Pwnning The User
Will you be the next victim?

Month XX, 2016
Agenda

- Introduction
- Brief History on Hacking
- Why is InfoSec Important?
- Identity Theft
- The Most Common Attacks Leveraged Against End Users
  - Social Engineering
  - Trojan Horses
  - Drive-by-Downloads
  - Mobile Device/Wireless
  - Web Application Security
Andrew Weidenhamer, OSCP, CISSP, CISA, CIPP, QSA, PA-QSA
Security and Privacy Director with RSM
- National Security Testing Lead, Security and Privacy Consulting
- Ethical hacking, Risk Assessments, Regulatory Compliance
- Over 10 years of Information Security Consulting experience
- andrew.weidenhamer@mcgladrey.com
1903 – Wireless Telegraph

- Inventor and Magician, Nevil Maskelyne, hacked the Wireless Telegraph
- Intercepted communication and changed the message to “There was a young fellow of Italy, who diddled the public quite prettily”
Axis governments used cipher machines called Enigma to encrypt morse code.

Marian Rejewski succeeded in cracking the axis ciphers using the theory of permutation and groups.

\[ C(n,r) = \frac{n!}{r! (n-r)!} \]

\[ P(n,r) = \frac{n!}{(n-r)!} \]

- **n** = set size: the total number of items in the sample
- **r** = subset size: the number of items to be selected from the sample
1972 – Phone Phreaking

- John Draper aka. Cap’n Crunch, discovered that certain pitches could be used to make free long distance calls
- Used whistle found in box of Captain Crunch
1980’s

- 1981 - Dawn of Computer Clubs
  – Chaos Computer Club forms in Germany
  – The Warelords forms in USA

- 1982 – The 414s break into 60 computer systems from the Los Alamos Laboratories to Manhattan’s Memorial Sloan-Kettering Cancer Center
  – Newsweek story – Beware: Hackers at Play
  – First mass-media use of the term hacker
1980’s – cont’d

- 1983 – 1988 - Ushered the era of Malware
  - 1983 - First virus named “Brain” was developed
  - 1983 - The movie “WarGames” is released
  - 1986 - Congress passes the Computer Fraud and Abuse Act
  - 1986 – Computer hacker, Kevin Poulsen was featured on America’s Most Wanted. Arrested in 1991
  - 1988 - Morris Worm infects 6000 networked computers
1990’s – Dawn of the Modern Day IS Industry

- 1992 – Dark Avenger writes polymorphic code used to circumvent Anti-virus software
- 1993 – DEFCON hacking conference introduced
- 1994 – AOHELL is released
- 1995 – The movies The Net and Hackers are released
- 1996 – The MP3 format gains popularity. Hackers set up sharing sites
1990’s – cont’d

- 1997 – First high-profile attacks on Windows Operating System
- 1998 – 7 members of the hacker think tank testify in front of congress on “Weak Computer Security in Government”
- 1999 – Software security goes mainstream in the wake of Microsoft’s Windows 98 release
2000’s – Dawn of Major Criminal Enterprises

- 2000 – 2002
  - Microsoft Windows becomes widely attacked
  - ILOVEYOU worm becomes one of the most damaging worms ever
- 2003 – Hacker group “Anonymous” was formed
- 2004 – North Korea claims to have trained 500 hackers to successfully crack South Korean, Japanese, and their allies’ computer systems
2006 – Turkish hacker successfully hacked 21,549 websites in one shot
2008 – Chinese hackers claim to have gained access to the world’s most sensitive sites including The Pentagon
2008 and beyond.....

Lots and Lots of other Hacking Events Occurred
Why is InfoSec Important?
Common Sense

- How else would we protect the confidentiality, integrity, and availability of our data?
- How else would we protect against identity theft?
- How else would we protect our critical infrastructure (power grid, water resources, etc)?
- How would we respond adequately to an incident
- Etc
- Etc
- Etc
Breach Statistics

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>37%</td>
<td>of breaches affected financial organizations</td>
<td>(+)</td>
</tr>
<tr>
<td>24%</td>
<td>of breaches occurred in retail environments and restaurants</td>
<td>(-)</td>
</tr>
<tr>
<td>20%</td>
<td>of network intrusions involved manufacturing, transportation, and utilities</td>
<td>(+)</td>
</tr>
<tr>
<td>20%</td>
<td>of network intrusions hit information and professional services firms</td>
<td>(+)</td>
</tr>
<tr>
<td>38%</td>
<td>of breaches impacted larger organizations</td>
<td>(+)</td>
</tr>
</tbody>
</table>

Victims in this report span restaurants, retailers, media companies, banks, utilities, engineering firms, multinational corporations, security providers, defense contractors, government agencies, and more across the globe. A definite relationship exists between industry and attack motive, which is most likely a byproduct of the data targeted (e.g., stealing payment cards from retailers and intellectual property [IP] from manufacturers).

