase can be cracked with a simple rainbow table.
Red Hat	- Hybrid (can be converted to fit your environment)	- Developing - Virtualization	- MRG Grid	- Good if you have a smart login system. Harder for an attacker to access.
Oracle	Enterprise Management Command Line Interface(EMCLI) using one of the following: - Oracle Access Manager (OAM) SSO - Repository-Based Authentication - SSO-Based Authentication - Enterprise User Security Based Authentication (EUS) - Oracle Internet Directory (OID) Based Authentication - Microsoft Active Directory Based Authentication	- Developing - Application	- N/A	- Most of these are passed upon passphrases and user lookups. Easy to spoof or crack.
Microsoft, Azure	- Active Directory (AD)	- Microsoft based application	- Hyper-V	- Uses Microsoft security for AD. Security holes are always possible.
Citrix	- Active Directory - Radius with RSA	- Application needing Citrix services	- N/A	- Same as Azure with AD. - RSA keeps for a nice secure connection.
Apple,	IMAP Authentication	- Data / Backup	- Photo Stream	- IMAP a smart attacker

Listing 2. Differences in services

Development	Development is a different kind of beast when using a cloud. Developing in the cloud is great and saves huge amounts of time. When a developer needs they can spin up an instance and test their code. They can backup on the fly and launch their code on the fly not disturbing anyone else. This allows for concise engineering by the developer.
Application	Resources are an applications best friend. When resources are needed in a cloud the smart system pulls its sources from a section of the cloud that isn't using any at the time. Allowing balanced access to the environment.
Virtualization	Needing specialized machines can make virtualization a hassle. If you need a specific server type such as, Linux, Unix, Apple, or Microsoft, you have to worry about the machine working properly with the virtualization environment. With a clouded environment you do not need to worry about resources and failover.
Data Backup	Data backup, everyone's nightmare. Nobody likes to admit it but we all hate having to setup or design some sort of data backup solution; one that is secure and redundant enough that you never have a failure. Backing up to the cloud is a safe bet and allows access at anytime.



make a difference when it comes to securing your information and keeping you private.

CHRISTOPHER PEDERSEN

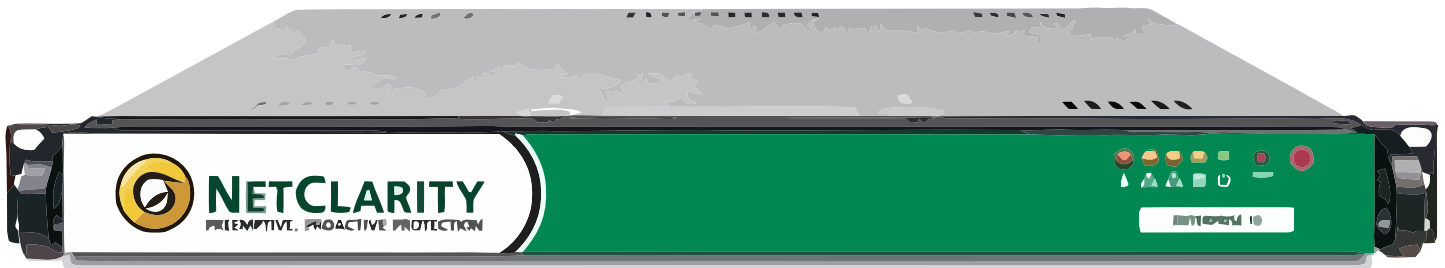
Chris has been in the Information Systems Field for more than 14 years. He has worked in both the public and private sectors. Currently he holds a position with the Department of the Navy as an IT Specialist.



NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION



Harden your Network from the Inside Out



Network Access Control



Asset Vulnerability Management



Compliance Auditing and Reporting



www.netclarity.net

Available through Partners Worldwide

Secure commerce in the Mist

We are starting to move to IPv6 and the cloud. Right now, the uptake is minimal at best with very few early adopters for all of the hype. The climate is changing. Soon, IP addresses will be on everything and even the concept of non-disclosure agreements and contracts designed to protect intellectual property will require that we consider the nature of the cloud and the Internet as a platform for contractual negotiation.

What you will learn...

- The Nature of Online Contracting
- Secure Servers and Pockets of Clouds

What you should know...

- What Cloud Computing is
 - How to secure your Cloud
-

As we move towards a cloud based system of interconnected islands, we first need to look at the issues surrounding online contracting using the Internet and the cloud as it has been termed before we can look into the specific problems that are associated with selected forms of contracts itself. More, to consider the security of these systems, we need to understand the risks inherent to shared environments and how we can best use the new technologies in creating a future business platform.

Introduction

Network systems work on an exponential growth curve. Things are exponentially less expensive each year and incrementally more powerful. This will drive applications and uses that people have not even thought of. The following are ideas that are just a few years from deployment:

- Disposable communication tablets. Basically these could be dropped in places such as Iran or North Korea and allow for communications no matter what the incumbent government tries to filter. Think \$1 devices.
- Milk, Coke cans and more in supermarkets with IP addresses and RFID. Why, well first as they can integrate this with smart appliances, but more importantly, merchandising and stock control. Who needs to do stock take when the store tells you what it contains.

- Light bulbs with web and IP addressing. Well actually these are already available.

There are many reasons why IP addressing will be used up quickly and these are but a few and more reasons why we will start to move towards distributed and hence cloud based systems. It is also one reason why we will move to IPv6. Mobility and security is another.

The catch-cry of the 21st century will be, Anytime, Anywhere.

Done correctly, IPv6 can make for extremely secure networks. It is already possible to make a secure mobile network. It is more difficult under IPv4 due to the constraints on the protocol. What we need to think of in this endeavour is how this will enable and change the business dealings that have driven the growth of the web.

The Nature of Online Contracting

Technological developments and the advent of the Internet have led to new paradigms in international as well as local commercial activity. These changes have reduced the certainty of contractual negotiations leaving a commonly held belief that the law of offer and acceptance does not readily apply to such transactions when conducted online (Rasch, 2006). We have already created islands of clouds in our dealings and now these clouds are becoming finer. What was once a

set of connected clouds and islands is fast becoming a nebulous web of connected systems.

The increased use of international commercial transactions using the Internet is something no company can escape. In the past, international commercial transactions were generally restricted to negotiations between commercial entities. The Internet has increased the scope of business to consumer dealings, and even consumer-to-consumer transactions across jurisdictional borders (Department of Communications, Republic of South Africa *Discussion Paper on Electronic Commerce Policy* (1999)). For this reason, the formation of contract using the Internet creates segregation into two initial categories. These categories include both those negotiations that occur strictly within a single jurisdiction, and next, those negotiations that involve multiple legal jurisdictions. Where the cloud is involved, security can be seen to encompass many localities and hence jurisdictions even when dealing within a single organisation.

Another concern for cloud based systems focuses on the relationship of parties. Many Web based transaction engines already act as third parties during the process of offer and acceptance. This interaction can complicate the formation of contract. Because of this, it is necessary to determine the legal standing of the third party (*Debenhams Retail Plc v Customs and Excise Commissioners* [2004] EWHC 1540). The third party could be a party to the contract, an agent or one of the two contracting parties, or may just be an ancillary facilitator or medium, across which, and through whom the contractual bargaining occurs (McKendrick [1], 2005 (pp163-164)).

Without legislation detailing the legal position of electronic contracts, the process of offer, acceptance and the terms of a contract created using the Internet will establish itself by means of the general law of contract. This will happen for the most part in the same manner as for the negotiation of terms of a contract in the physical world (Lee, 2002 (pp 62-100)). Thus, establishing offer, acceptance and the terms of a contract remains the same whether the form is in writing, orally, or implied though the conduct of the parties in the same manner as existed prior to the rise of ecommerce over the Internet.

Contractual formation is inherently uncertain in and of itself (Gamage & Kedem, (Nov, 2006)). Being that electronic contracts form a logical subset of the contractual superset and that there is uncertainty within contract formation in general; it must naturally follow that there are areas of uncertainty, which will remain in the formation of electronic contracts. The formation of contracts on the Internet and with *cloud* providers will suffer from the nexus of jurisdictional issues.

A contract is not required to be in writing (Columbia Law Review, (Apr., 1929), pp. 497-504; Columbia Law Review (Jun., 1907), pp. 446-449; McKendrick, E, (2005), p 184) meaning that there is little additional uncertainty created when the contract is completed electronically. In fact, it is clear that electronic evidence must hold greater weight than verbal evidence (Lord Justice Auld (Sept 2001), Cpt 11). What is not clear is the extent of the weight attached to the various forms of electronic evidence. The strength of a digital signature algorithm and the security surrounding the mechanisms used to sign an electronic document will respectively influence the weight associated with any piece of electronic evidence. That stated, we still come back to the issue of jurisdiction and also in the case of intermediary agreements.

An electronic contract has a twofold structure. Thought of electronically, the contract is a sequence of numbers and code saved to some electronic or magnetic medium. Alternatively, the contract becomes perceptible through a transformation of the numeric code when broadcast to a computer output device such as a printer or screen (Bainbridge (2000); Reed (2004); Brownsword (2000)). This dichotomy exasperated the uncertainty contiguous with whether an electronic contract can be regarded as being a contract in writing in the past, but has been settled in most western jurisdictions through a combination of legislation and judicial review.

At the most fundamental level, the existence of an offer and an acceptance is one of the primary requirements for the creation of a contract. The set of laws used to determine whether there has been a valid offer and an acceptance created across the Internet or a mere invitation to treat have their lineage in the case law concerning postal and telex communications.

As an offeror may stipulate the method of acceptance (*Eliason v Henshaw* (1819) & *Manchester Diocesan Council for Education v Commercial and General Investments* (1970).), it would be wise for parties to agree to the form of acceptance prior to the conclusion of the contractual negotiations.

A further important issue that surrounds Internet contracting is the general rule of law that, for an acceptance of an offer, it must be *communicated* to the offeror (McKendrick [1], 2005; p43 – 44). Under normal circumstances, the offeror must actually receive the acceptance before a contract will come into existence.

Amazon.com (<http://www.amazon.co.uk/exec/obidos/tg/browse/-/1040616/026-9370677-1792435>) provides an example of this practice. Amazon has a page defining the terms and conditions associated with the site. Terms designed to protect the seller from entering into a unilateral offer consisting of an agreement that it did not intend to make link to the site for general download. This feature helps ensure that both parties

understand the point at which the close of negotiations occurs and forms a binding contract.

Electronic Agency Issues

The inclusion of electronic agents makes the traditional requirement for a *meeting of minds* more difficult to prove. With many smaller vendors, hosting and creating their own e-commerce enabled web site requires the interaction of a third party. Often, this involves the use of an external service provider, which offloads the Internet shopping trolley function. In this way, smaller vendors can create an e-commerce enabled site quickly and simply.

The issue, which arises in this instance, is in determining the contracting parties. Many small vendors provide little more than billboards style advertising through their web site. The complex task of maintaining the databases, transaction processing, and the shopping cart function becomes simplified when outsourced to another provider. In some instances, a redirection takes the customer to a completely new site or domain.

In such cases, it may be necessary to investigate whether a contractual arrangement has resulted between the client browsing a web site and the transaction agent or if indeed the transaction facilitator is a contractual agent for the Web store vendor (Lim, 2002). Agency has become a specialised area of contract law in itself. As such it will not be covered in any depth in this paper, though it is an area that does require due consideration and may influence the process of offer and acceptance.

What can now be done is to create logical islands in place of what was once a set of isolated systems.

