NUIT Tech Talk:
Data and Information Security at Northwestern

January 24, 2007

Roger Safian, Senior Data Security Analyst, NUIT
Agenda

- Introduction and brief bio
- Security statistics
- Protecting yourself from online threats
- Tools
- Questions
What is a Security Incident?

• Incident Response Protocol: Any known or highly suspected circumstance that results in an actual or possible unauthorized release of information deemed sensitive by the University or subject to regulation or legislation, beyond the University’s sphere of control.

[http://www.it.northwestern.edu/policies/procedures](http://www.it.northwestern.edu/policies/procedures)
Security Incident Examples

- Compromise or unauthorized access of a system (PC, server, PDA)
- Theft / loss of PC holding files with SSNs
- Printed copies of student loan applications found in a dumpster
- E-mail with unencrypted sensitive data sent to wrong recipient
- Data storage devices/media missing
About Me

• IT – Senior Data Security Analyst
  – Information & Systems Security/Compliance
  – 20+ years at Northwestern

• NU-CERT

• NU’s FIRST representative
  – Former Steering Committee member

• CIC/Big Ten Security Working Group
  – Former chair
Security Statistics

NU Security Incidents

AY 01/02
AY 02/03
AY 03/04
AY 04/05
AY 05/06

NU
Dorms
Security Statistics

NU Security Incidents 9/1/05 - 8/31/06

Incident Type

- Virus: 515 (NU), 201 (Dorms)
- Malware: 395 (NU), 102 (Dorms)
- NU SA: 1343 (NU), 441 (Dorms)
- DMCA: 163 (NU), 132 (Dorms)
- Total: 2428 (NU), 804 (Dorms)

Information Technology
Security Statistics

![Security Statistics Graph](Image)

**Graph Description:**
- **Incident Type:** Virus, Malware, NUSA, DMCA, Total
- **Comparison Periods:** Q1 2005 - 2006, Q1 2006 - 2007
- **Data Analysis:**
  - Virus: 199 (Q1 2005-2006), 110 (Q1 2006-2007)
  - Malware: 158 (Q1 2005-2006), 37 (Q1 2006-2007)
  - NUSA: 673 (Q1 2005-2006), 441 (Q1 2006-2007)
  - DMCA: 89 (Q1 2005-2006), 50 (Q1 2006-2007)
  - Total: 1121 (Q1 2005-2006), 659 (Q1 2006-2007)
What’s at Stake?

• Your personal information
  – Protect yourself, deter identity theft

• Safety of our constituents
  – Ensure privacy and compliance, deter identity theft, avoid litigation & fines

• Network performance
  – Help ensure stability, enhance performance

• Northwestern’s reputation
  – Avoid adverse publicity
YOU are the KEY to reducing these numbers
Why Incidents Occur

• Weak Passphrases
  – All machines and accounts need passphrases
  – Use rules similar to the NetID rules

• Opening viral attachments
  – Don’t open unexpected attachments
  – Only open specific types of extensions
  – Make sure to look at the LAST extension
Why Incidents Occur

• Updates not applied
  – Ensure Windows update runs automatically
  – Don’t forget about layered products

• Network use
  – P2P
  – Be careful when clicking on links
Why Incidents Occur

• Instant Messaging
  – Be careful of links in messages
  – Don’t add extensive plug-ins

• Out of date anti-viral software
  – Ensure you install the NU supplied software
  – Set to update automatically EVERY day
Why Incidents Occur

• Lack of firewall
  – Even if user has one they don’t understand it
    • Sometimes blamed for problems
      – Then removed
    – Often installed after the infection
      • Not a good idea
Ground Rules

• Microsoft focused
• In your department
  – Check with your department tech support
  – Report anything that seems unusual
• At home
  – You are the tech support
  – Know what your family does online
  – Never share your NetID or passphrase
Turn Your Computer Off

• If your computer is off, it can’t be compromised
  – You save energy as well

• Lock computer when you leave
  – *Hold down the Windows Key and press L*
Sensitive Data

• Think about the data on your computer
  – Is it regulated?
  – Does it have financial value?
  – If it was about you, would you want strangers to see it?

• Encrypt it
  – Delete it if it is no longer needed

• Never e-mail sensitive information in plain text
Passphrases

• NU NetID Passphrase
  – Be cr34t1v3 (creative)
    • Fth,oM (From the halls of Montezuma)
  – Longer is better
    • NUIT is working to extend the length of passphrases
  – Never share your passphrase

• Windows Passphrase
  – Separate accounts; separate passphrases
  – Change regularly
Software Updates & Patches

• Windows Update
  – Should be set to run automatically
  – Check manually as well

• Other software
  – E-mail software
  – Web browser
  – Microsoft Office
  – Antivirus software
  – Instant Messenger
Firewall Protection

• Standard with Windows XP SP 2
  – And many other products/operating systems
• Always keep your firewall active
• Combine with hardware firewall if possible
• Zone Alarm is free for home use
  – Search for “free Zone Alarm”
Antivirus Software

- Never open unexpected files
- Keep up to date
  - Set to auto-update
  - Manually check as well
- Run regular scans (weekly or more)
  - Try from Safe Mode (reboot, hold F8)
- Delete files from quarantine
Instant Messenger

• Malware spreads via buddy lists
  – Often done without the knowledge of the infected user.