The ratio among organizational sizes is fairly even this time around, rather than tipping toward the small end of the scale as it did in our last report.

27 different countries are represented.

Credit: 2013 Verizon Data Breach Report
Ponemon – 2015 Cost of a Data Breach Study

![Pie chart showing percentages of data breaches caused by different types of events.]

- 47% Malicious or criminal attack
- 29% System glitch
- 25% Human error

**Figure 5. Per capita cost for three root causes of the data breach**

Consolidated view (n=350), measured in US$

- Malicious or criminal attack: $170
- System glitch: $142
- Human error: $137
Figure 12: Variety of external actor

Credit: Verizon Data Breach Report
Figure 13: Origin of external actors: Top 10

- China: 30%
- Romania: 28%
- United States: 18%
- Bulgaria: 7%
- Russia: 5%
- Netherlands: 1%
- Armenia: 1%
- Germany: 1%
- Colombia: 1%
- Brazil: 1%

Credit: Verizon Data Breach Report
<table>
<thead>
<tr>
<th>VICTIM INDUSTRY</th>
<th>ORGANIZED CRIME</th>
<th>STATE-AFFILIATED</th>
<th>ACTIVISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Manufacturing</td>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>Professional</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Food</td>
<td>Transportation</td>
<td>Other Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REGION OF OPERATION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>East Asia (China)</td>
<td>Western Europe</td>
<td></td>
</tr>
<tr>
<td>North America</td>
<td>North America</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMMON ACTIONS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tampering (Physical)</td>
<td></td>
<td>Backdoor (Malware)</td>
<td>SQLi (Hacking)</td>
</tr>
<tr>
<td>Brute force (Hacking)</td>
<td></td>
<td>Phishing (Social)</td>
<td>Stolen creds (Hacking)</td>
</tr>
<tr>
<td>Spyware (Malware)</td>
<td></td>
<td>Command/Control (C2) (Malware, Hacking)</td>
<td>Brute force (Hacking)</td>
</tr>
<tr>
<td>Capture stored data (Malware)</td>
<td></td>
<td>Export data (Malware)</td>
<td>RFI (Hacking)</td>
</tr>
<tr>
<td>Adminware (Malware)</td>
<td></td>
<td>Password dumper (Malware)</td>
<td>Backdoor (Malware)</td>
</tr>
<tr>
<td>RAM Scraper (Malware)</td>
<td></td>
<td>Downloader (Malware)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stolen creds (Hacking)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TARGETED ASSETS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Laptop/desktop</td>
<td>Web application</td>
<td></td>
</tr>
<tr>
<td>POS controller</td>
<td>File server</td>
<td>Database</td>
<td></td>
</tr>
<tr>
<td>POS terminal</td>
<td>Mail server</td>
<td>Mail server</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Directory server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DESIRED DATA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment cards</td>
<td>Credentials</td>
<td>Personal info</td>
<td></td>
</tr>
<tr>
<td>Credentials</td>
<td>Internal organization data</td>
<td>Credentials</td>
<td></td>
</tr>
<tr>
<td>Bank account info</td>
<td></td>
<td>Internal organization data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trade secrets</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System info</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identity Theft
What is Identity Theft

- Financial Identity Theft occurs when SSN’s and other personally identifying information (PII) is used to establish new lines of credit.
- Most credit reporting agencies do not verify age of the applicant on the credit application.
- Criminal Identity Theft occurs when a person steals information to get a driver’s license or uses the another’s identity when caught in a criminal act.
Identity Theft Statistics

- 17.6 million people experienced identity theft in 2014
- Most common type of identity theft was the unauthorized misuse or attempted misuse of an existing account (16.4 million people)
- 8.6 million people experienced the fraudulent use of credit cards
- Most victims only discovered the incident when contacted by a financial institution (45%); 18% notice fraudulent transactions
- 14% of victims experienced a loss greater than $1000