These isolated systems can allow us to treat pockets of cloud based systems as if they were physically isolated and not simply logically created pockets.

Secure Servers and Pockets of Clouds

The deployment of secure server and client trust models can already be achieved using workgroups using encrypted sessions set to allow communications to and from clients to trusted servers. This can be configured to stop client to client communications in a domain.

Why restrict clients this way?

In a large organisation, client peer to peer communications can be a means of malware dissemination. There is rarely any real need that cannot be achieved on the server to have clients talking to clients over the network directly. Rather they should be controlled via a server. What this can allow is those only authorised clients hosts are allowed to communicate with servers. In an organisation, even mobile users can be forced to communicate to company servers. This is where the cloud becomes important. With disk encryption, IPv6 with IPsec enabled and the right controls, each and every host can be firewalled.

Such an example is displayed in Figure 1. Here, mobile user (A) can be restricted to communications with only allowed systems (such as a home office (D), and the corporate servers (D)). All attempts to connect to the system with an untrusted host will be dropped as the host attempting this will be allowed to communicate through policy and host firewall rules. This can already be achieved using tools such as Group Policy and NAP in the Windows world with a large number of tools being available for Linux and Mac environments.

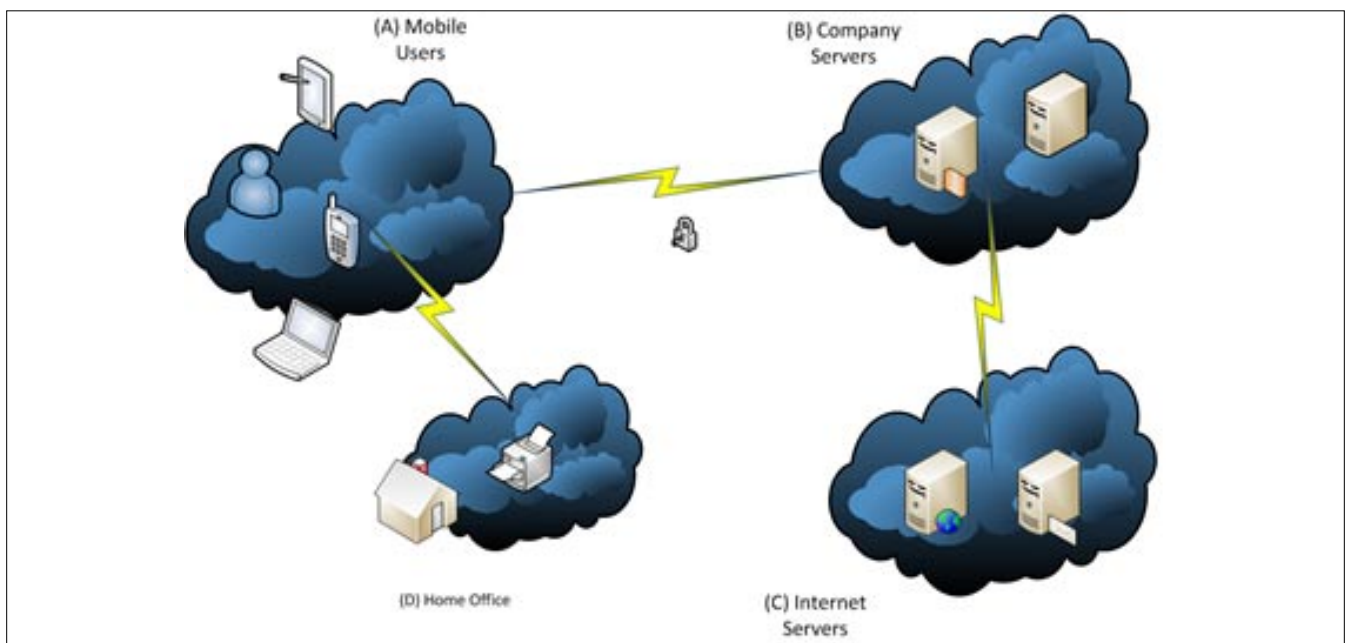


Figure 1. Islands of clouds

In this example, the client host can be restricted to connecting to the organisational proxy server and no more. Extending this, using DaaS (*Desktop as a Service*) with mobile tablet makes this even more secure. The desktop can be configured to be accessed only from selected tablets with a key and at best, the loss of a tablet will provide only a key to the remote desktop which still needs to be authenticated to. This restricts local access to the host as the *desktop* is stored in a data centre. The user cannot use local escalation attacks based on physical access to the system as they are never actually on the system. More, if the user loses a tablet or other device, they are not actually connected to the system and files and the loss of the tablet will not lead to a loss of data.

As the desktop is configured to only talk to the tablet and the organisational servers and all communications are encrypted, the location of the user does not actually matter and they can be truly mobile (as IPv6 allows). More, this allows the organisation to control access to the Internet through organisational proxy and email servers.

There are security benefits *IF* these services are managed correctly, but here, as with any service, it all depends on how it is maintained.

Pockets of Clouds

Through isolating systems into logical pockets, we can treat these as discrete units in analysing dealings made with and through these systems. In isolating trusted hosts from untrusted devices, we can take the dealings of contracting parties into account without many of the jurisdictional issues that will naturally come from data having passed through multiple jurisdictions in a commercial transaction.

Controls that are implemented at the network level using technologies such as IPSec (and this becomes easier when using IPv6) create pipes that segregate data logically from the environment it is physically passing or residing in.

In these zones, we can start to look at the endpoints as separate and isolated systems rather than having them integrated within the mesh of the internet we now see. As it stands, the internet cloud is really an open environment. External parties can connect to and interact with others with few endpoint restrictions for all the firewalls and other technologies we profess to have defending us.

Logically isolated, we can start to track and manage the systems we are seeking to protect and more, we can start to ensure that contractual arrangements are limited to set and selected parties. In creating logically isolated systems, we limit exposure to outside influence and increase the perceived value of online negotiations.

Using IPSec and the host firewall allows you to create secured logical zones that separate the systems and services within a domain forest. In doing this, you can deploy technologies such as NAP (Network Access Protection) to control communications based on a contracting parties rights.

NAP has been used with *Health Certificates* in the Windows world for a number of years now. Generally, this is used to ensure that a system is patched and that the anti-virus signatures are up to date, it can also be used to ensure that contracting parties are configured correctly and more, that they accept terms and conditions that an online agent implies or has issued. Integrating contractual terms into a health certificate allows little leeway for a third party to impose or alter terms. If the certificate is not accepted or if it is altered, the encryption process fails and no transaction can result.

Here again, we also see an avenue for electronic agencies. This time as a means to ensure that the certificates and status of the client is acceptable through the provisioning of selected terms and conditions and brokering different rates that are then linked to selected health certificates.

Conclusion

As strange as it may seem, a well-defined and deployed cloud and IPv6 system can actually be far more secure than the traditional crunchy shell firewall model. More, these systems can be used in order to create a secure platform for commercial dealings that removes many common contractual problems. Extending this, we can expect to see a rise in external agencies that provision and facilitate the use of selected signed tunnels and also log and report on the status of clients. Hence, for high value transactions, systems can be checked for common issues and problems (such as a failure to adequately patch and update anti-virus signatures) before the transaction has been completed.

CRAIG S WRIGHT

GSE GSM LLM MStat

Craig Wright (Charles Sturt University) is the VP of GICSR in Australia. He holds the GSE, GSE-Malware and GSE-Compliance certifications from GIAC. He is a perpetual student with numerous post graduate degrees including an LLM specializing in international commercial law and ecommerce law, A Masters Degree in mathematical statistics from Newcastle as well as working on his 4th IT focused Masters degree (Masters in System Development) from Charles Stuart University where he lectures subjects in a Masters degree in digital forensics. He is writing his second doctorate, a PhD on the quantification of information system risk at CSU.

Understanding Cyber

Warfare and its Strategic Applications

There has been a lot of buzz going on about “Cyber Warfare”. Examples have been given ranging from the 2009 attack on Estonian web sites by pro-Kremlin hackers [1] to the Stuxnet worm that attacked the Iranian nuclear plant in 2010 [2].

What you will learn...

- The principles that war fighters use to determine the best course of action
- How these principles can be used in CNO
- What role CNO can take in combined arms operations

What you should know...

- Basic computer-based attack terminology and theory
 - Basic military terminology, or know how to find it
 - The difference between CIA and the CIA
-

In this article I will not attempt to officially define or debate what exactly cyber warfare is or what threat it poses. Instead, I am looking to determine if and how modern military operational strategy will utilize, respond and evolve to this new spectrum of warfare. Both as an asset in combined arms operations as well as in a purely cyber confrontation.

We will be reviewing the 9 principles of war used by the U.S Military to plan its military operations. Although these principles have been defined and grown from the mold of kinetic warfare, I believe that these principles translate into the cyber spectrum as well. In order to make a sound argument for this I will attempt to not only define and apply the principles in a way that yields victory in combined arms and cyber confrontations, but also demonstrate how the failure to do so will greatly increase the likelihood of defeat.

History and Definitions

There seems to be a lot of *crying wolf* when it comes to cyber warfare. A great example is the *false alarm* hack of the Illinois water pump in late 2011 [3]. Fancy phrases like APT are thrown around way too loosely and are joined together with threats of cyber warfare and cyber terrorism. In reality, many of these threats are coming from hacktivists like Anonymous or groups like the Russian Business Network looking for lucrative opportunity. Although these threat agents deserve significant mention we must separate them from state-

sponsored cyber warfare. Later in this article I will go over how grouping these threats together actually detracts from our defensive cyber posture, but at this time I will simply state that we need to separate these threats from each other.

Before we can really get into details about how the principles of war can be applied to cyber war, we must first define cyber warfare in the context of this article. This can best be done by a brief review of acts of actual cyber war.

Titan Rain

Starting in 2003 a series of attacks from China managed to infiltrate numerous portions of the U.S Department of Defense network. This is seen as one of the first major acts of cyber war. To this date the extent of the intrusion is not yet known, but what is known is that terabytes of data were taken from the DoD’s unclassified NIPRNet [5].

The connection back to the Chinese is made through one specific hacker. Tan Dailin, known as Wicked Rose, who started a group within China that targeted Taiwanese government systems. He was quickly recruited into the PLA and later went dark for a number of years. At the onset of Titan Rain, specialists were able to make the connection using digital forensics and code writing analysis. Their findings suggested that those who were at least trained by Wicked Rose perpetrated the attacks [6].

Byzantine Hades

This operation first made headlines when Wikileaks published some diplomatic cables. The disclosed information suggests that Chinese military, intelligence and private hacking assets used massive spear-phishing attacks to siphon terabytes of valuable information from government and military systems [4].

Aurora

In 2010 Google disclosed knowledge of a massive cyber attack originating from China. These attacks were aimed at stealing intellectual property of large corporations. Utilizing an IE Zero-Day, the attackers were able to steal corporate secrets and possibly alter public code base [7].

These attacks were linked back to the Chinese via technical means as well as the timeliness of Google's content-filtering dispute with the Chinese government and their subsequent withdrawal from the country.

Stuxnet

In 2010 a revolutionary computer virus was used to disrupt production at the Iranian uranium enrichment plant. Supposedly developed in the U.S and tested within Israel, this malware demonstrates the true capabilities and value of state-sponsored cyber attacks. This malware was designed as a smart-bomb of sorts. It's logic is set to only attack SCADA systems with specific configurations like those found in Iran's enrichment plant. Utilizing a series of zero-days and numerous other techniques, this malware caused sufficient damage to even physical assets [8].

