Sense of Security™
Security that enables business

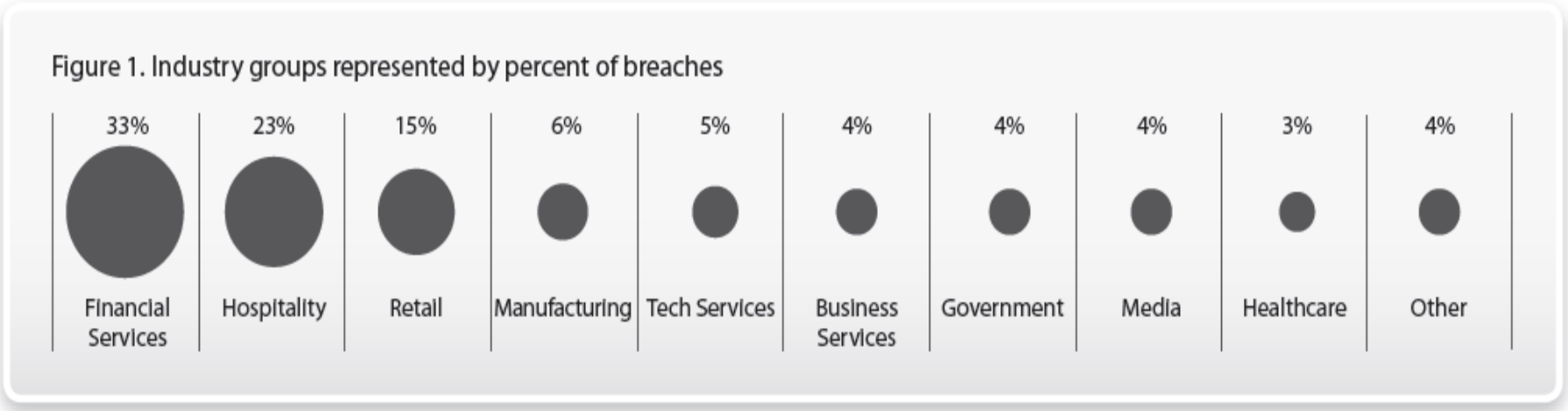
Information Security in the Information Age

Presenter: Neville Gollan

SOS - Information Security Professionals

Sense of Security
Security that enables business

The Current Landscape - Data Breach Cases

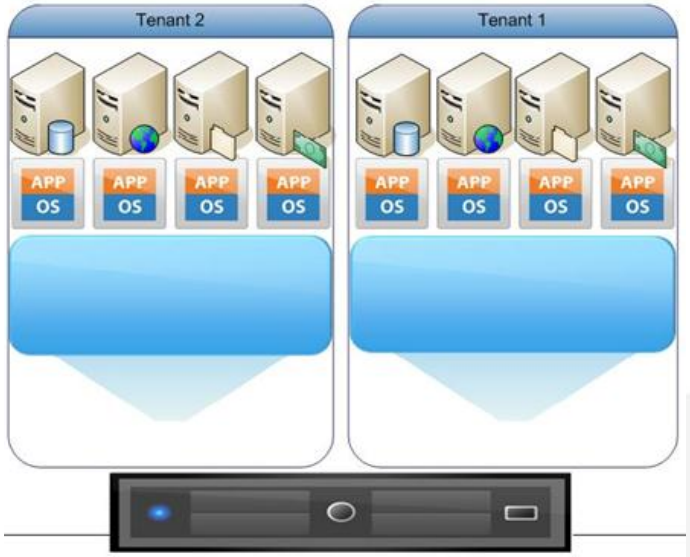


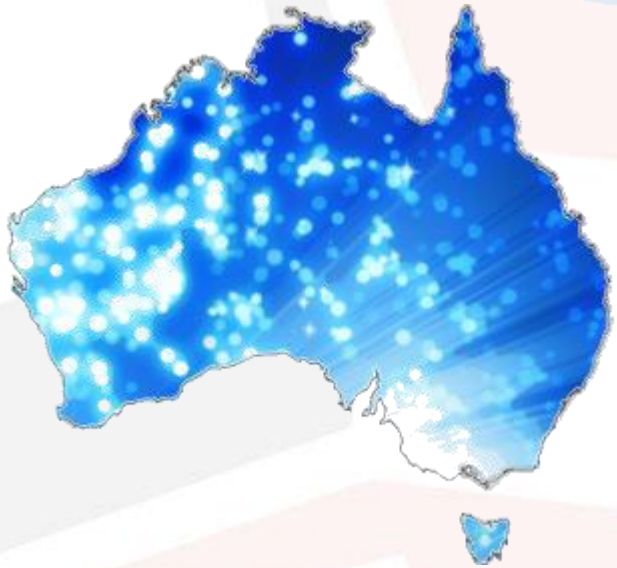
The Statistics

- An astounding 94% of all compromised records in 2009 were attributed to the Financial Services Industry
- Servers and apps account for 98% of total records compromised
- 96% of breaches were avoidable through the use of simple or intermediate controls

Source: Verizon 2010 Data Breach Investigations Report

The Information Age





Desired Business Outcomes

What happens if we get it wrong!