Credit:
http://www.bjs.gov/content/pub/press/vit14pr.cfm
**TABLE 2**
Persons age 16 or older who experienced at least one identity theft incident in the past 12 months, by victim characteristics, 2012 and 2014

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Number of victims 2012</th>
<th>Number of victims 2014*</th>
<th>Percent of all persons 2012</th>
<th>Percent of all persons 2014*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>16,580,500</td>
<td>17,576,205</td>
<td>6.7%</td>
<td>7.0%</td>
</tr>
<tr>
<td><strong>Sex</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>7,902,800</td>
<td>8,332,900</td>
<td>6.6%</td>
<td>6.9%</td>
</tr>
<tr>
<td>Female</td>
<td>8,677,700</td>
<td>9,243,300</td>
<td>6.9%</td>
<td>7.2%</td>
</tr>
<tr>
<td><strong>Race/Hispanic origin</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whitea</td>
<td>12,417,600</td>
<td>13,264,100</td>
<td>7.3% ‡</td>
<td>8.0%</td>
</tr>
<tr>
<td>Black/African Americana</td>
<td>1,494,100</td>
<td>1,407,700</td>
<td>5.0</td>
<td>4.7</td>
</tr>
<tr>
<td>Hispanic/Latino</td>
<td>1,544,100</td>
<td>1,789,800</td>
<td>5.2</td>
<td>4.9</td>
</tr>
<tr>
<td>Othera,b</td>
<td>841,400</td>
<td>861,100</td>
<td>6.4</td>
<td>6.1</td>
</tr>
<tr>
<td>Two or more racesa</td>
<td>270,700</td>
<td>253,400</td>
<td>9.0</td>
<td>9.0</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16–17</td>
<td>35,200</td>
<td>38,600</td>
<td>0.4% †</td>
<td>0.5% †</td>
</tr>
<tr>
<td>18–24</td>
<td>1,466,400</td>
<td>1,300,800</td>
<td>4.8</td>
<td>4.3</td>
</tr>
<tr>
<td>25–34</td>
<td>3,293,500</td>
<td>3,566,400</td>
<td>7.8</td>
<td>8.3</td>
</tr>
<tr>
<td>35–49</td>
<td>4,914,800</td>
<td>5,012,300</td>
<td>8.0</td>
<td>8.2</td>
</tr>
<tr>
<td>50–64</td>
<td>4,739,400</td>
<td>5,061,100</td>
<td>7.8</td>
<td>8.1</td>
</tr>
<tr>
<td>65 or older</td>
<td>2,131,100†</td>
<td>2,596,900</td>
<td>5.0</td>
<td>5.8</td>
</tr>
<tr>
<td><strong>Household income</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$24,999 or less</td>
<td>1,888,000</td>
<td>1,838,600</td>
<td>4.9%</td>
<td>4.9%</td>
</tr>
<tr>
<td>$25,000–$49,999</td>
<td>2,809,100</td>
<td>3,010,900</td>
<td>5.4</td>
<td>5.9</td>
</tr>
<tr>
<td>$50,000–$74,999</td>
<td>2,598,500</td>
<td>2,493,700</td>
<td>7.7</td>
<td>7.6</td>
</tr>
<tr>
<td>$75,000 or more</td>
<td>6,274,800</td>
<td>6,758,000</td>
<td>10.0</td>
<td>10.7</td>
</tr>
<tr>
<td>Unknown</td>
<td>3,010,100‡</td>
<td>3,474,900</td>
<td>5.1</td>
<td>5.4</td>
</tr>
</tbody>
</table>

How does it Occur

- Stealing your wallet and purse
- Stealing your mail
- Shoulder surfing
- Going through your garbage
- Breaching an organization that has your data
- Social Engineering tactics
  - Calling you
  - Clicking on links
- Skimming devices in ATM’s and Pay-at-the-Pump devices
My new credit card came in yay! And the security code is just like my birthday 527 RichBitch pic.twitter.com/d5lWoNZ9OP
55% of teens have given out personal info to someone they don’t know
29% of teens have posted mean info, embarrassing photos, or spread rumors about someone
29% of teens have been stalked or contacted by a stranger or someone they don’t know
24% have had a private or embarrassing info made public without their permission
Child Identity Theft - Warning Signs

- When attempting to open a savings account or college fund for the child. In this scenario, an unoffending parent discovers that there is already an account with that SSN or that the new account is denied due to a bad check record.
- When numerous credit cards, checks, pre-approved credit card offers, bills or bank statements are received in the name of the child.
- When collection agencies call or send letters about accounts not opened by the child.
When a teen is denied the right to get a driver’s license because another person has a license with that SSN as ID. The imposter may even have accumulated tickets or citations in the child’s name.

