

**Session Resources**  
**ADAPT Meeting - February 12<sup>th</sup>, 2004**

---

**Microsoft's Ten Immutable Laws Of Security**

- Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
- Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore
- Law #3: If a bad guy had unrestricted physical access to your computer, it's not your computer anymore
- Law #4: If you allow a bad guy to upload programs to your web site, it's not your web site anymore
- Law #5: Weak passwords trump strong security
- Law #6: A machine is only as secure as the administrator is trustworthy
- Law #7: Encrypted data is only as secure as the decryption key
- Law #8: An out of date virus scanner is only marginally better than no virus scanner at all
- Law #9: Absolute anonymity isn't practical, in real life or on the web
- Law #10: Technology is not a panacea

**Some History of Cyber Crime:**

**1998**

- Solar Sunrise, a series of attacks targeting Pentagon computers, leads to the establishment of round-the-clock, online guard duty at major military computer sites.
- Ehud Tenebaum, an Israeli teen-ager known as "The Analyzer," is arrested in Israel. Officials suspect him of working in concert with American teens to break into Pentagon computers. Israeli Prime Minister Benjamin Netanyahu calls Tenebaum "damn good ... and very dangerous."
- Hackers alter The New York Times Web site, renaming it HFG (Hacking for Girls). The hackers express anger at the arrest and imprisonment of Kevin Mitnick, the subject of the book "Takedown" co-authored by Times reporter John Markoff.
- Two hackers are sentenced to death by a court in China for breaking into a bank computer network and stealing 260,000 yuan (\$31,400).

**1999**

- Classified computer systems at Kelly Air Force Base in San Antonio, Texas, come under attack from a number of locations around the world, but the attacks were detected and stopped by newly developed Defense Department systems.

- ❑ U.S. Information Agency Web site is hacked for the second time in six months. The hacker circumvented the agency's Internet security and damaged the hard drive, leaving behind the message "Crystal, I love you" and the signature "Zyklon."
- ❑ Rep. Curt Weldon, R-Pennsylvania, says Defense Department computers are under a "coordinated, organized" attack from hackers. "You can basically say we are at war," he said.
- ❑ The San Francisco-based Computer Security Institute reports that corporations, banks and government agencies all face a growing threat from computer crime -- committed both inside and outside their organizations.
- ❑ President Clinton announces a \$1.46 billion initiative to improve government computer security. The plan would establish a network of intrusion detection monitors for certain federal agencies and encourage the private sector to do the same.
- ❑ Kevin Mitnick, detained since 1995 on charges of computer fraud, signs plea agreement.

**2003** President Bush signed the *National Strategy to Secure Cyberspace*

- <http://www.whitehouse.gov/pcipb/>

How's the Government doing so far? Excellent Videos from Frontline on CyberWar

- <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/view/>

### **The Current Environment:**

- ISP, PSINet put two "dummy" sites on the net. One with a firewall, one without. The protected site was attacked 200 times per day, the unprotected site 2000 times per day. Over an eight week period the unprotected site was attacked every 4 minutes or 19,128 times, while the protected site was attacked once an hour or 1,672 times.
- 2,524 New Vulnerabilities discovered in 2002 on all platforms.\*
- 7 New Vulnerabilities per day.\*
  - ❑ Increased reporting and media exposure for vulnerability researchers\*
  - ❑ New methodologies to exploit software bugs.\*
- US accounts for 36% of all attacks worldwide. South Korea #2
- 60% of new vulnerabilities are easily exploited because exploit code is readily available, or not needed.

### **Excellent Video, which will bring the awareness to the home user:**

Frontline: Sensational hacker attacks on large e-commerce and corporate sites get a lot of media attention. But computer security analysts discuss in this video-clip why these break-ins are probably only the tip of the iceberg and corporate America is turning to their own private intelligence agencies to protect itself.

<http://www.pbs.org/wgbh/pages/frontline/shows/hackers/etc/video.html>

### **Hacker Communities:**

- **alt.2600 Newsgroups:**  
<http://www.petascale.org/inls80/2600list.html>
- <http://www.2600.com/>
- <http://phrack.org/>

#### Interviews & Information:

- <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/reidcount.html>
- <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/curador.html>
- <http://tlc.discovery.com/convergence/hackers/hackers.html>

#### Attacks we discussed:

- **Network Attacks**
  - Type of attack where the goal is to gain unauthorized access to or disrupt internal networks or communication between internal networks and the Internet.
- **Software Attacks**
  - Type of attack where Operating systems and applications are specifically targeted.
- **Physical Attacks**
  - Is it locked up?
- **Social Engineering Attacks**
  - Use of trickery and deception to take advantage of people's natural inclination to help and to trust.
- **Email Attacks**
  - Attacks on the most widely used form of communication

#### We Talked about Port Scanning Attacks:

- A Port Scanning attack is when a potential attacker scans the systems that are connected to the Internet (border routers, firewalls, web servers) to see which TCP and UDP ports are listening and which services on the system are active
- The goal of Port Scanning is to determine where vulnerabilities lie in a organizations infrastructure
- Common Ports: FTP (21), Telnet (23), SMTP (25), DNS (53), BOOTP (67,68), HTTP (80), POP3 (110), NNTP (114), NetBios (137,138,139, 445), HTTPS (443)
- <http://www.iana.org/assignments/port-numbers>

#### We talked about script kiddies:

- **Read: Strange tales of a Denial of Service Attack:**  
<http://grc.com/dos/grcdos.htm>

## **We talked about Trojan horse Programs:**

- **Trojan Port List:**

- <http://www.nccn.net/~ncpcug/trojans.htm>

## **I demonstrated a password attack:**

- **Password guessing**

- In a password guessing attack, an attacker tries to guess user passwords either manually or through the use of scripts

- **Brute force**

- In a brute force attack, the attacker employs an application to exhaustively try every alpha-numeric combination to crack encrypted/hashed passwords

- **Dictionary**

- Method of breaking passwords by using a predetermined list of words as input to the password hash
- Only works against poorly chosen passwords

## **Why Have Strong Passwords? Here's a statistic that's quite illustrative:**

Example: A lower case password of eight characters has  $26^8$  possibilities (208,827,064,576). At one million attempts per second it would take 59hrs to crack. A complex eight character password has  $62^8$  possibilities (218,340,105,584,896). At one million attempts per second, it would take 6.9 years

## **We talked about social Engineering, and the master Kevin Mitnick:**

- **Kevin Mitnick on Social Engineering:**

- <http://zdnet.com/2100-11-522261.html?legacy=zdn>
- <http://www.intenseschool.com/bootcamps/security/mitnick/default.asp?bc=mitnick>

- **Fabulous video:**

- <http://www.techtv.com/screensavers/answerstips/story/0,24330,3360637,00.html>

## **Valuable tools for the home user:**

[www.zonealarm.com](http://www.zonealarm.com)

Every home should have one of these:

<http://www.linksys.com/Products/product.asp?grid=34&scid=29&prid=561>

OR, if wireless:

<http://www.linksys.com/products/product.asp?grid=33&scid=35&prid=544>

I am pretty sure you can get them at Staples ☺

**Contact me with further questions:**

John H Rogers  
Sage Data Security  
[johnr@sagedatasecurity.com](mailto:johnr@sagedatasecurity.com)  
[www.sagedatasecurity.com](http://www.sagedatasecurity.com)  
207.879.7243 x2