In Summary

- The threat of data breach remains high; particularly in the financial services industry
  - The introduction of simple and or intermediate security controls will help reduce the chance of security breach
- The use of technological advancements, and out-of-box thinking, will be critical to product marketing, customer retention and customer acquisition
  - But…….. make sure you use technology innovation wisely; it is your responsibility to protect the information assets under your charge
- Get help from the professionals; there are many reputable consulting firms available who specialise in IT security

Sense of Security™
Security that enables business

Sense of Security™
Security that enables business

Addressing the security challenges of two emerging technologies: Mobility and Online Applications

TSWG Innovators Forum

Coolum, Oct 2010

Agenda

- Intro to Web Applications
- Web Application Security Issues
- Intro to Mobility
- Corporate Response – Permit or Deny
- Mobility Security Issues
- Conclusion

Statistics

We are going to be talking a lot about current statistics

So I thought I would put this disclaimer in

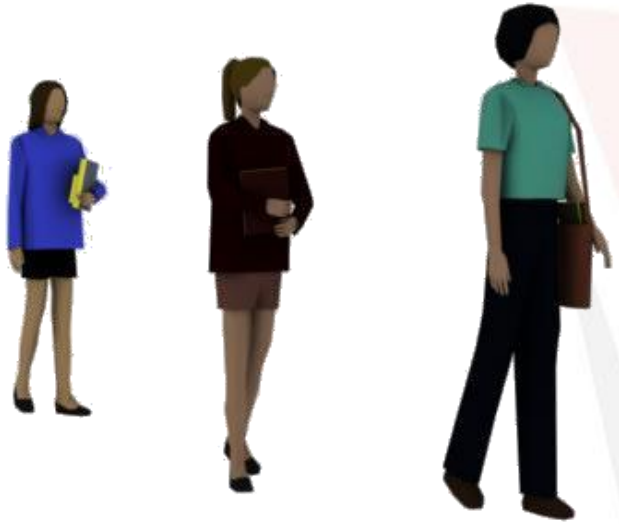
DISCLAIMER

“42.7 percent of all statistics are made up on the spot."
--The Hon. W. Richard Walton, Sr.

…. But I believe I am using credible sources and it is all referenced

People and Information

It's all about giving



access to

securely!

Sense of Security
Security that enables business

What is Web 2.0?

Online Web Applications (Web 2.0) refers to today's "second generation" of Web technologies

- Rich Internet Applications (RIA): Feature rich web sites; mimic thick client applications.
- Collaboration and Participation: Generating and sharing content in real time; wikis, extranets, blogs, social networking sites, online forums.
- Syndication: RSS or Atom feeds and mashups. Broadcasting of data.

Look familiar?

Social Networks

facebook

myspace a place for friends

bebo

hi5

Instant Messaging

meebo

RSS

Google Reader

Tagging

del.icio.us

digg

reddit

Personalised Home Pages

iGoogle

netvibes

MY YAHOO!

Windows Live

Pageflakes

Widgets

Windows

Google Desktop

YAHOO! WIDGETS

[Source: Worklight]

Sense of Security
Security that enables business

Widgets, Apps & Consumers

- 65% of internet users (615 million people) engaged with a widget
- Mac Dashboard has over 90 million users
- iGoogle experienced 267% Growth in 2 years
- Over 400 million Facebook users
- More than 550,000 active applications on Facebook
- Over 50 Million iPhone users
- 3 Billion iPhone app downloads

[Ref: "Worklight, Multi Channel Apps, May 2010]

Channels

[Ref: "Worklight, Multi Channel Apps, May 2010]

Business Drivers - Applications

Agenda

- Intro to Web Applications
- Web Application Security Issues
- Intro to Mobility
- Corporate Response – Permit or Deny
- Mobility Security Issues
- Conclusion

Responding to Market Demands

Vulnerabilities

- Over 6,600 new vulnerabilities introduced in 2009
- Web application vulnerabilities are still the biggest category of vulnerabilities (more than half since 2006, and 49% in 2009)

[Source: IBM X-Force® 2009 Trend and Risk Report: Annual Review of 2009]