When law enforcement comes to the door with a warrant for an arrest of the child.
Adult IT – Warning Signs

- Are denied credit, mortgage or loan for a vehicle or college tuition
- Are unable to open a bank or checking account
- Receive collection notices in the mail or by telephone
- Are denied tenancy, utility or phone service
- Are denied driver’s license renewal
- Are discharged from a job or continually and unexplainably denied employment
- Have been receiving bills or credit cards they never requested, perhaps for years
- Are arrested for an activity they never committed
- Are denied SSI or welfare services
Recommendations

- Protect your personal belongings
- Always use your Credit Card as opposed to Debit Card
- Uniball 207 pens to write checks
- Observe people around you to avoid shoulder surfing
- Always question why someone needs your personal information
- Identity Theft protection
The Most Common Attacks Leveraged Against End Users
Social Engineering
What is Social Engineering

- A deliberate attempt by a hacker to get you to perform an action you otherwise may not do
- Plays on the innate nature of human beings to typically want to be non-confrontational and nice
- Exploits human’s curiosity
Organizational Issues

- Only 54% of organizations have privacy or data protection awareness programs\(^1\)
- 63% of employees have used personal email to send sensitive work documents
- 45% of employees have used sites like Dropbox and Box.net to share sensitive information
- 1 and 5 employees are tricked by phishing emails.
The attack vector of choice for many advanced attackers

- Typical countermeasures such as firewalls, anti-virus, and intrusion detection systems are almost worthless

- Pharming
  - Large scale, unfocused attacks directing users to malicious websites

- Phishing
  - Attempts to acquire information via fake emails, texts, and web pages

- Spear Phishing
  - Small scale, focused attacks against a limited audience

- Whaling
  - Ultra focused attacks against a high-profile targets
Types of Social Engineering Techniques

- Calling and pretending to be someone I’m not
- Emailing you to try to get you to click on a link or install a program
- Trying to tailgate into a building that I do not have access to
- Dropping malicious flash drives around your home or facility to see who is foolish enough to plug them into their computer
Trends

- 197,252 unique phishing email reports were seen in the 4\textsuperscript{th} quarter of 2014\textsuperscript{3}
  - 18\% increase from Q3
- 47,094 unique phishing websites detected
- The United States continues to be the top country hosting phishing sites\textsuperscript{3}
  - Germany, Russia, and China are also major players
- Payment and financial services are the largest targeted industries\textsuperscript{3}
Email based Social Engineering – Old School

Earthquake and tsunami breed web scams, malware
Dan Kaplan March 11, 2011

The 8.9-magnitude earthquake and deadly tsunami in Japan also has triggered a tidal wave of cybercrime, say experts.

From: Internal Revenue Service [mailto:notice@irs.gov]
Sent: Thursday, May 23, 2008 11:40 PM
To: [redacted]
Subject: Notice of Deficiency #23-79913-263326-344

Dear [redacted],

We have determined that you owe additional tax and other amounts, or both, for the tax year(s) identified above. This letter is your NOTICE OF DEFICIENCY, as required by law. The enclosed statement shows how we figured the deficiency.

If you want to contest this determination in court before making any payment, you have 90 days from the date of this letter (150 days if addressed outside the United States) to file a petition with the United States Tax Court for a redetermination of the deficiency.

Please click here to download a copy of the Order, Letter, Notice and Other Document Being Filed.

If you decide not to sign and return the waiver, and you do not file a petition with the Tax Court within the time limit, the law requires us to assess and bill you for the deficiency after 90 days from the date of this letter (150 days if this letter is addressed to you outside the United States).

---

Charlie Sheen Not Dead, But Virus Spreads On Facebook

American Red Cross

Together, we can save a life

Online Donation Form

NOTE: Credit card information is required and securely processed for the processing of the credit card transaction.