I have intentionally left out examples like Estonia or Anonymous & Lulz Sec. Although these have been branded as cyber-warfare and may have ties to specific nations, these are most certainly not entirely state sponsored events or organizations. I would therefore brand these at most as cyber-terrorism. And just as there is a difference between COIN and conventional kinetic warfare, there most definitely is a similar difference in the cyber realm.

We must avoid the overly large umbrella of saying that APT is synonymous with cyber war, or that any

attack against a nation is an act of cyber war. Doing so would be like stating that acts of vandalism against a city hall were some sort of act of war. In short, the term cyber warfare should be restricted to instances where one nation state uses or directly sponsors cyber attacks against another nation state.

The Principles of War

The principles of war were pioneered by Napoleon, but were first published by Carl von Clausewitz. From the organization of staff to the strategy on the field, every major military to this day is structured and commanded based upon these principles. Originally developed for both tactical and strategic settings, these principles were a way of turning the art of warfare into a qualitative and quantitative science. Although these principles are now largely utilized in only strategic scenarios, they provide the guidelines of decision-making that has led to the victory or defeat of many nations.

For students of military science the principles can be used to identify the faults and genius of nearly any conflict. For strategists they can be used to give proper attention to vital tasks or to decide between differing courses of action. Because of this high level use, we can apply these principles to cyber conflict as well.

You will find that the term *combat power* is used widely within the principles. The official definition is:

"The total means of destructive and/or disruptive force which a military unit/formation can apply against the opponent at a given time." – D.o.D Dictionary of Military and Associated Terms (emphasis added)

The emphasis is added to help the reader understand to what ends combat power is applied (i.e. destructive or disruptive force), and what limitations are put on its capabilities (i.e. total means available at a given time). In conventional warfare these are easily defined. In cyber warfare it may be a little more difficult. Please look at the provided Table 1.

Hopefully this diagram shows you how combat power is divided. The first row lists things that are capable of causing actual harm or directly affecting the target. The

Tabela 1. *Combat Power*

	Conventional Warfare	Cyber Warfare
Disruptive/ Destructive Force (quantitative)	<ul style="list-style-type: none"> Missiles Bombs Bullets CBRN PsyOps 	<ul style="list-style-type: none"> Zero-Days Throughput/Traffic Social Engineering Malware Any reasonably effective attack vector
Total Means at a Given Time (qualitative)	<ul style="list-style-type: none"> Soldiers Weapons Systems (tanks, jets) Fuel Intelligence 	<ul style="list-style-type: none"> Hackers Botnets Bandwidth Intelligence Existing access

second row contains the assets used to apply the force. Usually the first row is dependant upon the second row, while the second row is more often bound. However, the first row tends to be a quantitative asset, while the second row tends to be qualitative. This leads to the concept of force multipliers.

A *force multiplier* is an asset that can offset a level of the enemies combat power at a ratio greater than the quantitative value of the asset itself. Or from a different perspective, *a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force.* A great example of this can be made utilizing the analogy of soldiers. A single well-trained soldier, like a sniper, could potentially *disrupt* or *destroy* an enemy force more effectively than a single lesser-trained soldier. Just as so, a well-trained hacker may be able to disrupt or destroy an enemy force in less time than a group of lesser-trained hackers.

With those definitions we are now ready to discuss the principles of war [9]. There will be a direct format for each principle covered. First, I will give the definition of the principle. Second, I will explain the relevance of the principle from a joint-arms perspective. Third, I will cover the applications of the principle in a strictly CNO confrontation, much like has been seen in the historical examples given earlier. And finally, I will show how neglecting the principle will increase the chances of failure.

Objective

“Direct every military operation toward a clearly defined, decisive and attainable objective.”

The principle of objective assists the commander in developing criteria for the necessity and effectiveness of possible actions on the battlefield. By clearly stating the purpose of the mission, he can quickly identify what sort of assets he would like to help achieve his goal, as well as disregard any tasks that do not directly lead to completing the objective.

The integration of cyber warfare into the combined-arms model allows for the commander to expand his options for completing the mission. Just as air support greatly changes the possibilities on the battlefield, so would having cyber assets available. For example, the 1991 Gulf War began with the Coalition’s Operation Instant Thunder. This plan consisted of three phases leading to direct combat with the Iraqis. Phase two was targeted against Iraqi infrastructure with the purpose of preventing the military from conducting an effective defense. As a result 11 of Iraq’s 20 main power stations and over 100 substations were destroyed, with many others being damaged. In just a few short days Iraq’s power production was reduced to 4 percent of its normal levels [10].

Strategically this was seen as an essential task to ensure limited losses of coalition forces as well as degradation of Iraqi moral. However, according to the Gulf War Air Power Survey, *The aim was not destruction of one particular target set ... but rather a synergistic degradation of the whole, in which friction, confusion, and uncertainty would combine to make the defenses generally ineffective.* [10] Clearly we see that the actual destruction of the power stations was not essential to achieve the objective. In fact, disruption would most likely been preferred.

The availability of Cyber assets could have provided such an option to the Coalition commander. Not only that, but the availability of cyber assets may have allowed the commander to look beyond the scope of the current mission and focus on the greater objective. Imagine the money, time and public relations efforts saved on if instead of destroying and rebuilding a power plant (more than likely causing loss of life of local families), the Coalition were able to simply shut them down long enough to achieve the same strategic goals. This example shows us exactly how overall military objectives can be easier to achieve when integrating cyber assets.

In a strictly CNO situation the principle of objective remains just as important. In HD Moore’s Black Hat training entitled *Tactical Exploitation*, he shows us what it means to conduct cyber warfare using the principle of objective. He states, *Vulnerabilities are transient. Target the application, target the processes, target the people, target the trusts... Hacking is not about exploits. That target is the data, not root* [11]. Focusing on the preferred method or the process can distract us from getting the target. How often has a penetration tester given up on an entry point because he felt it left no chance of a root shell? If we define and focus on an ultimate goal (in this case stealing/protecting data), then the middleware will no longer distract us.

Offensive

“Seize, retain, and exploit the initiative”

To truly seize and exploit the initiative means to posture one’s own forces in a way that the enemy is forced to react to your movements rather than choose his own decisions.

Within a combined arms environment cyber warfare can assist in seizing the initiative by attacking C&C channels utilized by the enemy commander. Imagine a Crew competition in which two boats are neck and neck. If one team were able to disrupt the communication line of the oppositions coxswain, they could potentially pull ahead while that team struggled to regain its tempo. This extends beyond even communications scenarios. Any simple misstep that could be caused or intelligence

that could be stolen via cyber assets could allow a force to seize the initiative. Retention and exploitation of the initiative with cyber assets could go as far as conducting Man-In-The-Middle type attacks against the enemy after allowing them to *regain control* of their C&C channels. In some ways cyber attacks can serve as spies or resistance forces disrupting operations from within the enemy's territory.

The principal of the offensive is easy to map to the strictly CNO spectrum. Any infiltration will lend the initiative to the attacking party; assuming that the enemy hasn't seized the initiative first. The use of root kits and hidden malware buried deep within enemy systems will guarantee the retention and exploitation of the initiative. Such attacks will this force the enemy into diverting efforts (a.k.a combat power) into incident handling procedures. It will also permit the attacker to keep a close watch on any offensive behavior currently occurring (prior breaches) or being newly initiated. Almost based on this principal alone we can determine the loser of a cyber war. It will most likely be the force that yields the initiative soonest and for the longest amount of time.

Mass

"Concentrate combat power at a decisive place and time"

The important part of mass is understanding that an attack is not always decisive. It is dependant upon the posture of the enemy, the place once chooses to attack, and the timing associated with those two factors.

In kinetic warfare this often means hitting the enemy at the time and in the place where it will cause the most damage. Even more so, it means ensuring that enough combat power is available to make such an attack succeed. Within combined arms situations cyber assets can act as major force multipliers. Whether it be in a counter-attack, an attack, or defensive maneuver, cyber assets can quickly lessen the enemy's combat power, thereby increasing the effectiveness of your own. Some methods may include denial-of-service on vital utilities, manipulation of intelligence or battle plans, and the interception of valuable communications.

Applying the principal of mass within a CNO situation takes on a different role. In this situation the cyber assets are not supporting a kinetic effort, but are rather the main effort themselves. In situations like these small time frames can determine the success of an attack or not. Perhaps the enemy has opened up a service for routine updates or some similar attack of opportunity arises. It is vital for all cyber assets to be available to capitalize upon such situations. This includes personnel, skill sets, computing power and bandwidth.

Even in a defensive situation it is important to have enough combat power available to counter any attacks. And in some cases even exploit openings the enemy may have revealed in his attack.

Maneuver

"Place the enemy in a position of disadvantage through the flexible application of combat power"

Maneuver is a critical element for conventional kinetic forces. Freedom of movement allows a commander to bypass certain defenses, as well as manipulate the enemies posture. In combined arms situations Cyber assets can be used to ensure that the enemy does not limit your force's ability to maneuver. The Haditha Dam raid at the beginning of the 2003 Iraq invasion is an example of an operation aimed at maintaining maneuverability. In that situation the threat of flooding was considerable enough to warrant the capturing of the dam. Cyber assets could assist in similar situations by locking down systems that may be used to cause similar disruption to a force's offensive.

Maneuvering within a strictly cyber conflict takes on a different meaning. Maneuvering throughout cyber space is dependant upon multiple factors; physical links, understanding protocols and knowing topologies to name a few. Just as a kinetic commander would want to maximize available avenues of maneuver, so would a cyber commander. Ensuring multiple paths to a target system is critical. Creating redundant layers of connection should be a top priority in a cyber conflict. At the highest-level normal physical WAN links could be relied upon. However, those could be, and in the past have been, severed creating a virtual zone of separation. The next step would be satellite or other non-physical links spanning large geographic separations. If those were disabled then the next level down could involve *boots on the ground* within the cyber zone of separation. These operatives could then use the WAN links still available within the target area to conduct operations. Or if necessary establish ad-hoc links back to the attacking country; effectively creating a sort of pivot. In the event that the existing WAN links were also compromised (i.e. an air gap), then the operative could then be used to conduct similarly stated attacks utilizing wardriving-like techniques. Even if those connections are compromised, internal operatives could still try to plant malware infected USB drives.

The failure and success of cyber operations is strongly dependant upon such connections. Not only is a connection required, but also numerous avenues greatly increase the chances for success. More maneuverable avenues means greater attack surface

and a larger area to defend. Just like the *fatal funnel* that exists within kinetic warfare, allowing the enemy to limit your virtual avenues of approach greatly increases the risk of a cyber operation.

Economy of Force

“Allocate minimum essential combat power to secondary efforts”

Economy of force is the principal that forces each commander to understand that war is still a game of numbers. In kinetic warfare cyber assets have the great opportunity to allow forces to be diverted to other tasks. Like in Operation Instant Thunder a cyber attack could not only be monetarily cheaper (Tomahawk Missiles are very expensive), but also would have allowed manpower and weapons systems to be used at other parts of the battlefield.

There are numerous ways to apply economy of force to CNO operations. Since it is a fairly simple thing to do, I will only share a few brief examples. One of the limited assets that exist is processing power. If a number of critical systems needed to be cracked into, you would want to divert as much possible processing cycles to the task. This would require to minimizing of secondary or non-critical tasks.