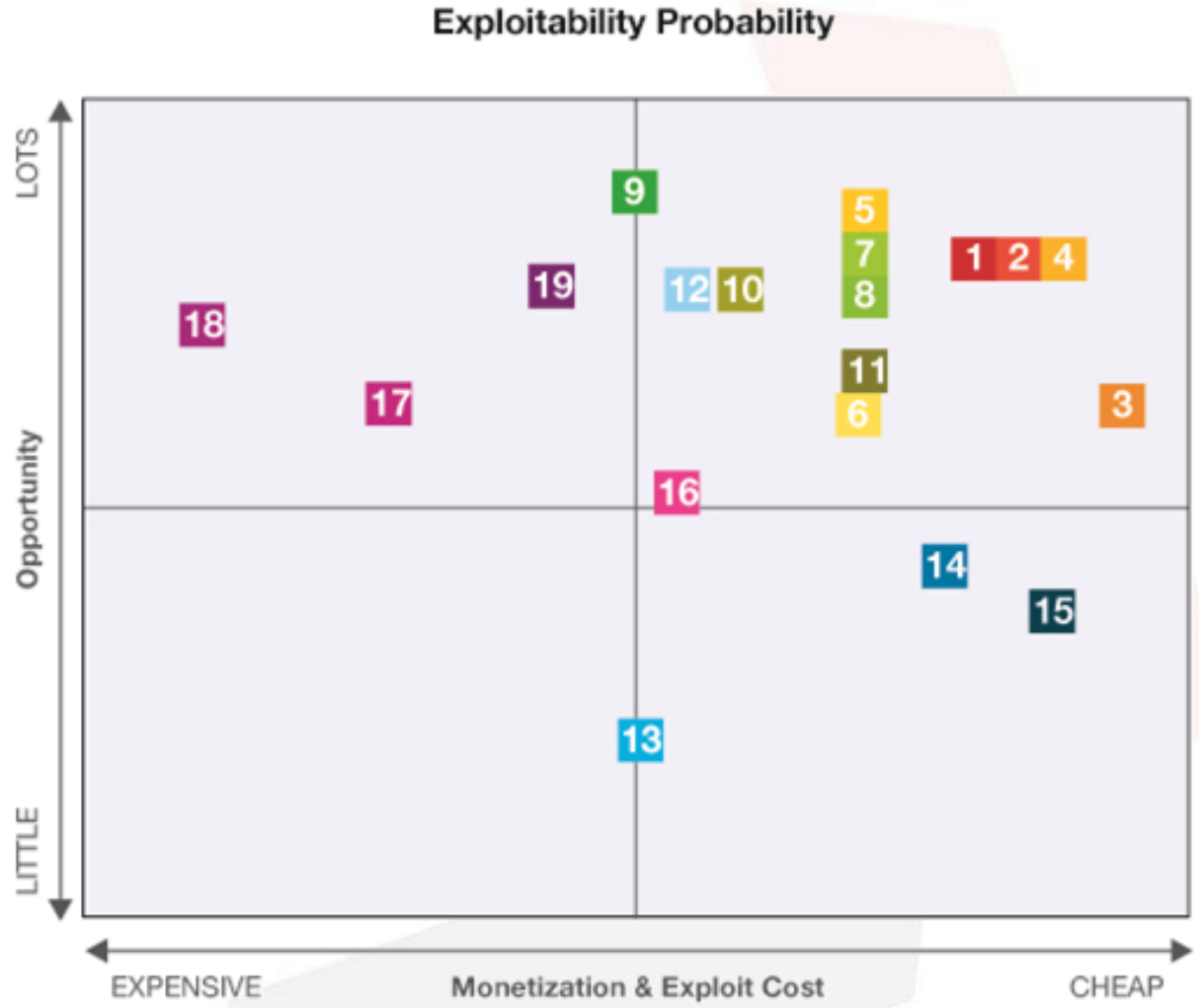
Web Application Security

- Web app vendors patch base platforms; but plug-ins remain vulnerable.
- Predominant Problems: Cross-Site Scripting (XSS), SQL Injection, and File Include vulnerabilities
- Client side threats focused on document format vulnerabilities (e.g. malicious PDF's)
- Obfuscation increasing (exploits hidden)
- Multimedia vulnerabilities increasing. Product footprint large; difficult to patch

[Source: IBM X-Force® 2009 Trend and Risk Report: Annual Review of 2009]