Gift Information

I want to make a contribution of

Select ONE of the following donations:

[Options]

American Red Cross volunteers have

---

[Image]
Flash Drive based Social Engineering – Old School
Example Social Engineering Techniques – New School

- Social Engineering with Ransomware

![Ransomware Image](image-url)
Example Social Engineering Techniques – New School

- Social Engineering IVR and Robocalls

  This is your credit card company. We are checking on a potential fraudulent charge on your card. Did you purchase...? Press 1 for yes or 2 for no
Recommendations

- Awareness
- Don’t fall for any cheesy scams. If it sounds too good to be true, it usually is.
- Evaluate the URL to ensure that the domain name matches what you would expect
  - https://www.bankofamerica.com - Correct
  - http://www.bankofmerica.com – Incorrect
- Hold repeat offenders accountable
Trojan Horses
Definition

- A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.
Many Different Types

- Remote-Access Trojans
- Anti-Protection Trojans
- Destructive Trojans
- Data-Sending Trojans
- DoS Attack Trojans
- Proxy Trojans
Propagation Methods

- Email
- Mobile
- Download from a website
- Road apple
- etc
Drive-by-Downloads
Definition

- A drive-by download refers to the unintentional download of a virus or malicious software (malware) onto your computer or mobile device.
  - Typically takes advantage of vulnerabilities
    - Browser vulns
    - Operating system vulns
    - Etc
  - After exploitation, malware will contact 3rd party site to download further malicious code
Typical Exploitation Steps

1) Attacker compromises a legitimate web application.

2) Attacker uploads malicious Javascript.

3) User sends web request to a compromised server which sends malicious Javascript to the victim.

4) Attacker now controls the victim.
Do Use Virus Total

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

By clicking 'Scan it', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.
Do Use Website Malware and Security Scanning Portals

Free Website Malware and Security Scanner

Enter a URL (ex. sucuri.net) and the Sucuri SiteCheck scanner will check the website for known malware, blacklisting status, website errors, and out-of-date software.

Scan Website

Disclaimer: Sucuri SiteCheck is a free & remote scanner. Although we do our best to provide the best results, 100% accuracy is not realistic, and not guaranteed.
Do Use Antivirus and Anti Malware Solution

• MalwareBytes is actually a solution worth purchasing

Do Update Your Computer and 3rd Party Software

Windows Update
- Check for updates
- Change settings
- View update history
- Restore hidden updates

Windows is up to date
There are no updates available for your computer.

Secunia System Score 88%

Programs that need updating (9)
- Updating Apple QuickTime 7.x
- Updating Apple iTunes 11.x
- Click to update Microsoft Internet Explorer 11.x (64bit)
- Click to update Microsoft Internet Explorer 11.x
- Click to update Microsoft Windows 7
- Click to update Microsoft XMIL Core
- Oracle java 1.6.2 3rd Party Software Workspace
- Click to update
- Click to update
Do Use Longer than 8 Character Passwords and Password Safes
Run Vulnerability Scans

![Nessus vulnerability scan interface](image)

- **172.16.71.128**
  - Port 137 (udp)
  - Port 139 (tcp)
  - Port 445 (tcp)

- **172.16.71.128**
  - Port 137 (udp)
  - Port 139 (tcp)
  - Port 445 (tcp)

- **445 / tcp**
  - Port 445 (tcp)

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Name</th>
<th>Port</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>10394</td>
<td>Microsoft Windows SMB Log In Possible</td>
<td>cifs (445/tcp)</td>
<td>Low</td>
</tr>
<tr>
<td>10397</td>
<td>Microsoft Windows SMB LanMan Pipe Server Listing Disk</td>
<td>cifs (445/tcp)</td>
<td>Low</td>
</tr>
<tr>
<td>10785</td>
<td>Microsoft Windows SMB NativeLanManager Remote System</td>
<td>cifs (445/tcp)</td>
<td>Low</td>
</tr>
<tr>
<td>11011</td>
<td>Microsoft Windows SMB Service Detection</td>
<td>cifs (445/tcp)</td>
<td>Low</td>
</tr>
<tr>
<td>18502</td>
<td>MS05-027: Vulnerability in SMB Could Allow Remote Code Execution</td>
<td>cifs (445/tcp)</td>
<td>High</td>
</tr>
<tr>
<td>26917</td>
<td>Microsoft Windows SMB Registry : Nessus Cannot Access</td>
<td>cifs (445/tcp)</td>
<td>Low</td>
</tr>
<tr>
<td>26920</td>
<td>Microsoft Windows SMB NULL Session Authentication</td>
<td>cifs (445/tcp)</td>
<td>Low</td>
</tr>
<tr>
<td>35362</td>
<td>MS09-001: Microsoft Windows SMB Vulnerabilities Remote</td>
<td>cifs (445/tcp)</td>
<td>High</td>
</tr>
</tbody>
</table>
Do not Install Software from Untrusted Sources