Another example could be the utilization of backdoors or botnets. Certain attacks would disclose to the enemy the presence of compromised hosts within their organization or throughout the globe. As a result the enemy would then know how and where to deter future attacks. Therefore, a cyber commander would want to employ economy of force by only utilizing such assets on essential operations.

Unity of Command

“For every objective, seek unity of command and unity of effort”

Having a unified decision making group is essential in all aspects of war fighting. It prevents the duplication of efforts, reduces the risk of fratricide, and allows for combat power to be used at its greatest potential.

Cyber warfare forces will rarely, if ever, be the primary force within a combined arms environment. It is most likely that they will be utilized as a form of fire support for units down to company size. However, as mission dictates, certain smaller operations may be planned and tasked primarily to cyber units. If we were to take the previous example of Operation Instant Thunder, we could possibly have seen the commanding unit being a cyber warfare element. Attached to them may have been artillery or air support assets. In this situation unity of command would ensure that the commanders of the attached units would not use kinetic means

to destroy the target power stations. Only when the cyber unit's commander had decided that such action is necessary would such force be used. Often time issues like this arise when officers from differing battle spectrums are tasked with the same objective.

Unity of command is an essential principal applied in penetration testing today. Certain groups must be tasked with specific assignments as to prevent reproduction of work as well as even counter-productive efforts. Human senses are far more involved in kinetic warfare than in cyber warfare. As a result, overlapping efforts are easier to see and therefore remediate. However, if too friendly cyber units happen to be attack the same target simultaneously, than issues may arise in terms of stealth and even possibly loss of attack surface.

Security

“Never permit the enemy to acquire unexpected advantage”

In kinetic warfare security means having good situation awareness, always having a solid perimeter, and constantly conducting intelligence/counter-intelligence operations. Cyber assets can contribute to security within a combined arms environment in two main ways. First, don't allow any of the numerous mentioned attack vectors to destroy or disrupt your operations. Second, gather intelligence, protect vital data or even plan false data as part of a full-spectrum reconnaissance mission. This goes with a CNO environment as well.

Surprise

“Strike the enemy at a time or place or in a manner for which he is unprepared”

Again, this principal is obvious as to how it will influence the outcome of a kinetic battle. Applying cyber assets to assist in such a conflict will sound much like has been previously stated. However, the biggest difference here is that attacking the enemy at a time, place or in a manner from the cyber realm is much easier to do. Because the enemy will have certain services that are meant to be available, or will have intricate interdependencies within their infrastructure, the possibilities for attack are endless. From social engineering to remote overflow exploits, the opportunities for surprise more directly apply here than in the kinetic realm. Within a combined arms environment such disruption caused by cyber can have longer reaching effects than some kinetic attacks. For instance, a surprise kinetic attack can be geographically tracked. However, a cyber disturbance could occur in numerous places, attacking a variety of assets, all within milliseconds of each other. Such

References

- [1] Estonia's Hack Attack – <http://computer.howstuffworks.com/hacker-crash-country-network1.htm>
- [2] Iran was prime target for SCADA Worm – http://www.computerworld.com/s/article/9179618/Iran_was_prime_target_of_SCADA_worm
- [3] Water pump hack 'false alarm' – <http://www.bbc.co.uk/news/technology-16003138>
- [4] Byzantine Hades – http://threatpost.com/en_us/slideshow/10-hacks-uncle-sam/byzantine-hades
- [5] Red Storm Rising – <http://gcn.com/articles/2006/08/17/red-storm-rising.aspx>
- [6] Testimony of Allan Paller – http://hsgac.senate.gov/public/_files/042809Paller.pdf
- [7] Hackers attack Google source code – <http://www.wired.com/threatlevel/2010/03/source-code-hacks/>
- [8] Stuxnet – <http://en.wikipedia.org/wiki/Stuxnet>
- [9] US Army FM 3-0
- [10] Masterminding an Air War – <http://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/wargoals.htm>
- [11] Tactical Exploitation – http://www.slideshare.net/amiable_indian/tactical-exploitation-hdm-valsmith

disruption will definitely offset combat power from other enemy positions.

It works in a very similar way within a CNO confrontation. The primary difference is time. Within the cyber realm surprise will require a great degree of preparation in order to cause the destruction or disruption at the desired moment. To apply the principal of surprise to CNO means that great efforts should constantly be made to infiltrate the enemy at all layers; a sort of *offense in depth*. Because future objectives are not known, every attack of opportunity should be taken to posture one's own forces for surprise operations at a future time. A failure to do so will limit the effectiveness of cyber operations when need arises.

Simplicity

"Prepare clear, uncomplicated plans and concise orders to ensure thorough understanding"

Simplicity is very important in every aspect of warfare. It is very difficult to coordinate such a large group of people to do a variety of tasks perfectly synchronized with each other. Every level of complexity adds an exponential amount of time that is needed to train and rehearse the coordinated effort. Because of this cyber assets should keep their tasks relatively straight forward when working within a combined arms mission. When follow on units will be relying upon the efforts of a non-kinetic cyber force, it creates a large amount of *what-if* scenarios for that unit. Cyber assets should be given specific tasks as a form of fire support, not to be seen as a maneuvers element itself when in a combined arms environment.

When talking about a CNO campaign the exact opposite is expected. In deed the cyber assets should be seen as the maneuvers element with any kinetic attachments being a sort of support role. However simplicity still applies the same. Complexity will limit the combat power of a cyber warfare element by relying too strongly upon a smaller group of people with a large skill set. As a result, the lesser skilled

forces will be ineffective in further exploitation or attack. Keeping the attacks as simple as possible will permit the greatest application of combat power.

Conclusion

Obviously volumes of information, theory and strategy could be written on the topic. I hope that this article will help the reader envision the future of cyber warfare. Whether or not you agree or disagree, I do believe that the principles of war do apply to nation-state cyber confrontations in both a combined-arms conflict as well as a strictly CNO situation.

SKYLER ONKEN

Skyler Onken, CCENT, CISSP (Associate), CEH, ECSA, Security+ is a student of security, penetration testing and military science at Brigham Young University – Idaho. He has a background in software development and QA testing. He has developed numerous open source tools including being the project lead of the OWASP AJAX Crawling Tool. He has also presented at OWASP Salt Lake Chapter meetings and BSides Los Angeles.

<http://securityreliks.securegossip.com>
[@skyleronken](#)

** The opinions shared in this article are strictly those of the author and even then do not reflect any official positions of those of whom he is affiliated.*

Understanding

the Crime Revolution

Welcome to our time. Time dominated by Internet real estate developers such as Facebook, Microsoft and Google. With a few billion registered user units sold (accounts registered) everyone is enjoying a gorgeous view of the latest technology.

What you will learn...

- Process reverse engineering
- Business model analysis
- Activity pattern recognition
- Event and data correlation

What you should know...

- Social media capabilities
 - Principles of risk management
 - Personally Identifiable Information protection
 - Statistical analysis
-

Each room of each building of our wonderful technology paradise is equipped with the most modern appliances: easy to use interfaces, polished data delivery, crisp display of videos and music. Our units are protected by 24/7 security, locked with privacy controls, equipped with encrypted panic rooms and have spam detection sensors able to identify malicious language 50 miles away. Our toilets share knowledge about water quality and everything runs on green energy. Every morning a good looking floor technician with a security clearance and a PhD takes our garbage out. The only two things we did not consider were neighborhood crime and parking.

Our Internet Earth is currently too small to host all of our ideas because our space is defined by IPv4 address limitation. Asian companies, for example, can't park anywhere or build anything new because they are officially out of IP addresses. We have a sound solution, IPv6, and it is scheduled to take affect soon. Once it is in place our mega-technology-churches will create new neighborhoods full of buildings and parking lots and aggressively recruit members away from already existing networks by implementing seeker-friendly approach based on intensive market research and targeted advertising. This will be accomplished in order to re-pay their business loans, in the name of our personal desires and this will change our neighborhood crime ratings again.

The crime rating I am referring to is quite simple to understand. Outside of the Internet it is measured by

a number of reported crimes, sorted by crime type and divided by population of the area of study. This is a simple but imperfect formula: crime reporting is not a requirement and it means no one knows for sure if our numbers are accurate. Federal and Local law enforcement (e.g. FBI) are using this formula, but others, including the American Society of Criminology, are not. The interesting thing is that our real estate prices are hard wired to these imperfect ratings. It works like a clock: crime ratings go up, real estate prices going down.

Let's see if the same logic can be used in our Technology Paradise today. Facebook is getting close to 1 billion units sold milestone, and in my book this translates to they now have lots of data. How many crimes are there reported by Facebook users, by crime type and time period?

Facebook says not to worry about questions like this because *...there is no evidence to suggest that the use of Facebook was the cause or carrier of a criminal act ...* If we look outside of Facebook we will see crime growth reports with numbers like 300%, 400% or 500%. Both answers do not assure the consumer of anything as we have outdated data or do not include crime types, times and numbers by population at the time.

While Facebook is looking for this data, let's see what our IT Earth police are saying about the neighborhood crime. IC3 (www.ic3.gov) is free for everyone and available 24/7. It is designed, provided and managed by the FBI and we expect the FBI to be everywhere and

know everything. So how many crimes and crime types occurred on LinkedIn between March of 2009 and April of 2010? I see no answer.

Let's make sure we are all on the same page and discuss further what happens to a neighborhood crime rating once new businesses open or old ones close. The neighborhood crime rate changes depending on the business type and size. Think of what is going to happen to the price of your home if someone builds a 10 million seat capacity stadium 3 miles away from it and replaces every single tree in your area with an advertising billboard? This kind of development is sure to affect the value of your home, your ability to sell it, your ability to get to work on time, and will undoubtedly change your sleeping habits. It is also guaranteed to increase your chances of being raped, robbed or murdered, and you are going to have to deal with it.

Our technology builders know how to raise capital in a very short time using elevator pitches and *sell me your idea in 10 words my dog can repeat* technique. It is all about the impression and promises they make to the banks and to us, the users. It looks easy but in reality their million dollar bonuses and billion dollar stock options always come with a hefty price tag. On one hand they have us, the users, who never sleep and want to run naked and shoot guns. On the other hand they have banks demanding high return from a business model based on allowing a bunch of people to run naked shooting guns. Our Technology Super-Marios have to explain how they are going to do this in 10 words or less. So as you can imagine, these college dropouts make mistakes from time to time, and because technology is cheap these mistakes are changing our lives forever and we have to deal with it.

We want to post pictures of our kids, talk about our lives and make new friends. They build wonderful networks for sharing of our personal data. We make new friends, they generate millions of dollars, and identity fraud becomes the most profitable business on our little sunny planet. We want new jobs. They build us professional networking applications allowing us to describe our work in detail. We get new jobs and we feed priceless insider information to anyone who is willing to listen. We want to share our locations with friends because we are too busy to call them. No problem: our cars, watches and cell phones are doing it now with ease. Developers get paid and our houses are broken into more, home invasion risk goes up and so do the profits.

Yes, we are all told to be careful and to watch our backs. We know that if we leave a laptop in a parked car overnight it can be stolen. Once it is gone we always have to answer why, especially if we want someone to reimburse us for the loss. It is true that the car manufacturer had an overnight laptop charging station installed in the car. It is true they also provided a wonderful leather laptop

holding case on the back seat and enabled us to sync our laptop data with any device in the world including the *Mir* space station. Yes the car also had a video conference system and performed *parked-overnight-only* laptop data online backup and data encryption for free. The car also included a patent protected sign *LAPTOP FRIENDLY CAR*, which was printed on all windows and doors, and it had a blinking indicator on the roof which turned itself on if a laptop was detected. However, the car manufacturer also told us to be careful and never use our laptops in this type of car, because it may cause traffic incidents and property theft.