• Verify that a link was sent to you
  – Ask the sender if they sent you a link

• Be very cautious about installing extra plug-ins to your client
Spyware

• Disable ActiveX and Javascript
  – Tools > Internet Options > Security

• Be careful when downloading programs

• Use a spyware removal program
  – More than one is better
  – Spyware – Search & Destroy:
    • http://www.safer-networking.org/en/
Junk E-mail (Spam)

- Never reply to remove
- Use junk e-mail filters
- E-mail Defense System (EDS)
  - Filters some junk e-mail and viruses at server level; only for central mail servers
    - Only monitors the alias – not the actual mailbox
Phishing & Pharming Scams

• Phishing: getting you to do an activity
• Pharming: getting your computer to do an activity
• Never give your personal information in response to a unexpected request
• Use out-of-band communication to verify
• Double-check embedded URLs
Copyright Violation

• Peer-to-peer (P2P) software is legal
• Violation of copyright is illegal
• Malware targets P2P software
• Be aware of what your children and household members are doing
  – It’s you who gets sued (and pays penalty)
• Never plug your computer directly into DSL or cable modem
• Do not use default SSID (*service set identifier*; wireless network name)
• Make sure your signal does not go too far
• Do not broadcast your SSID
• If you still use a modem, bring Windows & software updates home
Recommendations

- Windows update set to automatic
- Anti-Virus software up to date
- Strong Windows passphrase
  - 15 characters is the “sweet spot”
- File sharing is OFF
- Firewall is ON
- System Restore is OFF
- Guest account is disabled
Tools I Use

• SAFER
  – Available for IE, Office, Messenger, etc.
  – http://blogs.msdn.com/aaron%5Fmargosis/
• Process Explorer
• Autoruns
• Rootkit Revealer
  – http://www.sysinternals.com/
• HijackFree
Tools I Use

• Baseline Security Analyzer

• Malicious Software Removal Tool

• Windows Defender – Beta 2
Tools I Use

• Port Reporter
  – http://support.microsoft.com/kb/837243

• Ad Aware
  – http://www.lavasoftusa.com/software/adaware/
  – Don’t forget to look at the Add-Ons

• Spybot Search and Destroy
Tools I Use

• Trend Micro
  – scans for virus and spyware

• Sophos Anti-Rootkit

• Symantec Web Site
Tools I Use

• Internet Storm Center
  – http://isc.sans.org/

• Active Ports
  – http://www.protect-me.com/freeware.html

• Microsoft Power Toys
  – http://www.microsoft.com/windowsxp/download\s/powertoys/xppowertoys.mspx
    • Tweak UI

• Task Manager
Tools I Use

• Reformat & Reinstall
  – Make sure to backup any needed data
    • Make an extra copy, just to be safe
  – Do not have network access enabled
    • That includes wireless
  – At least SP2 before connecting to network
    • Then download the remaining patches
      – If you can NAT even better
  – Make sure to get up to date AV software
Tools I Use

• Ask questions
  – What version of OS?
    • If Windows verify version on system
  – Is your anti-viral software up to date?
    • Check the date
  – Is firewall active?
    • Verify and check for holes
  – Have you changed anything recently?
  – What were you doing when you noticed?
Things NOT To Do

• Turn off automatic updates
• Turn off firewall
• Turn off Anti-Virus software
• Uninstall Service Packs or Hotfixes
• Relying on browser X as “secure”
• Forget to check that the admin account has a strong passphrase
Things NOT To Do

• Rebuilding a machine while it’s on the NU Network
• Put infected machine on the NU Network to download updates and fixes
• Install a firewall to limit malware already on an infected machine
• Knowingly work with pirated software
Internet Resources

• Get Help
  – http://www.it.northwestern.edu/security/help.html

• Secure the Work Environment
  – http://www.it.northwestern.edu/security/working.html

• Computer and Network Security
  – http://www.it.northwestern.edu/security/index.html
Contact Information

• Roger Safian
  – (847) 491-4058
  – security@northwestern.edu
  – r-safian@northwestern.edu

• NUIT Support Center
  – (847) 491-HELP (4357)
  – consultant@northwestern.edu

• Northwestern Network Operations Center
  – (847) 467-6662 (staffed 24 hours per day)
Questions?
Save the date!

January 31: Windows Vista Preview
February 7: Data Security at Northwestern
February 21: Support with NUIT

University Library, Forum Room, Noon – 1 p.m.