Experience the power...
Don’t Run as “Local Administrator” if not needed

```
C:\Users\admin>net localgroup administrators
Alias name      administrators
Comment          Administrators have complete and unrestricted access to the computer/domain

Members

admin
Administrator
Domain Admins
Enterprise Admins
The command completed successfully.
```
Mobile Device/Wireless Security
Mobile Devices

Mobile Risks Overview

- Mobile devices have many ways of communications and access to sensitive systems and data

Trends

- Many of the risks inherent to wireless
  - Interception, plain-text or “crackable” encryption
  - Passwords, session management, MitM
- Portable is Latin for “easy to leave in the back of a taxi”
  - Many high-profile “data breaches” are actually lost or stolen devices
- Easily available software can unlock smartphones in seconds or minutes
- Forensics and investigations
- Compliance
  - Are you sure you’ve moved all required regulatory controls onto the mobile devices touching your sensitive data? How would you show it?
- Patching and updates are necessary just as with any other device
- There are traditional attacks available for these devices
- Malware… and iOS folks shouldn’t get all high-and-mighty
- Lack of attacks for Mac/Apple was a function of economics not technology
Mobile Malware

Android Malware Surges, Botnet Business Booms

McAfee reports thousands of new malware apps targeting Android appeared early this year, along with a steady stream of botnet updates.

By Mathew J. Schwartz, InformationWeek
May 24, 2012 03:00 PM

Malware loves Android, but iOS users could be at risk too

A new study from Juniper finds that Android is the hardest hit by malicious apps but says iOS could be vulnerable as well.

Security company Kaspersky warns malware attacks on iOS will "mean disaster for Apple"
In order to be perceived as a “hip” or simply to make the process easier, many organizations are quickly pushing out mobile applications to make it easier for people to do business with them such as make donations.

Many of these applications are rife with security issues. Many of the same application development issues encountered with web applications are repeated with mobile devices.

For example some applications will encrypt the original login authentication mechanism, but later pass an unencrypted session key that could be hijacked and used to impersonate the user.

How will your reputation hold up if it leads to credit card or bank account theft as part of the process?
Real Life Example

```
lib
shared_prefs
root@generic:/data/data/com._________ # cd shared_prefs
cd shared_prefs
root@generic:/data/data/com._________/shared_prefs # ls
ls
com._________.preferences.xml
root@generic:/data/data/com.________/shared_prefs # cat com.________.preferences.xml
.lat_preferences.xml
< ?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="test@test.com" string>
    <long name="test@test.com" long>
      <value>1234567890</value>
    </long>
  </string>
</map>
root@generic:/data/data/com._________/shared_prefs # cat com.________.preferences.xml
.lat_preferences.xml
< ?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="4Life" string>
    <long name="4Life" long>
      <value>1234567890</value>
    </long>
  </string>
  <string name="test@test.com" string>
    <long name="test@test.com" long>
      <value>1234567890</value>
    </long>
  </string>
</map>
root@generic:/data/data/com._________/shared_prefs #
```
• What happens if your system or credentials get compromised while you’re on the road?
  • Is the attacker polite enough to say, “Oh, they went back to work, I better shut down that backdoor. It is the only civilized thing to do.”?
• Many controls are designed with the assumption that other security controls in the environment are protecting you
• When you are on the road there is little, or nothing, covering you
  • aka. You’re on your own, bub.
• Hotels, coffee shops, airports, etc.
• Kiosks and hotel work areas
  • Really? Does this strike anyone as a good idea?
• New and Snazzy! Charging station attacks!
  • aka. Juice-Jacking
Case Study: BYOD
Bring Your Own Disaster

• Situation:
  • Many corporations feel that by allowing employees to bring their own device to work they have a win/win situation. The company reduces cost by not having to provide the employees with a mobile device, and the employee has the freedom of choice to use any phone of their choosing, and only has one phone to carry around.

• Issues:
  • The biggest issue with this approach is that many companies don’t implement a mobile device management strategy, and rather rely on what has been in place for laptop computers.
  • Who owns the burden of device replacement when a device is seized for discovery? What personal rights of privacy can be expected by the employee? What happens with the data after they leave?
Case Study: Mobile Device Security

• Situation:
  • Approaches taken by corporations to secure end device vary. Often due to BYOD corporations are forced to limit how much they can control on the device due to the fact that employees expect a certain degree of separation and privacy on their devices.