Sense of Security™
Security that enables business

High Yields



IBM **X-Force® 2009 Trend and Risk Report:** *Annual Review of 2009*

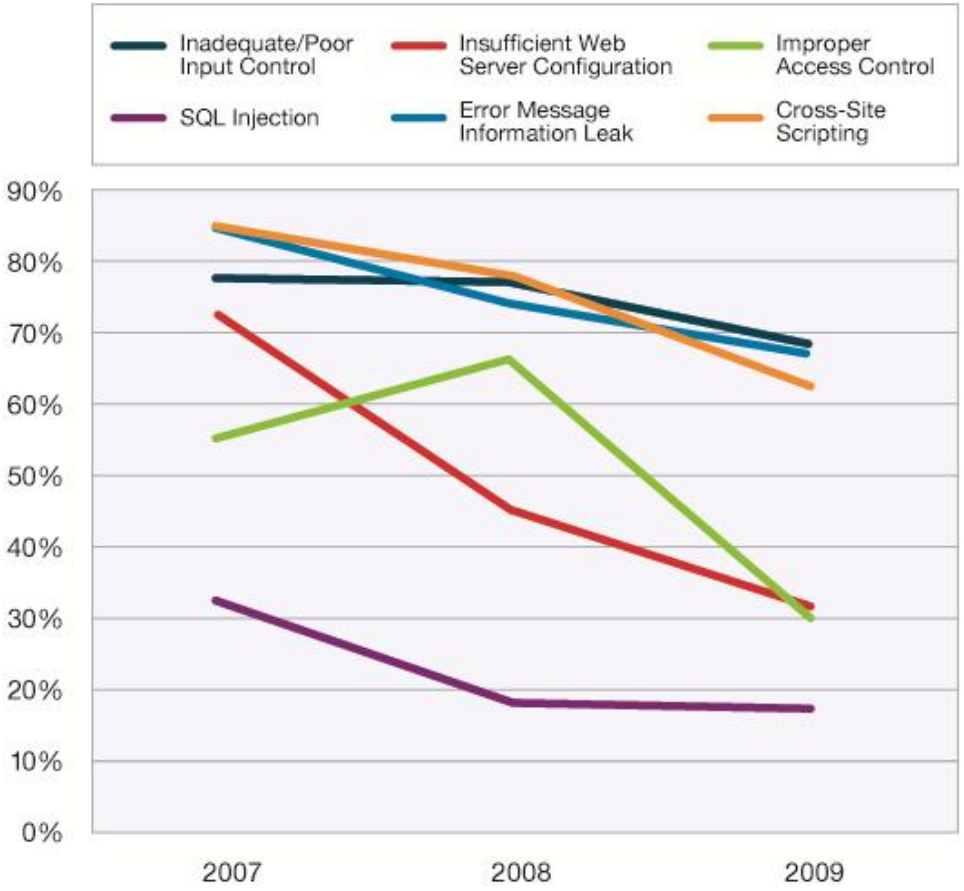
High Yields

1	December 15, 2009	Adobe Acrobat and Acrobat Reader Remote Code Execution
	October 9, 2009	Adobe Acrobat and Acrobat Reader Remote Code Execution
	July 22, 2009	Adobe Acrobat and Adobe Flash Remote Code Execution
2	November 23, 2009	Microsoft Internet Explorer mshtml.dll RCE
	July 6, 2009	Multiple Microsoft Video Control ActiveX Remote Code Execution Vulnerabilities
	July 20, 2009	Microsoft Office Web Components Spreadsheet ActiveX Control RCE
3	September 10, 2009	Microsoft Windows SRV2.SYS Remote Code Execution Vulnerability
4	July 16, 2009	Mozilla Firefox Font HTML Tags Remote Code Execution
5	July 14, 2009	Multiple Microsoft DirectShow Remote Code Execution Vulnerabili-
6	November 10, 2009	Microsoft Windows WSDAPI Remote Code Execution Vulnerability
7	October 13, 2009	Microsoft Windows Indexing Service ActiveX Control Remote Code Execution Vulnerability
	September 8, 2009	Microsoft Windows JScript Remote Code Execution Vulnerability
8	August 11, 2009	Network Security Services (NSS) Parser Remote Code Execution Vulnerability
9	August 11, 2009	Network Security Services (NSS) Certificate Security Bypass Vulnerability
10	October 13, 2009	Multiple Microsoft Windows GDI+ Image Remote Code Execution Vulnerabilities
	August 11, 2009	Microsoft Windows AVI Remote Code Execution Vulnerability
	November 10, 2009	Microsoft Windows Kernel Font Code Execution Vulnerability
	July 14, 2009	Multiple Microsoft Windows Embedded OpenType Font Engine Remote Code Execution Vulnerabilities
11	August 11, 2009	Microsoft WINS Replication Remote Code Execution Vulnerability
12	August 11, 2009	Microsoft Windows RDP Services Client ActiveX Control Remote Code Execution Vulnerability
	July 28, 2009	Microsoft Internet Explorer ATL Killbit Evasion Vulnerability
	July 28, 2009	Multiple Microsoft Visual Studio Active Template Remote Code Execution Vulnerabilities
13	November 9, 2009	Transport Layer Security (TLS) Handshake Renegotiation
14	August 11, 2009	ISC BIND dns_db_findrdataset() DoS Vulnerability
15	September 2, 2009	Microsoft Internet Information Services FTP Remote Code Execution Vulnerability
16	December 9, 2009	HP OpenView Network Node Manager Remote Code Execution Vulnerability
17	December 1, 2009	Novell eDirectory Remote Code Execution Vulnerability
18	July 14, 2009	ISC DHCP Client Buffer Overflow Vulnerability
19	October 13, 2009	Microsoft Internet Explorer Arguments Remote Code Execution Vulnerability

Source: IBM X-Force®

Sense of Security™
Security that enables business

Web Application Security Improvements
IBM Rational AppScan onDemand Premium Service
2007-2009



