

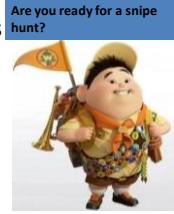
Introduction

- Russ McMahon
 - Associate Professor of Information Technology
 - Teach (11 yrs at UC)
 - Programming (C#)
 - Database Mgmt & Business Intelligence (SQL Server)
 - Information Security
 - Taught IT-related subject matter since 1980
 - Know a lot about a lot of useless stuff
 - Active in the local IT community
 - History – 50 Yrs of Computing at UC
 - IBM-650 arrived at UC in 1958
 - Race walker (reformed runner)



New “Internet” Threats

- Introduction
- Some Interesting Facts
- The Decade’s Top 10 Cybercrimes
- Today’s Internet Threats
- Today’s Headlines
- Cloud Security
- SCADA
- RFID
- ZARF is with you again
- Final Thoughts



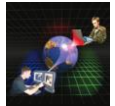
Some Interesting Facts

- What year was the 1st federal prosecution of computer fraud?
- For an expert bent on crime, cracking a computer system’s defenses is about as difficult as _____.
- Human error accounts for _____ of all data losses
- Dishonest insider (>, <, or =) evil outsider
- _____ of detected frauds are never reported
- Very few people have learned how to exploit software errors
- Problems
 - Social engineering
 - Mother nature
 - Vanishing paper trail
 - The sheer complexity of today’s systems
 - Security comes at a cost including inconvenience
- There is still reluctance to spend money for computer security



The Decade’s Top 10 CyberCrimes

- www.wired.com/threatlevel/2009/12/ye_cybercrimes
- Michael “Mafiaboy” Calce(2000) – DDOS
- California Payroll DB Breach (2002)
- Slammer (2003) – SQL Server
- Foonet (2004) – Saad Echouafni
- The LA Traffic Signal Attack (2006)
- Max Vision (2006) – 2mil credit cards == \$86 mil
- San Francisco’s network lockdown (2007)
- RBS Worldpay Heist (2008) – 44 gift cards ~\$ 1/2 mil/each
- Albert Gonzalez (2005-08) 7-11, D&B, TJX, Heartland
- Conficker (2009)
- Money Mules (2009) – Zeus & URLZone – work-at-home



Today’s “Internet” Threats

- The most common Web-based attack observed in 2009 was related to malicious PDF activity, which accounted for 49 percent of Web-based attacks. This is a sizeable increase from 11 percent in 2008.
- In 2009, the second most common Web-based attack was associated with the Microsoft Internet Explorer ADOBE.Stream Object File Installation Weakness, which accounted for 18 percent of the global total— a decrease from 2008 when this vulnerability accounted for 30 percent of the total during that reporting period.
- While ActiveX vulnerabilities are currently on the decline, vulnerabilities in other plug-in technologies such as Java SE and Adobe Reader are on the rise.
- Financially motivated attacks against both enterprises and individuals remain a large part of the threat landscape.
- www.wilderssecurity.com/showthread.php?t=271134



U.S. Federal Cybersecurity Market Forecast 2010-2015, Tabular Analysis, Publication: 03/2010, Pages: 69, Figures: 19, Tables: 30, Single User Price: \$3,950.00

Today’s Headlines

Even spammers are outsourcing these days.

The iPad already accounts for .03% of Web traffic. ... that’s compared to the BlackBerry’s .04%.

New details about the cyberthefts at Google last December seem to prove one thing: even the best of us can fall for routine hacker tactics.

A McAfee executive apologized for an “antivirus signature update” his company ran that crippled thousands of computers.

10th annual Cyber Defense Exercise

Security budgets will continue to grow in 2010. The biggest spending increase will be in the area of network security.

The cost of a data breach rose again last year. ...average breach studied was \$6.75 million. (cost per record lost = \$204)

Next on the Cyberhacker’s Victims List: Industrial Infrastructures




OWASP Top 10 (2010)





- Injection
- Cross Site Scripting (XSS)
- Broken Authentication & Session Mgmt
- Cross Site Request Forgery (CSRF)
- Security Misconfiguration (new)
- Failure to Restrict URL Access
- Unvalidated Redirects & Forwards (new)
- Insecure Cryptographic Storage
- Insufficient Transport Layer Protection
- www.slideshare.net/jeremiahgrossman/owasp-top-10-2010-release-candidate-1



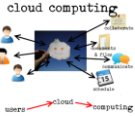
SANS Top 25





- www.sans.org/top25-programming-errors
- Insecure Interaction b/t Components (8)
- Risky Resource Mgmt (10)
- Porous Defenses (7)
- Common Weakness Enumeration (CWE)
 - cwe.mitre.org/


Cloud Computing





- NIST -- csrc.nist.gov/
 - cio.nist.gov/
 - csrc.nist.gov/groups/SNS/cloud-computing/
 - SaaS, IaaS, PaaS
- Jim Reavis – Co-founder of the Cloud Security Alliance (CSA)
 - Cloud Computing Security Risks
 - <http://www.cloudsecurityalliance.org/or/20100301a.html>
 - Abuse and Nefarious Use of the Cloud
 - Insecure APIs (Weakest Link Security)
 - Insider Threat
 - Shared Technology Vulnerabilities
 - Data Loss/Leakage
 - Account/Service and Traffic Hijacking
 - Unknown Risk Profile
- www.pdc.kth.se/events/event-repository/cloud-computing-security-an-oxymoron
- PKI – Public Key Infrastructure
 - www.pkispace.org/
 - csrc.nist.gov/groups/SNS/pki/pki/index.html
- ENISA – www.enisa.europa.eu/
- CloudSecurity.org – cloudsecurity.org/