We don't know how to understand our Internet neighborhood crime, but every single person connected to the Internet knows which neighborhood has the "laptop friendly" cars and where to look for them. We all know it by design because every single building in our Internet city is designed to host a special type of a car/user/garage and broadcast its technical type, capability and availability using all existing frequencies at the same time. That's why everybody knows where to go for PII (Personally Identifiable Information) or for business intelligence. LinkedIn Tower hosts business intelligence. Facebook Radio Tower broadcasts personally identifiable information. Craigslist Park is also currently known for serial killers after dark.

Still there's no crime rating, however we now have detailed crime types and we can make our research specific to a certain building (online service) or a real estate developer (company or investor) in general. Before we do so, we will need to agree on what we are looking for. I propose to select a few types of criminal activity for a start. Something we're all aware of and don't have to research at all:

- Password Guessing (theft of credentials)
- Corporate Insider Knowledge
- Identify Fraud

Password Guessing

Remember the game of 20 questions? Mathematically, if each question is structured to eliminate half the objects, 20 questions will allow the questioner to distinguish between 220 or 1,048,576 subjects. The good news is these big numbers are directly applicable to the cracking of your online bank password. Any data allowing simplification of gaining unauthorized access to your online accounts (personal and corporate credentials, online banking, email accounts, benefits management, investments, medical records, employment history, etc.) can be helpful. If *123456* (this password was actually blocked by Hotmail on July 18, 2011) and *jesus*, *password* and *love* did not work to open your Bank of America account, the next step should be to learn a few things about your *favorite pet's*

EXTRA ARTICLES

N	Question Type	Question
1	Administrative	Account type
2	Administrative	Anniversary
3	Administrative	Anything Else
4	Administrative	Profile visibility to public
5	Administrative	Your primary email address
6	Administrative	Your secondary email address
7	Administrative	Your secret question
8	Administrative	Your Secret question 2
9	Administrative	Bragging rights
10	Administrative	Title
11	Insider Knowledge	Associations you are a member of
12	Insider Knowledge	Awards
13	Insider Knowledge	Company
14	Insider Knowledge	Education
15	Insider Knowledge	Employer
16	Insider Knowledge	Industry
17	Insider Knowledge	Job Description
18	Insider Knowledge	Job Status
19	Insider Knowledge	Job Time Period (from to)
20	Insider Knowledge	Job Title
21	Insider Knowledge	Occupation
22	Insider Knowledge	Profession
23	Insider Knowledge	Projects you are involved with
24	Insider Knowledge	Recommendations
25	Insider Knowledge	Skill name
26	Insider Knowledge	Work address
27	Insider Knowledge	Work City
28	Insider Knowledge	work country/region
29	Insider Knowledge	Work Division
30	Insider Knowledge	work email
31	Insider Knowledge	work fax
32	Insider Knowledge	work pager
33	Insider Knowledge	Work phone
34	Password Guessing	Best Features
35	Password Guessing	Books I want to read
36	Password Guessing	Favorite Books
37	Password Guessing	Favorte Authors
38	Password Guessing	Elementary School Country
39	Password Guessing	Elementary School Name
40	Password Guessing	Elementary School State
41	Password Guessing	Family
42	Password Guessing	Favorite Actors
43	Password Guessing	Favorite athletes
44	Password Guessing	Favorite Foods
45	Password Guessing	Favorite Games
46	Password Guessing	Favorite heroes
47	Password Guessing	Favorite Movies
48	Password Guessing	Favorite Music
49	Password Guessing	Favorite Places
50	Password Guessing	Favorite quotations
51	Password Guessing	Favorite quotes
52	Password Guessing	Favorite sports
53	Password Guessing	Favorite teams
54	Password Guessing	Favorite Television show
55	Password Guessing	General interests
56	Password Guessing	Groups you belong to
57	Password Guessing	Hometown
58	Password Guessing	Junior High School Name
59	Password Guessing	Junior High School State
60	Password Guessing	Junior High School Country
61	Password Guessing	Languages you speak
62	Password Guessing	Looking for (interested in)
63	Password Guessing	Maiden name
64	Password Guessing	Movies I want to see
65	Password Guessing	Neighborhood
66	Password Guessing	People I'd like to meet
67	Password Guessing	People who inspire you
68	Password Guessing	People who like you online (featured friends)
69	Password Guessing	People you like online (subscriptions)
70	Password Guessing	Places I want to visit
71	Password Guessing	Places lived
72	Password Guessing	School Activities
73	Password Guessing	School Additional notes
74	Password Guessing	School City
75	Password Guessing	School Country
76	Password Guessing	School dates attended (from to)
77	Password Guessing	School degree
78	Password Guessing	School field(s) of Study
79	Password Guessing	School Societies
80	Password Guessing	School State
81	Password Guessing	Student Status
82	Password Guessing	Urls about you
83	Password Guessing	Urls featuring your work
84	Password Guessing	Urls you are interested in
85	Password Guessing	Website
86	Password Guessing	Your Activities
87	Password Guessing	Your Facebook account
88	Password Guessing	Your IM Screen Name(s)
89	Password Guessing	Your Interests
90	Password Guessing	Your Twitter account
91	Password Guessing	Your url
92	PII	About me
93	PII	Bio
94	PII	Birth day
95	PII	Birth year
96	PII	Body Type

name, food, movie, school, band, brand, music, movie, T.V. show, car, sports team and other interesting things like middle name or place of birth, places you want to visit. This approach works for the majority of human population of the Internet today.

97 PII	Children
98 PII	College/University Class Year
99 PII	College/University Concentration
100 PII	College/University Name
101 PII	Country
102 PII	Current City
103 PII	Drinker
104 PII	Employment
105 PII	Ethnicity
106 PII	First name
107 PII	Full Middle Name
108 PII	Full Name
109 PII	Gender
110 PII	High School
111 PII	High School Class Year
112 PII	High School Concentration
113 PII	Home address
114 PII	Home Fax
115 PII	Home Phone Number
116 PII	Honors
117 PII	Income
118 PII	Last Name
119 PII	Location
120 PII	Marital status
121 PII	Middle Initial
122 PII	More about you
123 PII	Nicknames
124 PII	Other names
125 PII	Personal Mobile number
126 PII	Photo
127 PII	Political Views
128 PII	Relationship status
129 PII	Religion
130 PII	Sexual orientation
131 PII	Significant other
132 PII	Smoker
133 PII	State
134 PII	Time Zone
135 PII	Your Phone number(s)
136 PII	Your Zip Code

Summary of questions asked by Gmail, HotMail, Yahoo, Twitter, LinkedIn, Facebook, MySpace and Tagged

Corporate Insider Knowledge

Data provided by insiders is considered more accurate and valuable than in-depth theoretical analysis performed by an outside expert. This is due to the insider's firsthand knowledge of a company's project, team, team climate, corporate culture, goals, as well as current financial situation and priorities. Ask a stranger about confidential information pertaining to his/her job and he/she will tell you why these questions are none of your business. Some of the questions about our employment are also considered potential PII (*Personally Identifiable Information*), for example: salary, job location and job position. 20 questions, if crafted specifically, is going to help a 3rd party to understand not only your company's goals but what type of contracting it does for the government, for example.

Personally Identifiable Information (PII): Information that can be used to uniquely identify, contact or locate a single individual. It can also be exploited for identity fraud or committing a crime. Examples: full name, date of birth, birthplace; country, state, or city of residence; age, gender, nickname(s), other names, places lived, religion, school or university information. Availability of this information has a direct impact on global crime trends.

With this in mind let's take a look at a few large buildings in our Technology Manhattan of 2011: Gmail, HotMail, Yahoo Mail and AOL (email providers); Twitter Tagged, LinkedIn, Facebook and My Space (social networking). Let's see if any of them are playing the 20 question game by design and by doing so influence our neighborhood crime ratings.

At the time this article was written, the companies mentioned above asked every one of their approximately 2 billion users a few questions. MySpace and Facebook user profiles asked over 40 questions each; Tagged, Yahoo and LinkedIn 30 or more each; HotMail and Gmail under 30 each; and Twitter and AOL approximately 10 each. Once we collect all the questions together, we see the number of questions asked by all both as a collective and individually, by service type, by investor, by size or by technical capability. We begin to understand what types of data these companies prefer to collect and how much effort they put into collection of specific data. We now also know what they ignore and if they work together or not. We are able identify if we are probed for *Password Guessing*, *Corporate Insider Knowledge* and *PII* types of questions, and we want to know this because availability of this data defines our neighborhood crime ratings.

At the time of the study I identified more than 130 unique questions. If we ignore the administrative account setup questions (preferred login name, password, title etc.), we see 58 Password Guessing, 44 PII and 23 Insider Knowledge questions. Email Providers wanted to know 65 things and asked 27 PII, 16 Password Guessing and

13 Insider Knowledge questions. Social networking sites asked 70 questions: 31 Password Guessing, 23 PII and 11 Insider Knowledge.

Facebook

Facebook dedicated almost 60% of its 40 questions to Password Guessing game. It was also interested in your PII data but almost ignored your Insider Knowledge.

Neighborhood crime rating:

- Theft of credentials: 58%
- PII: 39%
- Insider Knowledge: 3%

LinkedIn

LinkedIn. With 30 questions and the mission of connecting professionals to each other and their companies, LinkedIn managed to ask more Password Guessing questions than Insider Knowledge. In my personal opinion their questions are the most balanced across the entire spectrum of our study and it makes them the foremost major equal risk opportunity network of our time.

Neighborhood crime rating:

- Theft of credentials: 37%
- Insider Knowledge: 33%
- PII: 30%

MySpace

MySpace posed over 40 questions about who you are, including whom you want to have sex with, how much you make and how you look. They also wanted to know if you use drugs and have kids. No other network wanted to know these things with the exception of good-ole MySpace.

Neighborhood crime rating:

- PII: 43%
- Theft of credentials: 40%
- Insider Knowledge: 16%

Tagged

Tagged offered over 30 questions with a concentration on Password Guessing business first and PII second. It showed no interest in professional life of any kind. This was the first network on our list which wanted to know what elementary school you had gone to and who you wanted sleep with at the same time. This is also the only network inquiring about your relationship status and your best feature, as well as reminding you not share personal information on the Internet on the same page, a good example of the *Laptop Car* manufacturer approach.

Neighborhood crime rating:

- Theft of credentials: 59%
- PII: 40%
- Insider Knowledge: 0%

Twitter

Twitter is doing best on the list of the social network providers. It only asks 10 questions, which is 60% less questions than the industry standard we established and 10 questions shy from qualifying for the 20 questions game analysis.

Now let's move to our email providers. During our social network review I saw two key questions they all wanted to know: your name and phone number.

In contrast to social networks email service providers wanted to know 5 things about you: name, birth date, gender, Facebook account and your secondary email. Seems strange because email providers are not in business of matching users socially and my Facebook account is irrelevant to my gender or sex.

And it gets more interesting from then on.