Source: IBM X-Force®

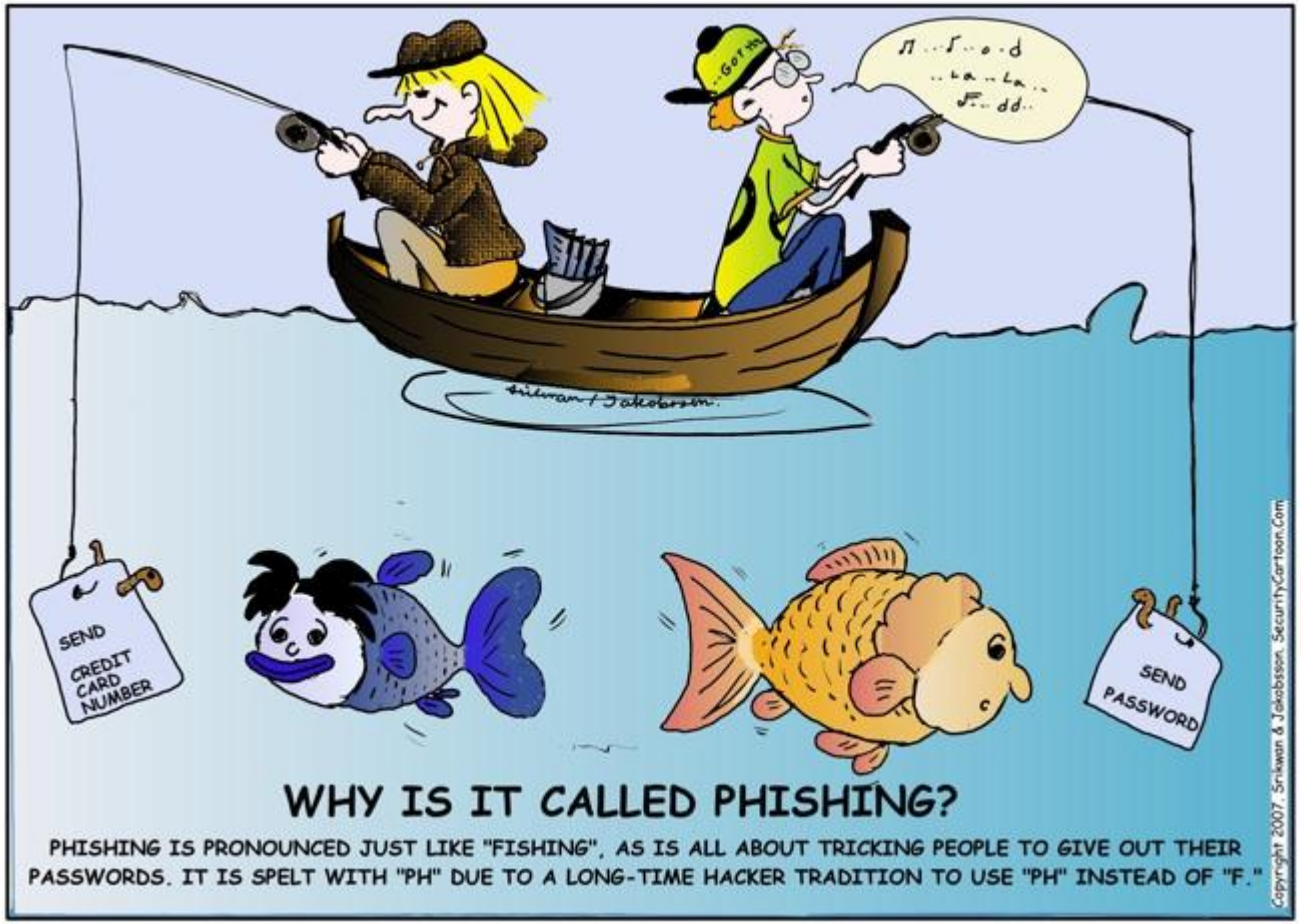
Vendors to the rescue?

Over half of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability

Financial Services		
Category	**Avg # Vulns**	**% Likely to Occur**
Improper Use of SSL	61.5	84%
Improper Access Control	3.2	76%
Error Message Information Leak	36.2	71%
Inadequate / Poor Input Control	12.0	61%
Cross-Site Scripting	11.3	58%
Information Disclosure	2.0	55%
Improper Application Deployment	2.6	50%

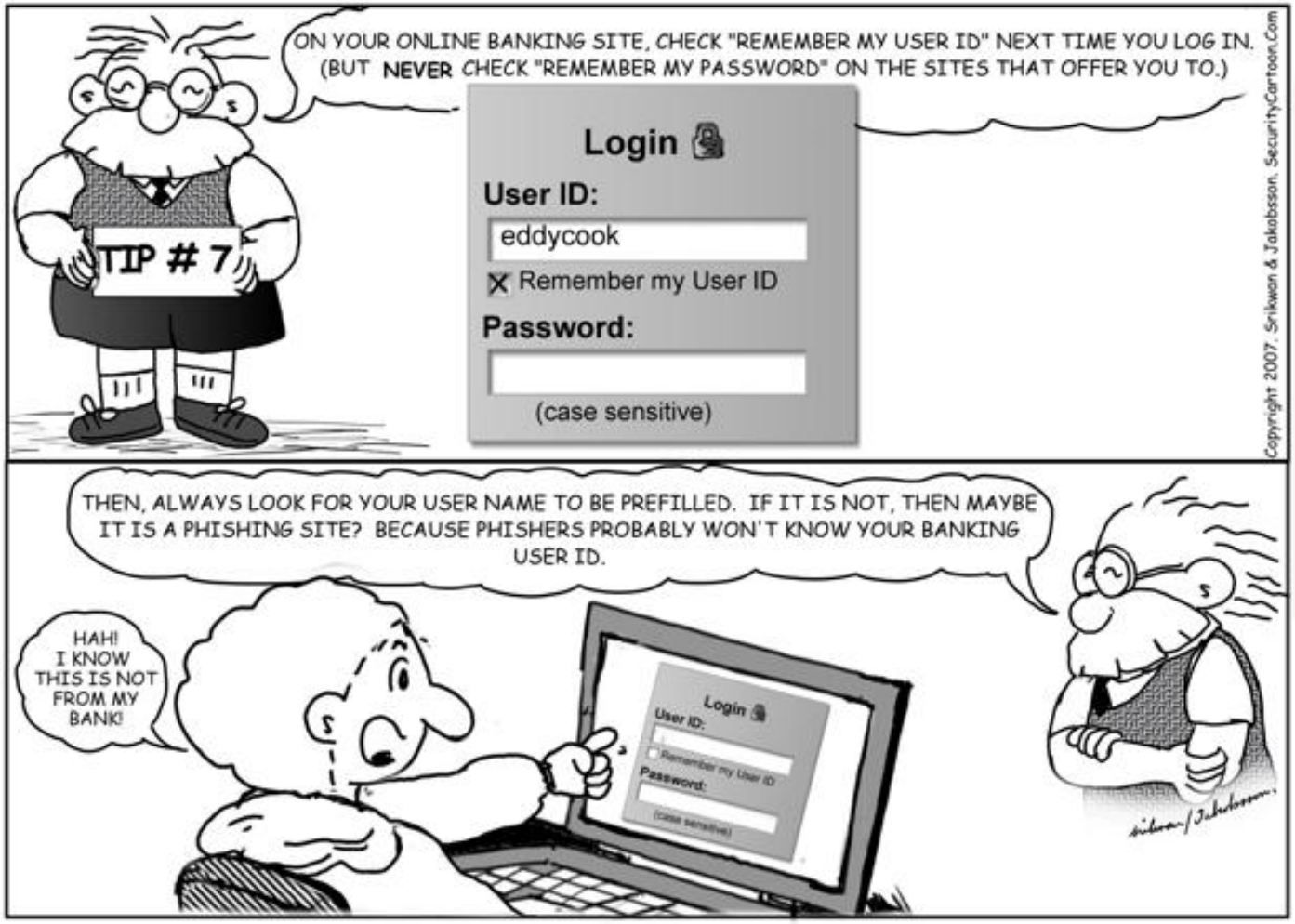
IBM **X-Force® 2009 Trend and Risk Report:** *Annual Review of 2009*