• Issues:
  • The attack vector on exploiting mobile phones is greatly increasing. The return on investment is much greater and the ability to get access to a person’s mobile phone is much easier than getting to their work computer.
  • The amount of information that is stored on a cellular device can be much more compromising and damaging: GPS, SMS messages, emails, web browser history, VPN passwords, personal wireless passwords, etc.
How much do you trust that free wi-fi?
  – Good answer.

Now how much do you trust that known wi-fi?
  – Good question. Wait, why is my home wireless in this hotel?

I’m looking for Alice’s wireless

I am Alice’s wireless
  Oh.. And Bob’s wireless

And here are those web pages you asked for

And don’t worry about that firewall alert or certificate errors

I’m looking for Bob’s wireless
 Meet the Wifi Pineapple
  – aka. Jasager ("Yes man")
Mobile/Wireless Hacking Goes Airborne
Recommendations

- Lock your device with a PIN or password
- Only install applications from trusted sources
  - Shop at reputable app stores (Android users deselect “unknown sources” option in your devices application settings menu)
  - Check users’ reviews and ratings
  - Read the app’s privacy policy
Recommendations – Cont’d

- Back up your data
- Install updates
- Don’t jail break/hack your device
- Always log out of banking and shopping sites
- Turn off wi-fi location services and bluetooth services when not in use
- Avoid texting or email personal information
- Don’t click on links or attachments in unsolicited emails or text messages
Recommendations – Cont’d

- Security
  - WPA Type
    - WPA2-Personal
  - Encryption Type
    - WPA or WPA2 - Personal
    - WPA-Personal
  - Security Key Type
    - Use Custom Key/Passphrase
    - t5c34wt^v5t#$%ydsfg5&36745y
Recommendations – Cont’d

- OPENVPN®
- CyberGhost
- CLOAK
- Hotspot Shield
- TunnelBear
- VPNBOOK
Web Application Security
What is a Web Application

- Any application that is internet facing that you typically use leveraging browser software such as Internet Explorer, FireFox, Safari, and Chrome.
Example Web Applications

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Graph Search.

Sign Up
It's free and always will be.

First Name
Last Name
Your Email
Re-enter Email
New Password
Birthday
Month
Day
Year
Why do I need to provide my birthday?

Female
Male

By clicking Sign Up, you agree to our Terms and that you have...
Be great at what you do.

Get started – it’s free.
Registration takes less than 2 minutes.

First name
Last name
Email address
Password (6 or more characters)

By clicking Join Now, you agree to LinkedIn's User Agreement, Privacy Policy and Cookie Policy.

Join now
Back in the Day....

- Web applications were mostly static meaning that there wasn’t a whole lot of user input
- Most did not authenticate users
- No need for sessions
- Compromise of the web server would usually not result in loss of sensitive data
But like anything else, things change. Today there are…

- Highly functional web applications
- Rely on two-way flow of information
- Support registration and login, financial transactions, search, and authoring content
- Much of the information processed is highly sensitive
- New and unique security threats
The sad reality is...

- 61% of applications have various defects with the applications login mechanism
- 71% of applications fail to properly protect access to its data and functionality
94% of applications are affected by some sort of Cross-site scripting

This vulnerability targets the user

SSL (i.e. HTTPS) does not protect against any common application attack and in some cases, can actually cloak an attack
Web Application – Key Problem Factors

- Underdeveloped Security Awareness
- Developers are more pressured to add functionality than to secure their code
- Custom Development
- Simplicity
  - Platforms and development tools make things too easy
- Evolving Threat Profile
- Resource and Time Constraints
Web Application – Recommendations

• Never input any sensitive information in websites that don’t use HTTPS
Web Application – Recommendations

• Some websites use what is called Extended Validation HTTPS as indicated by the “green” in the browser.
Web Application – Recommendations

• Be careful of “Invalid Security Certificate Error” messages
Web Application – Recommendations

• If at any time the application you are using causes a message such as what is shown below, be careful.

Server Error in '/Top10WebConfigVulns' Application.

Unclosed quotation mark after the character string "". Incorrect syntax near "".

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string "". Incorrect syntax near "".

Stack Trace:


Version Information: Microsoft .NET Framework Version 2.0.50727.42; ASP.NET Version 2.0.50727.42
Questions?