Yahoo

Yahoo is asking 300+ million users 30+ questions. Yahoo is the only email provider asking users for a Second Security Question. However, its seemingly great customer care record is flawed by a number of password guessing broadcasts (places I wanted to visit, favorite music, movies, favorite quotes, places, food, books, interests). Besides asking password questions this email service provider wants to know what high school and college users went to, including class year, school name and study concentration. On top of Password Guessing questions and education level inquiries this email provider also wanted to know whom Yahoo users were working for, including job title and time spent on each job. In my personal opinion none of the questions are relevant to email functionality at all. Neighborhood crime rating:

- PII: 42%
- Theft of credentials: 32%
- Insider Knowledge: 10%

Windows Live (HotMail)

Windows Live (HotMail) is asking 300+ million users just under 30 questions. It is the only email provider which wants to know your fax number, your home phone number and your personal mobile number, but doesn't ask for your home address. They also don't waste time and ask everyone about their profession, work pager, work fax, work email and work phone, but don't put much effort in password guessing business. Neighborhood crime rating:

- PII: 48%
- Insider Knowledge: 33%
- Theft of credentials: 11%

Gmail

Gmail is asking its 200 million users about 30 questions. This is the only email service provider that wants to know your other names and nicknames, see your picture and learn about places you lived and asks the same questions that are usually raised during security clearance investigations. Gmail is also the only email provider which asks for your work address and projects you are involved with, Urls about you, Urls featuring your work and Urls you are interested in. Gmail trusts you to have a primary email (the rest of email providers think their email is automatically the primary one). Not sure why they want to know about your education and employment history but I'm sure it is for a good cause.

Neighborhood crime rating:

- PII: 41%
- Theft of credentials: 26%
- Insider Knowledge: 15%

Examining this sample data made me think about how information technologies are impacting society and culture and how society and culture impacts information technology. What is going to happen if our Techno Giants are required to evaluate and report the expected crime influence of their services and applications on their users? What if services and applications are rated for user safety the same way our cars are rated for crashes? What if these ratings are clearly communicated and explained during each account creation? What is going to happen to a service if their crime rating goes up? Do you think some vendors will go away and some will have to perform heavy maintenance? Do you think doing this will enable us to understand Internet neighborhood crime better and live a safer life? What is going to happen if for each question in user profile we will see an explanation of the associated risks like: *Answering this question can increase your chances of being a victim of Identity Fraud?* We do this all the time during medicine, tobacco and liquor sales. It is the law.

Even if things are currently designed to make us crime targets no one can stop us from protecting ourselves and creating a building code helping us to prevent the crimes. This code is needed to protect our health, safety and general welfare. This code must be enacted by an appropriate authority, and we, the people, the users, the market, have this authority. All we need to do is to make it happen.

IVAN VENCLOVA

www.hakin9.org/en

[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?
Here's a chance to prove it.

[IT'S IN YOUR PULSE]

LEARN:

Advancing Computer Science	Network Security
Artificial Life Programming	Open Source Technologies
Digital Media	Robotics and Embedded Systems
Digital Video	Serious Games and Simulation
Enterprise Software Development	Strategic Technology Development
Game Art and Animation	Technology Forensics
Game Design	Technology Product Design
Game Programming	Technology Studies
Human-Computer Interaction	Virtual Modeling and Design
Network Engineering	Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

Please see www.uat.edu/fastfacts for the latest information about degree program performance, placement and costs.

Using Social Engineering to reconnaissance your victim

Social Engineering is a phase of hacking, that including the External reconnaissance. It is nontechnical approach to breaking a system of network. It is deceiving users of a system. With social engineering hacker is convincing user to perform acts useful.

What you will learn...

- How to brake Social Engineering
- Physical Social Engineering Tools

What you should know...

- Basic Knowledge on Social Engineering
-

Hacker can be earn information about victim. Social engineering is an important phase because hacker can use it to attack the human element. Hacker use social engineering before or during an attack, if you look at Wikipedia about it, you can see 'The practice of obtaining confidential information by manipulation of legitimate users.'

Some tools used for for social engineering, like: Internet or Telephone. In social engineering hacker exploit the natural tendency of a person but in another attack hacker use security holes. If we want say in one sentence, Social Engineering is to trick someone into providing valuable information, with social engineering hacker maybe trick user to execute some command, for example hacker tell user for login, in to the system and run a command. In most case hacker pretend that he/she is a part of another company that support your network. People are usually the weakest link in the security chain. in social engineering attack The manipulation of legitimate users is important. In most case Social Engineering is success because Unfortunately, humans are not as easy to secure as a web server. Defense against social engineering is hard, because a company can't use software or hardware for protect itself. Attacker use social engineering because 1-human not have any patch for bug fix 2- People are the largest vulnerability in any network.



Social engineering can be broken into two common types

Human-Based

Human-Based social engineering is person-to-person. for example hacker speak with some employee face to face and earn information. Impersonation of employee or user, Calling technical support, Shoulder surfing or maybe search in trash for information.

Computer-Based

Hacker use some software for trick user, for example phishing pages or fake emails. Hacker can be sent a fake mail for a company and bring up some security hole or problem.

We can categorized Human-based Attack as flow

Impersonating an Employee or Valid User

In type of attack, hacker pretends to be an employee or valid user on the system. When a hacker can successfully do it, he/she can gain physical access, because he/she pretending to be a janitor, employee, or contractor .in this type of attack hacker can Sitting behind a computer and find useful information.

Role as an Important User

In this type of attack, the hacker pretends that he/she is a manager that needs to gain access to a computer system or files. To achieve this goal,hacker find a lower-level employee like a help desk. Most of help desk won't question about who speak with them.

Using a Third Person

In this type,hacker pretend, he/she can be use your system as a legal user. This attack is especially effective because a real user maybe on vacation or can't be contacted for verification.

Calling Technical Support

It is a classic way. At a Company help desk or technical support trained for help users that they can be a good choice for Social Engineering.

Shoulder Surfing

It is a technique for gathering password. in this way hacker watch a valid user log in and then use that password to gain access to the system.

Dumpster Diving

This is a Dirty way, because hacker looking in the trash for information. Many Companies often waste useful information without destroy. For example they using crushing machine for destroy papers but many hackers Putting the paper together. Hacker can find password, file names or confidential information.

Advanced method of gaining illicit information is know as reverse social engineering .in this way, hacker create a person that appears to be in a position of authority.

Computer-Based Social Engineering

This type of attack include the following:

- Email attachments
- Fake websites
- Pop-up windows

In this way hacker not have any physical access and use their skills. hacker can be run a fake website or find other companies that contract with the victim, then hacker sent a fake email for victim.

With Phishing page, hacker make a fake website like credit card company, posing as a bank or other financial organization. Social engineering can be performed via some tools like physical, Computer-Based and Phone.

Physical Social Engineering Tools

Cameras

Cameras can be a useful tool, because they can capture necessary information. It is a best way for take a picture of information. A good feature of cameras is they can record video too. Cameras that are used for social engineering are Small and not make any noise when the picture is taken. You can use some type of this cameras:

- Small/Compact
- Cell Phones
- Covert
- Qik

GPS Tracker

GPS is another tools for track a victim. Hacker can be use Google Map via GPS for track a victim. Usually this device is light weight, easy to use and hide. It have a sensor and can be detect movement and stop. It runs off of vibrations. When it feels movement it turns on.

Pen Recorder

As the name is clearly, it is a pen that can be record. This device can be covers long range for records and for run it, no software is needed. It is fully functional pen, Means you can write with it.

Rf bug kits

It is a wireless audio surveillance gadget, with this device you can listen to conversations from 300+ meters away. Some of the features are:

- Complete audio spy kit
- Wireless audio transmitter + receiver in package

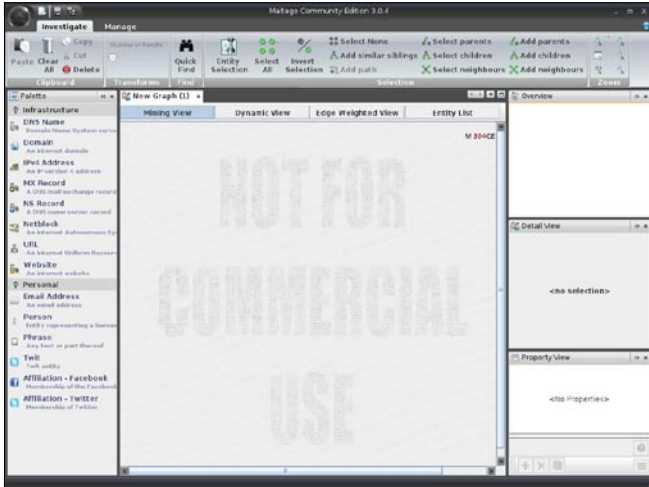


Figure 1. Maltego

- The transmitter is small enough to hide almost anywhere
- Professional grade audio bug with 300+ meter transmission
- Use receiver to listen to the audio or to record it for later review
- 3.5mm line OUT jack to record the audio to DVR or similar audio recording device

This device have a nice quality.

Computer Based Social Engineering Tools

Some tools can be used for this purpose that you can see they.

Maltego

Maltego is an open source tools for forensics purpose. This tools is used for mining and gathering of information and show the output in a easy to understand format. Maltego can be show you relationships between information. With this tools you can finding links between bits of information. It will save you time and will allow you to work more accurately and smarter. This tools have Free Version and a Commercial Version. Some of the features:

- Domain Names
- Whois Information
- DNS Names
- Netblocks
- IP Adresse

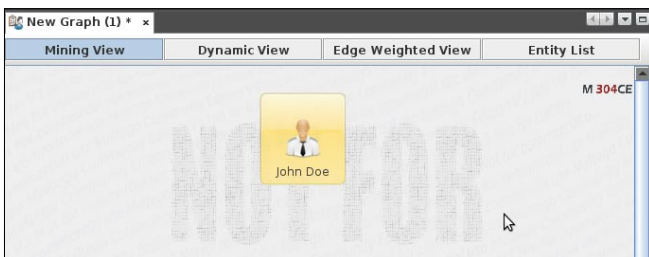


Figure 2. Add a element

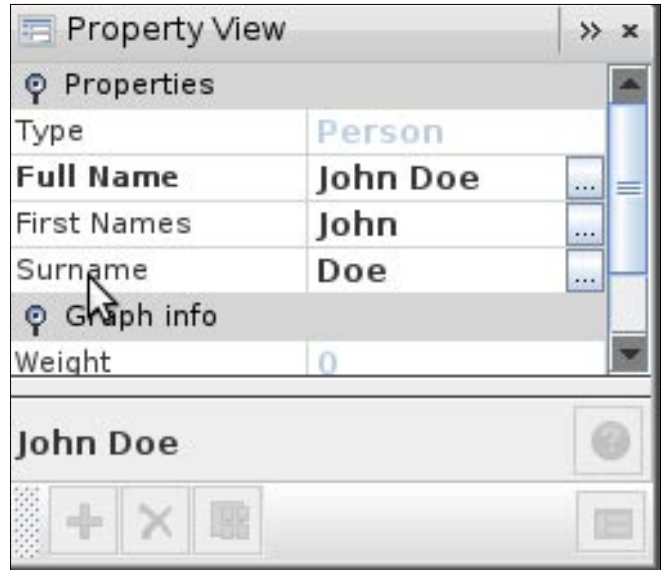


Figure 3. Property View

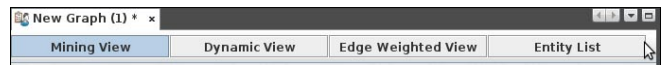


Figure 4. Toolbar

This tools can be used for enumerate People information therefor it is a good tools for Social Engineering. whit it you can determine the relationships and real world links between:

- People
- Groups of people (social networks)
- Companies
- Organizations
- Web site

When you run it,you must Register an account in *paterva.com* and then use it. Let us consider you did it. you can see Maltego Environment like below: Figure 1.