Credentials are gold



"Reproduced with permission. Please visit www.SecurityCartoon.com for more material."

“Remember Me” functionality



Impact: Increases the possibility of cross-site scripting & similar session hijacking attacks

"Reproduced with permission. Please visit www.SecurityCartoon.com for more material."

Password Security $%^@!@#$@#$

- Many applications limit password length and complexity!
- So even if users try to adopt good password measures they can't.
- This forces the user to be insecure.

SSL

- Why do so many sites not enforce SSL Logon?
- Even if SSL Logon is enforced – may still succumb to threats.
  - Ref SSLStrip tool. Redirects through ARP Spoof and creates a MITM attack.
- Always check server certificate.

Key steps to web application security

If Developing

- Develop Securely. Use Secure Coding Guidelines. Ref OWASP
- Run Vulnerability Management Lifecycle Program. Complement with frequent penetration tests.

If using 3rd party

- Review security measures in place.
- Understand how your information is secured.
- Review and understand T&C's of the service.

Firewalling

- Use Web Application Firewalls and Application/Protocol firewalls.
- Traditional network firewalls offer no protection.

Engage with experts

- Understand threat landscape.
- Perform technical and business aligned security reviews

Agenda

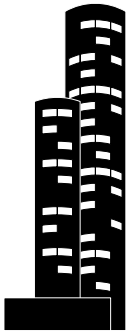
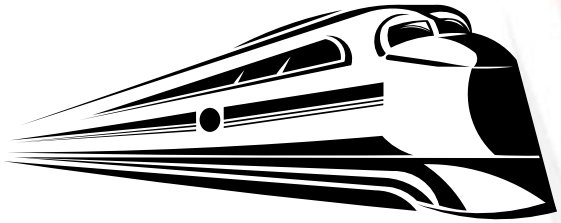
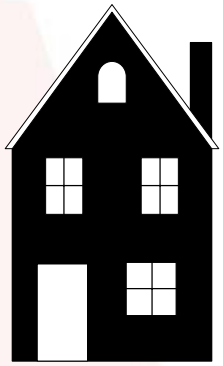
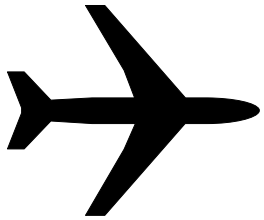
- Intro to Web Applications
- Web Application Security Issues
- Intro to Mobility
- Corporate Response – Permit or Deny
- Mobility Security Issues
- Conclusion

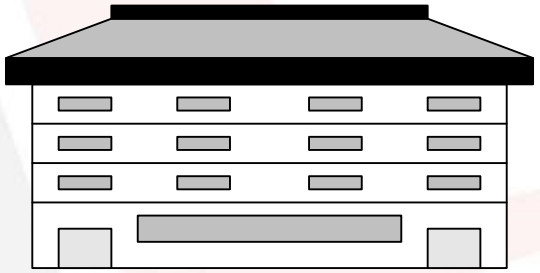
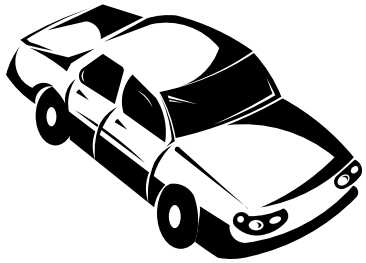
Corporate Drivers - Mobility

Business needs for mobility and online applications

- Corporate:
  - Reduce operational costs- compelling ROI
  - Efficient access to information from remote locations
  - Provide practical and reliable access to shared information regardless of geographical location and/or time zone
  - A desire to leverage contacts and content in more effective ways
  - Flexible work location options help retain skilled staff
  - Increase productivity levels in competitive markets

Access required from everywhere


Sense of Security
Security that enables business

Mobility, Availability, Storage

Sense of Security
Security that enables business

Instantaneous gratification

"**96%** of the time people have their cell phones within 1 meter of them"

[Ref Tony Saigh, business development manager for mobile at Skype
http://www.cnet.com.au/skype-s-mobile-dreams-339285053.htm]

Agenda

- Intro to Web Applications
- Web Application Security Issues
- Intro to Mobility
- Corporate Response – Permit or Deny
- Mobility Security Issues
- Conclusion

The corporate response

The usual (corporate) response is a mixture between

… and complete

Being too restrictive?