RFID





- Earliest ideas – WWII (radar) & developed in the 1950s
- Charles Walton – Father of RFID (1970s patents)
- NIST SP800-98 Guidelines for Securing Radio Frequency Identification Systems
 - <http://csrc.nist.gov/>
 - FIPS Pub 180-2
 - ISO/IEC 14443
- Marty Cooper (cell phone) – 60 Minutes interview
 - "I think the whole concept of privacy requires a new mindset among people. There are people who object to somebody monitoring their buying habits. I'm delighted if people know what I buy because they're gonna tailor their marketing to me and the products that are available to me, to my tastes. Well, that's a good thing."
- Security Concerns
 - illicit tracking of RFID tags
 - EPGlobal Network, by design, is also susceptible to DoS attacks
 - researchers have cloned passport data while the passport is being mailed to its owner
 - Skimming, eavesdropping, spoofing, data tampering, cloning, malware insertion
 - Killing the tag
- Electronic Product Code -- www.epcglobalinc.org/home/
- PASS card – www.uspasscard.com/
 - Western Hemisphere Travel Initiative – travel.state.gov/travel/cbpmc/cbpmc_22
- Reader Talks First vs Tag Talks First
- HIPAA issues


RFID




- HERO (Hazards of EMR to Ordnance)
- Authentication methods
 - Passwords
 - Keyed-hash Message Authentication Codes (MAC)
 - Digital signatures
- RFID Security Alliance & RFID Consortium for Security and Privacy
 - de facto authoritative organization
 - partnership between academic and industrial scientists
- A Bit of Privacy
 - www.rfidjournal.com/article/articleview/1536/1/133/
 - This article proposes that killing RFID chips located on a retail sale items does not allow RFID chips to attain their full potential. It proposes that, in order maintain consumers privacy, instead of killing the RFID tag, a "privacy" bit is flipped, that allows only certain readers (readers contained in "smart appliances, for example) to continue to read the tag by emitting a "privacy-read" command. The theory is that the chip would now only respond to these privacy-read commands, therefore ensuring privacy. (pretty shaky privacy policy, if you ask me)
 - I think the whole RFID thing is neat but at the same time kind of scary because of how stores will be able to have so much information on your habits of what you buy and etc. As long as you trust the government and business with your information and privacy measures are in place it would a very convenient way to shop and do business.

SCADA



- Supervisory Control and Data Acquisition
- Italian Job (2003), Die Hard 4 (2007)
- Aug 21, 2006 -- Gabriel Murillo and Kartik Patel allegedly hacked in to the Los Angeles city traffic center to turn off traffic lights at four intersections
 - John G. O'Leary (Security Summit 2009 – Cleveland)
- IEEE article -- The Cyberhacker's Next Victim: Industrial Infrastructures
 - <http://bmsmail3.ieee.org:80/u/16182/303921>
- Not quite true
 - The right people are concern about security and authentication in the design, deployment and operation of existing SCADA networks
 - Security exists via obscurity
 - They are physically secured & they are disconnected from the Internet



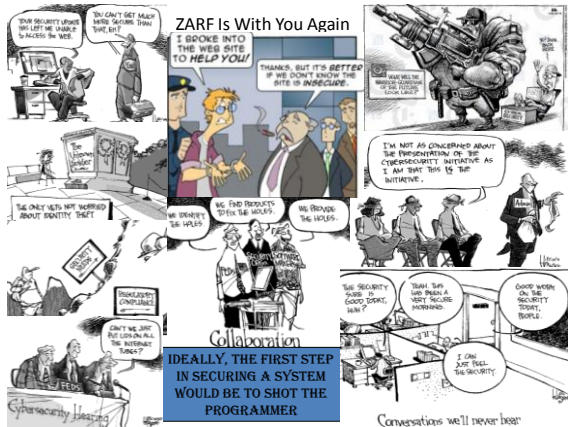
SCADA

- Threats
 - unauthorized access to the control software, whether it be human access or changes induced intentionally or accidentally by virus infections and other software threats residing on the control host machine
 - packet access to the network segments hosting SCADA devices
- ISA Security Compliance Institute (ISCI)
 - www.isa.org
 - www.isasecure.org



SCADA

- Open SCADA Security Project
 - www.scadasecurity.org
 - Initiative to create an open SCADA security community
- DHS Control Systems Security Program (CSSP)
 - www.us-cert.gov/control_systems
 - to reduce industrial control system risks within and across all critical infrastructure and key resource sectors
- The Center for SCADA Security (Sandia National Labs)
 - www.sandia.gov/scada
- National SCADA Test Bed Program (Idaho National Lab)
 - www.inl.gov/scada/index.shtml



Final Thoughts

- Waiting for the Great Computer Rip-off
 - Tom Alexander, Fortune, July 1974
 - Donn Parker
 - www.cbi.umn.edu/collections/nw/cbi00166.html
- International Information Integrity Institute (I-I)
 - i4online.com/
 - www.allbusiness.com/services/business-services/4529260-1.html
- Local IT Security Orgs
 - ISACA -- www.isaca-cincinnati.org/
 - ISSA –
 - OWASP -- www.owasp.org/index.php/Cincinnati
 - Infragard
- Stay hungry, stay foolish
 - www.wholeearth.com
 - Steve Jobs 2005 Stanford commencement speech