In the left panel, Click Person and Drag it in the midst: Figure 2.

On the right side you can see Property view and can be change Person information (Figure 3).

At the top in the middle we have four different views:

- Mining View
- Dynamic View
- Edge Weighted View
- Entity List (Figure 4)

As you see in the left side panel, you can select some palette for your victim, For example you can find relationships between your victim and a URL, Website, select your Items and drag they in midst, after it you should specify a Relationship between your victim and target, for do it click on person and you can see a arc and select target, after it a window appears that you should select a label for Relationship (Figure 5).

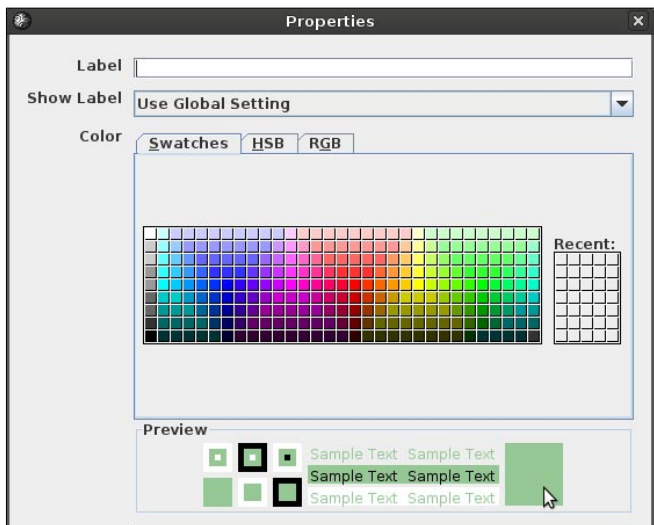


Figure 5. Add a Label

OK, in this Example I want find a Relationship between my victim and a person on the Facebook: Figure 6.

Now, Right click on Person and select *Run Transform* then you can select *All Transforms* or specify (Figure 7). After it you can see the result: Figure 8.

Maltego Mesh

It is a plugin for Firefox and help you to analysts a web site quickly and find usefull information within a page. By default Maltego Mesh searches for the following *entities* within a page:

- IP Addresses
- Email Addresses
- Netblocks
- Named entity Extraction (SillyNer)
- Phone Numbers
- Websites
- Dates

It is Free.

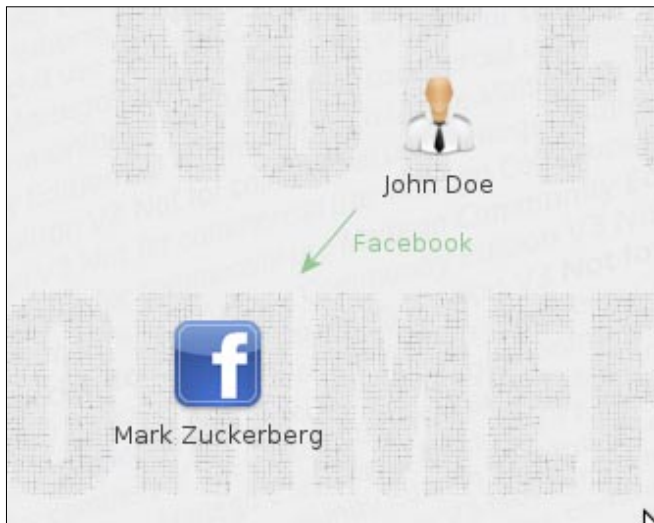


Figure 6. Relationship

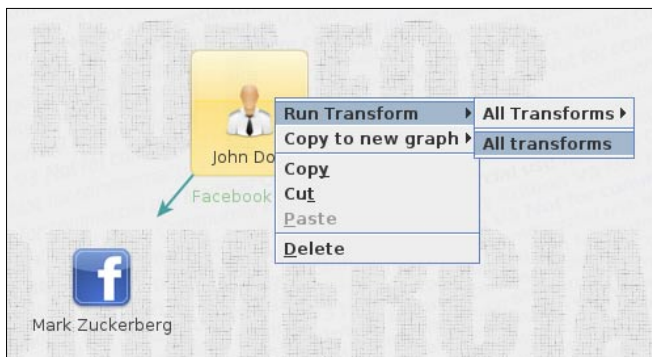


Figure 7. Run a Search

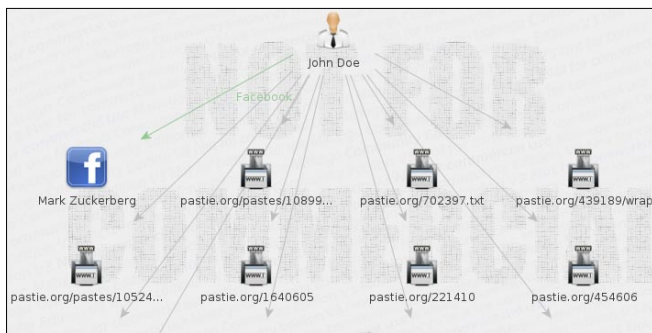


Figure 8. Result

Mesh can be find email address in the format of (andREMOVErewREPLACE-WITH-ATpatervaDOTCOM).

Social Engineer Toolkit (SET)

SET is designed to perform advanced attacks against the human element. This tools became a standard tool in a penetration testers arsenal. SET was written by David Kennedy. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test. You can find it in Backtrack Linux (Figure 9).

This tools offer:

- Spear-Phishing Attack Vectors
- Website Attack Vectors
- Infectious Media Generator
- Create a Payload and Listener



Figure 9. SET Console

- Mass Mailer Attack
- Teensy USB HID Attack Vector
- Update the Metasploit Framework
- Update the Social-Engineer Toolkit
- Help, Credits, and About
- Exit the Social-Engineer Toolkit

For more information about this tools and how it work, Please see <http://www.social-engineer.org>.

Common User Passwords Profiler (CUPP)

CUPP can predict specific target passwords by exploiting human vulnerabilities. This tools written in Python language. It can be used in situations like legal penetration tests or forensic crime investigations.

Who's Your Daddy Password Profiler (WYD)

It used for two reason:

- A penetration test should be performed and the default wordlist does not contain a valid password
- During a forensic crime investigation a password protected file must be opened without knowing the the password.

Phone

Many People in the world use Cell phone and They face every day with caller id,Therefore it is a good technique for Social Engineering. Some tools used for Caller ID Spoofing that you can see they below:

SpoofCard

A popular way for Spoof Caller ID is SpoofCard, with this Card you call up the 1-800 number, enter your PIN number and a number that you like the caller ID to display then Enter the the phone number that you want speak with it. It have some prons and cons.

Prons:

- Simple
- No extra hardware or software needed
- Proven service with thousands of customers

Cons:

- needed money

Asterisk

If you have a Voip service,then you can use Asterisk to Spoof Caller ID. It have some prons and cons.

Prons:

- Free.

Cons:

Reference

- CEH Certified Ethical Hacker Certification
- CEH Certified Ethical Hacker STUDY GUIDE Exam 312-50 Exam EC0-350
- Hacking the Human
- <http://www.social-engineer.org/>
- <http://www.ethicalhacker.net/content/view/202/24/>
- <http://www.paterva.com/web5/>

- Extra computer or VM needed
- Current VOIP service / provider

SpoofApp

If you use iPhone, Android or the Blackberry then You can use SpoofAPP, it use SpoofCard but it is a package in your Cell phone.

Voicemail

It is a major attacks that can be launched using cell phone. If an attacker was to obtain the victims cell phone number and spoof it, The Voicemail Is a good choice.

Unmasking Caller ID

There are some methods to help you find the actual source of a call.

Summary

As you read some of Social Engineering trick can be bypass and some they can't. the best way for prevent Social Engineering is Training users.

MOHSEN MOSTAFA JOKAR

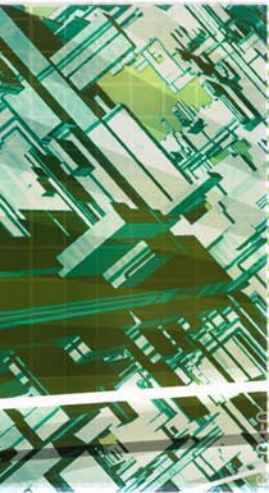
My name is Mohsen Mostafa Jokar. I'm a software engineer and a GNU/Linux Fan (RHCSA,RHCE). I like Security Research and work on it,I'm a Ethicalhacker too.

The Industry's First Commercial Pentesting Drop Box.

THE Pwn Plug.



Air Freshener?



Printer PSU?
...nope



FEATURES:

- ★ Covert tunneling
- ★ SSH access over 3G/GSM cell networks
- ★ NAC/802.1x bypass
- ★ and more!



PWNIE EXPRESS

@pwnieexpress.com

Discover the glory of
Universal Plug & Pwn

t) @pwnieexpress **e)** info@pwnieexpress.com **p)** 802.227.2PWN

Secure deletion

The Internet has empowered us to do more with our electronic devices. We do everything from our taxes to shopping and sending private messages.

Our devices become a hotbed of personal data that is of interest to malicious parties. Deletion of files and caching is insufficient in preventing harvesting of your information that resides on your devices. The solution is secure deletion or wiping to overwrite those files with random data to eliminate the chances of data recovery.

There are readily available tools out there that facilitates wiping of files. Free tools that can be downloaded and installed include popular tools like Eraser, CCleaner as well as BleachBit.

This column will explore wiping of files and caching with the use of a tool called Secure-delete.

Note: Secure-delete is installed and executed from Ubuntu 10.04 LTS.

Install the tool.

```
commandrine@bridge:~$ sudo apt-get install secure-delete
```

List the options by entering the srm command.

```
commandrine@bridge:~$ sudo srm
srm v3.1 (c) 1997-2003 by van Hauser / THC <vh@thc.org>
```

```
Syntax: srm [-dflrvz] file1 file2 etc.
```

Options:

- `-d` ignore the two dot special files „.” and „..”.
- `-f` fast (and insecure mode): no `/dev/urandom`, no synchronize mode.
- `-l` lessens the security (use twice for total insecure mode).
- `-r` recursive mode, deletes all subdirectories.
- `-v` is verbose mode.
- `-z` last wipe writes zeros instead of random data.

srm does a secure overwrite/rename/delete of the target file(s).

Default is secure mode (38 writes).