Usually when access to information is completely restricted, with the intention of protecting the information, you don't derive the benefit from the available technology and improved methods.

and this happens

People find way around it anyway

- Industry estimates state that **60%** of corporate data resides on unprotected PCs and laptops, **10%** of laptops are lost or stolen in the first year of purchase, and **66%** of USB devices are lost or misplaced in their lifetimes

  [Ref: Google, 2009. www.google.com/apps/intl/en/business/switch_benefits.html]

- Only **41%** of companies are encrypting their laptops, with **17%** planning to do so next year

  [Ref: "Ernst & Young, 12th annual global information security survey, Aug09]

Implications Can Be Significant

- Data breached diminish customer confidence and trust, leading to abnormally high customer turnover (churn) that directly drives data breach costs

  [Ponemon, 2009 Annual Study: Australia Cost of Data Breach]

- Malicious attacks and botnets are the primary drivers of data breaches (44%) and cost substantially more ($156) than those caused by human negligence ($94) or IT system glitches ($99)

  [Ponemon, 2009 Annual Study: Australia Cost of Data Breach]

Agenda

- Intro to Web Applications
- Web Application Security Issues
- Intro to Mobility
- Corporate Response – Permit or Deny
- Mobility Security Issues
- Conclusion

iPhone Encryption

iPhone encryption proven to be 'useless'

Asher Moses
July 27, 2009

A hacker has demonstrated how it is possible to crack the encryption on the iPhone 3GS within two minutes using free software, allowing access to all of the data on the device - even photos and emails that have long been deleted.

The iPhone 3GS is the first iPhone model to include built-in encryption technology, which Apple believes allows it to rival the BlackBerry for business users.

The company claims hundreds of thousands of the devices are being used by companies and government organisations around the world.

http://www.smh.com.au/digital-life/mobiles/iphone-encryption-proven-to-be-useless-20090727-dyfv.html

iPhone Encryption

26 May 2010, 15:40

« previous | next »

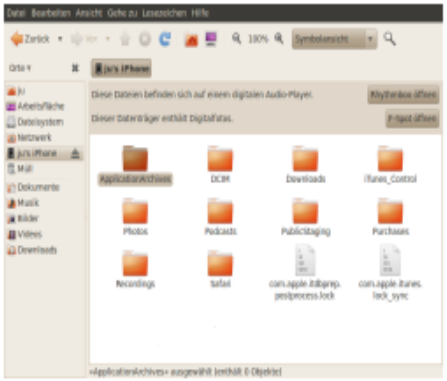
Vulnerability in iPhone data encryption

A lost iPhone is a bigger problem than previously thought. Despite encryption the finder can gain easy access to data including photos and audio recordings, even if the owner has set up their iPhone to require a pass code. And, of all things, this is made possible with Linux – the very operating system which Apple regularly cold-shoulders.

How it should be - the locked iPhone refuses the connection from a Mac.

According to Apple, all data on the iPhone 3GS is hardware-encrypted using 256-bit AES, which cannot be disabled by the user. Access to data on the iPhone is normally restricted to computers with which the iPhone has previously been connected and to which the requisite credentials have previously been transferred. This exchange of credentials is blocked when the iPhone is locked, so that connecting a locked iPhone to an unfamiliar computer will not allow the latter access to data on the iPhone.

However, Bernd Marienfeldt, security officer at UK internet node LINX, found that he was able to gain unfettered access to his iPhone 3GS from Ubuntu 10.04. If he connected the device whilst it was turned off and then turned it on, Ubuntu auto-mounted the file system and was able to access several folders despite never having previously been connected to the iPhone. The H's associates at heise Security have successfully reproduced the problem. An Ubuntu system which had never before communicated with the iPhone immediately displayed a range of folders. Their contents included the unencrypted images, MP3s and audio recordings stored on the device.



The Ubuntu system mounts the iPhone and allows access to the data.

Marienfeldt has informed Apple of the problem, which the company is now investigating. It thinks the problem is caused by a race condition, as the problem only occurs when the iPhone is turned on whilst connected to the USB bus. It is not yet clear whether an update to fix the vulnerability will be released – in response to an enquiry from heise Security, Apple stated that it does not provide information on ongoing investigations.

http://www.h-online.com/security/news/item/Vulnerability-in-iPhone-data-encryption-1008185.html

iPhone OS Vulnerability

The Register®

Hardware Software Music & Media Networks Security Public Sector Business Science Odds

Crime Malware Enterprise Security Spam ID

Print Post comment Retweet Facebook Alert

Apple kills browse-and-get-hacked bugs in iOS

iPhones, iPads, iPod touches safe again

By **Dan Goodin in San Francisco • Get more from this author**

Posted in Malware, 11th August 2010 20:57 GMT

Updated Apple has patched a critical iOS vulnerability that allows attackers to install malicious apps on iPhones, iPads, and iPod touches by doing nothing more than luring victims to a booby-trapped website or sending them a tainted email.