You can find updates at <http://www.thc.org>

Listing 1. Secure deletion of files within a folder

```
commandrine@bridge:~$ sudo srm -rllv test/*.*
```

```
Using /dev/urandom for random input.
```

```
Wipe mode is insecure (one pass [random])
```

```
Wiping test/1423.pdf * Removed file test/1423.pdf ... Done
```

```
Wiping test/Hakin9_03_2012.pdf * Removed file test/Hakin9_03_2012.pdf ... Done
```

```
Wiping test/Hakin9_Extra_2_2012_EN-ebook.pdf * Removed file test/Hakin9_Extra_2_2012_EN-ebook.pdf ... Done
```

Listing 2. Script ubuntuprivacy

```
#!/bin/sh
echo "\033[0;34mProceeding to clean your system to ensure your privacy.\033[0m"
echo
echo "\033[0;31mWiping Firefox history and cache.\033[0m"
#sudo srm -rllv .mozilla/firefox/*.default/*.sqlite
sudo srm -rllv .mozilla/firefox/*.default/addons.sqlite
sudo srm -rllv .mozilla/firefox/*.default/chromeappsstore.sqlite
#sudo srm -rllv .mozilla/firefox/*.default/content-prefs.sqlite
sudo srm -rllv .mozilla/firefox/*.default/cookies.sqlite
sudo srm -rllv .mozilla/firefox/*.default/downloads.sqlite
#sudo srm -rllv .mozilla/firefox/*.default/extensions.sqlite
sudo srm -rllv .mozilla/firefox/*.default/formhistory.sqlite
sudo srm -rllv .mozilla/firefox/*.default/permissions.sqlite
#sudo srm -rllv .mozilla/firefox/*.default/places.sqlite
sudo srm -rllv .mozilla/firefox/*.default/search.sqlite
sudo srm -rllv .mozilla/firefox/*.default/urlclassifier3.sqlite
sudo srm -rllv .mozilla/firefox/*.default/webappsstore.sqlite
sudo srm -rllv .mozilla/firefox/*.default/Cache/*
echo "\033[0;32mFirefox history and cache wiped.\033[0m"
echo "\033[0;31mWiping Trash.\033[0m"
sudo srm -rllv .local/share/Trash/
echo "\033[0;32mTrash wiped.\033[0m"
echo "\033[0;31mWiping Applications history and cache.\033[0m"
sudo srm -rllv .recently-used
sudo srm -rllv .recently-used.xbel
sudo srm -rllv .thumbnails
sudo srm -rllv .macromedia/Flash_Player/#SharedObjects/*
#sudo srm -rllv .openoffice.org/*/user/temp
#sudo srm -rllv .openoffice.org/*/user/backup
sudo srm -rllv .libreoffice/*/user/temp/*
sudo srm -rllv .libreoffice/*/user/backup/*
sudo srm -rllv .purple/logs/*/*
sudo srm -rllv .xsession-errors
sudo srm -rllv .gimp-*/tmp
echo "\033[0;32mApplications history wiped.\033[0m"

#"ubuntuprivacy" written by commandrine.
#Please send comments and queries to commandrine[at]gmail[dot]com.
#Version 4.0 dated 9th Nov 2011.

#Save this script to your home folder. Run "sudo chmod +x ubuntuprivacy.sh" to make it executable.
```

Listing 3. *Ubuntuparanoia*

```
#!/bin/sh
echo "\033[0;34mProceeding to wipe your memory, swap and free space. Please be warned that this is time
      consuming and may take hours.\033[0m"

echo
echo "\033[0;31mWiping memory.\033[0m"
sudo smem -lv
echo "\033[0;32mMemory wiped.\033[0m"
echo "\033[0;31mWiping swap.\033[0m"
#Please run "cat /proc/swaps" to determine your mounted swap devices and customise the following line for your
      machine.
sudo swapoff /dev/sda5
sudo sswap -llv /dev/sda5
sudo swapon /dev/sda5
echo "\033[0;32mSwap wiped.\033[0m"
echo "\033[0;31mWiping free space.\033[0m"
sudo sfill -llv /home/
echo "\033[0;32mFree space wiped.\033[0m"

#"ubuntuparanoia" written by commandrine.
#Please send comments and queries to commandrine[at]gmail[dot]com.
#Version 1.0 dated 16th Sept 2009.
#Pre-requisite is having "secure-delete" installed. Install it using "sudo apt-get install secure-delete".
#Save this script to your home folder. Run "sudo chmod +x ubuntuparanoia.sh" to make it executable.
```

Secure deletion of files within a folder is simple (Listing 1). Similarly, wiping a folder is straight forward too.

```
commandrine@bridge:~$ sudo srm -rllv test
Using /dev/urandom for random input.
Wipe mode is insecure (one pass [random])
Wiping test DIRECTORY (going recursive now)
Removed directory test ... Done
```

Besides file and directory wiping, Secure-delete can be applied to provisioning privacy on your desktops and laptops. I harness the tool to script the wiping of my browser history and cache, trash as well as my applications history and cache. I call the script *ubuntuprivacy* (Listing 2).

I wrote another script, *ubuntuparanoia*, to wipe the memory, swap and free space on your Ubuntu system (Listing 3).

Wiping can be applied to different areas of your life. It can be time consuming so strike a balance between practicality and paranoia.

MERVYN HENG

Mervyn Heng is into Ubuntu, Comic Universe characters, Pop culture and Art outside of Information Security. If you have any comments or queries, please contact him at commandrine@gmail.com.





Get the best real-world
Android education anywhere!

Attend

AnDevCon III

The Android Developer Conference

May 14-17, 2012

San Francisco Bay Area

AnDevCon is the biggest,
most info-packed, most practical
Android conference in the world!

"AnDevCon was an informative and comprehensive presentation of Android development concepts, tools and techniques."

—Patrick Burrell, Sr. Research Scientist, Amway

"The conference is worth the time and expense. It's a great place to meet talented people in the Android industry."

—Keith Collins, CTO, Neusoft

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."

—Joshua Turner, Software Engineer, Primary Solutions

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!

Register Early
and SAVE!



Follow us: twitter.com/AnDevCon

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

A BZ Media Event

Register NOW at www.AnDevCon.com

Zombies and Economics

– Why the Law Inhibits Good Security Business Cases

Considering information security as a standalone good or service that is demanded specifically by business leadership is incredibly misleading. A while ago, I was doing some academic research into cost models for information security.

What you will learn...

- A little bit about zombies
- Some basic economics – e.g. supply and demand

What you should know...

- How different pieces of legislation can work against each other
- The unintended consequences of legislation
- Why a real common body of knowledge on security incidents is extremely difficult to develop

As part of this, I developed a panel of experts to bounce some ideas off, drawing on individuals with extensive bodies of security experience in banking, government, telecoms, and a number of other areas. One of the ideas that was discussed was that organisations don't, in fact *buy security*. One of the panel members, a respected security manager with especial expertise in rooting out vulnerabilities in regulated environments (e.g. banking) went a little further.

He offered the view that *security* is a secondary attribute in any given application regarding either technologies or processes. Hence, he asserted that, in his mind, it was only ever a compliment in mainstream applications, in economic terminology. In other words, an analogy could be the demand for motor vehicles and tires. While some demand may exist for tires independent of wheeled vehicles, these would be small scale and relatively specialist applications. Moreover, he offered the view that demand was relatively weak compared to the primary attributes required of a project. Hence, a discussion ensued which established that he was referring to the concept of elasticity; in other words, in his view, the cross-elasticity of demand would be less than 1 (i.e. demand for one would not increase directly proportionately with demand for the other), but would vary based on factors such as the sector in which the decision was being made, the seriousness with which regulation was

taken, and *political* considerations (i.e. the relative bargaining power of internal stakeholders).

One of the underlying issues in determining the value of information security activity is the lack of a substantive benchmark for what *good* looks like. For example, the ISO 27000 series provide a purely qualitative guide for information security practices, with no hard quantities measures for what constitutes best practice or graduations thereof. In turn, this translates into a propensity for intuition based risk management practice, as identified as a problem by expert panel member B, given the implied information asymmetry between information security professionals and business decision makers. As has been noted, some data does exist, but these data sets are incomplete. Moreover, practical objections exist as to the usefulness of a pan-profession body of data, as opposed to a sector-based set – would it be useful for a small technology firm to know how much a security breach typically costs in a multinational bank and a government department for example?

However, there is an argument for a common body of knowledge of costs and benefits on a sector-by-sector basis, for example. One of the reasons that the data set for breaches surveys, such as those carried out periodically by PWC or Verizon, is incomplete is the potential embarrassment factor. However, if there was a mechanism for a) anonymising and aggregating data by sector, and b) incentivizing the protection of that data,

then there would be the potential for a usefully focussed benchmark. For example, it would be possible for a government department to compile data on security breaches within government departments, since these must in any case be reported. In the commercial sector, for example, a Banker's Association would be a good example of a body which could provide a *one-way blind* process for producing relevant sector benchmarks. In the UK, for example, the British Banker's Association includes all organisations which have a banking license in the UK, whether they are British, or foreign banks operating in Britain.

Such a body of information would be very useful. IT would facilitate the production of information security business cases, as decisions could be based on *harder* data sets, helping to eliminate the problematic, subjective assertions around probabilities and monetisation of estimated impacts. This, in turn, would allow for better risk management practices, and leaner information security functions within organisations. It would allow more focussed and effective government spending. It would be a vital reference source for all sorts of individuals, organisations, and professional organisations. And this, my friends, is why it is unlikely to happen – perversely, it's too interesting.

In the UK context, the government, and public organisations are bound by the Freedom of Information Act. Similar legislation exists in a number of other countries. This type of legislation was designed to combat the Cold War model of governments gathering all manner of information about their citizens, for all manner of purposes. In other words, it was meant as a mechanism for protecting public freedom, by allowing the public to ask for whatever information a public body holds on a specific topic. Specific exclusions include those that might:

- Prejudice defence or the capability, effectiveness or security of any relevant forces
- Prejudice international relations
- Prejudice relations between any administration in the United Kingdom and any other such administration
- Prejudice the economic interests of the UK
- Prejudice law enforcement (e.g., prevention of crime or administration of justice, etc.)
- Prejudice the auditing functions of any public authorities
- In the reasonable opinion of a qualified person: prejudice the effective conduct of public affairs; prejudice collective responsibility; or inhibit the free and frank provision of advice or exchange of views
- Endanger physical or mental health, or endanger the safety of the individual (s.38)
- Prejudice commercial interests

In the UK, over 120,000 are made every year; a significant proportion of these are made by journalists, but most are made by the general public, on topics of all sorts. Requests can be rejected if they are deemed deliberately vexatious. However, all rejections of requests are subject to a *public interest* test – in other words, if an overwhelming case exists. Of course, separating press enquiries from *genuine* ones is almost impossible. For example, one concerned citizen asked Leicester City Council about their plans in the advent of a zombie attack; needless to say, she was dismayed to find that, in fact, no such preparations were in place. Similar requests have been made to other British cities, including Bristol and Dudley. Other requests have included all records and locations regarding paranormal activity. All of these, though generated by private individuals, were reported in the media.

All of this has far reaching implications. For a start, managing a scheme of this sort has substantial cost implications – all those requests need effort to respond to. Secondly, there is no guarantee that any information submitted to a public body will be immune from disclosure. After all, there are also legal and regulatory requirements for organisations to protect certain classes of information – for example, in a UK context, the Data Protection Act requires that all organisations (including business and government departments) which process personally identifiable data abide with eight basic principles, which include maintain the security of that data. Therefore, any body of information that shows where this did not happen would be of public interest. This would make a serious hackers job much easier; you could see not only where security was weak, but also potentially what those weaknesses where.

So, next time you find an organisation that is struggling to pull together a sensible business case for investing more in security, just remember whose responsible for the fundamental problems – not management themselves, but an evil coalition, headed by lawmakers. And zombie enthusiasts.

DRAKE

Drake has worked on information security and strategy with government agencies, the military, financial institutions and other blue chip organisations in Europe, the Middle East, and Africa since Boris Yeltsin was President.

[IS IT IN YOUR DNA?]

IM Geek PH: 877.UAT.GEEK

UAt+ 110%
FPS 24
Double

06



[GEEKED AT BIRTH]

LEARN:

Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering

Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Games and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies



You can talk the talk.
Can you walk the walk?

www.uat.edu > 877.UAT.GEEK

You've been using us for years.



World-Leading Security Consulting.



Email sales@mdsec.co.uk

Tweet [@MDSecLabs](https://twitter.com/MDSecLabs)

www.mdsec.co.uk