The update plugs a hole in Apple-designed document-viewing software that allows attackers to inject code of their choosing into PDF files. By default, all three devices open the documents automatically when they are encountered in emails or on websites, leading to a classic browse-and-get-hacked exploit. The Foxit document reader was vulnerable to the same flaw, until it was patched last week. Adobe has said its Reader application is unaffected.

A second vulnerability in iOS allows attackers to break out of the iOS security sandbox and access to the OS's root account, which has unfettered access to the device.

The vulnerabilities have been exploited for weeks on Jailbreakme.com, a website that allows people to jailbreak their devices by flicking a slider on the home page. There has been nothing stopping people from carrying out more malicious attacks, but so far there are no known reports of that happening.

In addition to patching the PDF flaw in iOS, Apple has also bolstered its sandbox by nixing an integer overflow in the handling of what's known as IOSurface properties. The whole point of the design is to mitigate the severity of buffer overflows and other garden-variety software bugs by containing application processes inside protected walls that can't access sensitive parts of the OS.

There's no word of an accompanying update for Mac OS X. It remains unclear if that OS is unaffected or Apple hasn't gotten around to issuing a fix yet.

Apple's advisory suggests that users install the patch immediately, but it may make sense to wait until there's an ample amount of bandwidth available. The iPad update is a whopping 456.9MB in size and the iPhone download is 378MB. ®

Sense of Security™
Security that enables business

Android Trojan

Kaspersky warns of first Android trojan

By Kevin McLaughlin
Aug 12, 2010 2:46 PM
Tags: kasperksy | android | trojansmsandroidosfakeplayera

Trojan disguises itself in a 13-KB application called Movie Player.

Kaspersky Lab says it has identified the first SMS Trojan that specifically targets Android smartphones, although the application it piggybacks on isn't listed on the Android Market and appears to only be affecting users in Russia.

The malware, which Kaspersky has named Trojan-SMS.AndroidOS.FakePlayer.a, has already found its way onto "a number of mobile devices", Kaspersky said in a blog post earlier this week.

The Trojan disguises itself in a 13-KB application called Movie Player, which is available through a malicious Website and has the standard Android extension .APK. Once installed on the device, the Trojan begins sending SMS messages to premium rate numbers without the owner's knowledge, in some cases racking up fees of several dollars per message.

http://www.crn.com.au/News/224414,kaspersky-warns-of-first-android-trojan.aspx

And why does it happen? Mobility

Adoption of mobility solutions requires enterprise security to be extended BEYOND the enterprise perimeter.

- There is no corporate policy
- The backdoor is left open with USB keys.
- The side entrance door is left open with the wireless network.
- Information is published (read LEAKED) to blogs/collaboration/info sharing sites.
- Laptops, removable media, mobile phones store vast amounts of sensitive data and are still seldom encrypted.
- Data in transit is seldom encrypted.
- Poor (if any) authentication to corporate data for mobile users.

5 Steps to Mobility Security

Policy

- Create a policy that covers the device lifecycle, from selection to recovery.

Data In Motion

- Encrypt all data over mobile and WiFi networks. Use VPN clients or application layer encryption.

Data at Rest

- Encrypt data stored on device. Manage cached data with 3rd party software and passwords.

Malware Protection

- Protect against malware with policy (Bluetooth, downloads) and technology (anti-malware SW).

Authentication

- Require user authentication at points required for acceptable risk/aggravation.

[Ref: Opus1, Five Steps To Securing Mobile Devices, 2008]

Sense of Security™
Security that enables business

Agenda

- Intro to Web Applications
- Web Application Security Issues
- Intro to Mobility
- Corporate Response – Permit or Deny
- Mobility Security Issues
- Conclusion

Fundamentals

"The real best practices have been the same since the 1970s: know where your data is, who has access to what, read your logs, guard your perimeter, minimize complexity, reduce access to "need only" and segment your networks. Those are the practices and techniques that result in real security. There are loads of fads vying for people's attention, but when they come and go, the fundamentals will remain the same."

Marcus Ranum

Summary

- Online web applications are both a set of technologies as well as a new set of consumer behaviours.
- The interactive internet is growing daily and here to stay; Cloud Computing and Application Delivery revolution.
- Those who do not adopt these emerging technologies will eventually be left behind.
- Attacks against web applications are prevalent. Protect yourself against all attack vectors. Review web applications frequently.
- Data Loss will continue to plague organisations. Know where and what your data is and encrypt it in motion and at rest.
- Effective mobility solutions are required to deliver cross platform, multi vector access to web applications.
- You can find the balance between  and 

Sense of Security
Security that enables business

Thank You

Thank You

Murray Goldschmidt – COO

Sense of Security Pty Ltd

Tel: +61 2 9290 4444

info@senseofsecurity.com.au

www.senseofsecurity.com.au