NUIT Tech Talk:
Online Privacy and Security

National Cybersecurity Awareness Month

Presenter: Roger Safian, Senior Data Security Analyst, NUIT

NORTHWESTERN
UNIVERSITY

Information Technology

Agenda

- Introduction and brief bio
- Security statistics
- Protecting yourself from online threats
- Tools
- Questions

Security Incident Defined

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

Security Incident Defined

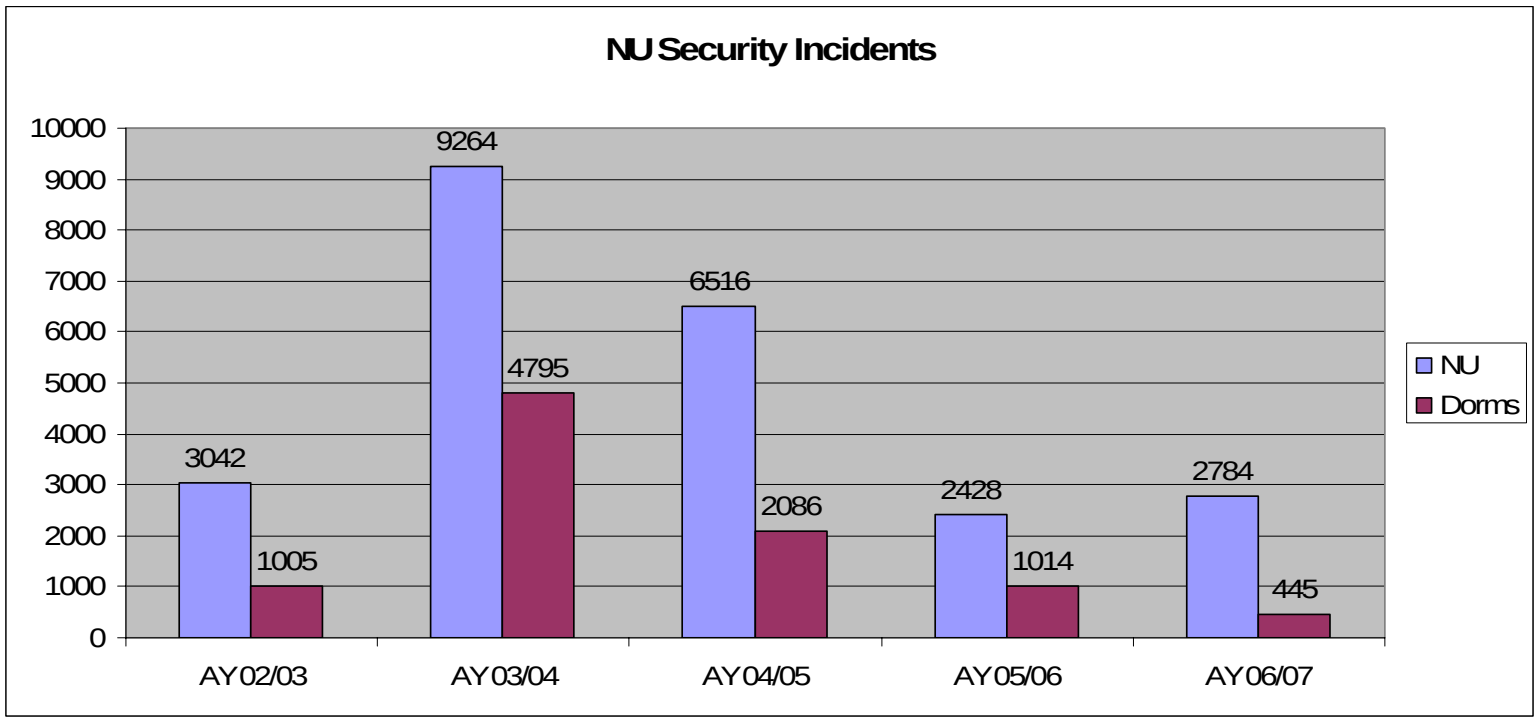
Examples

- 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

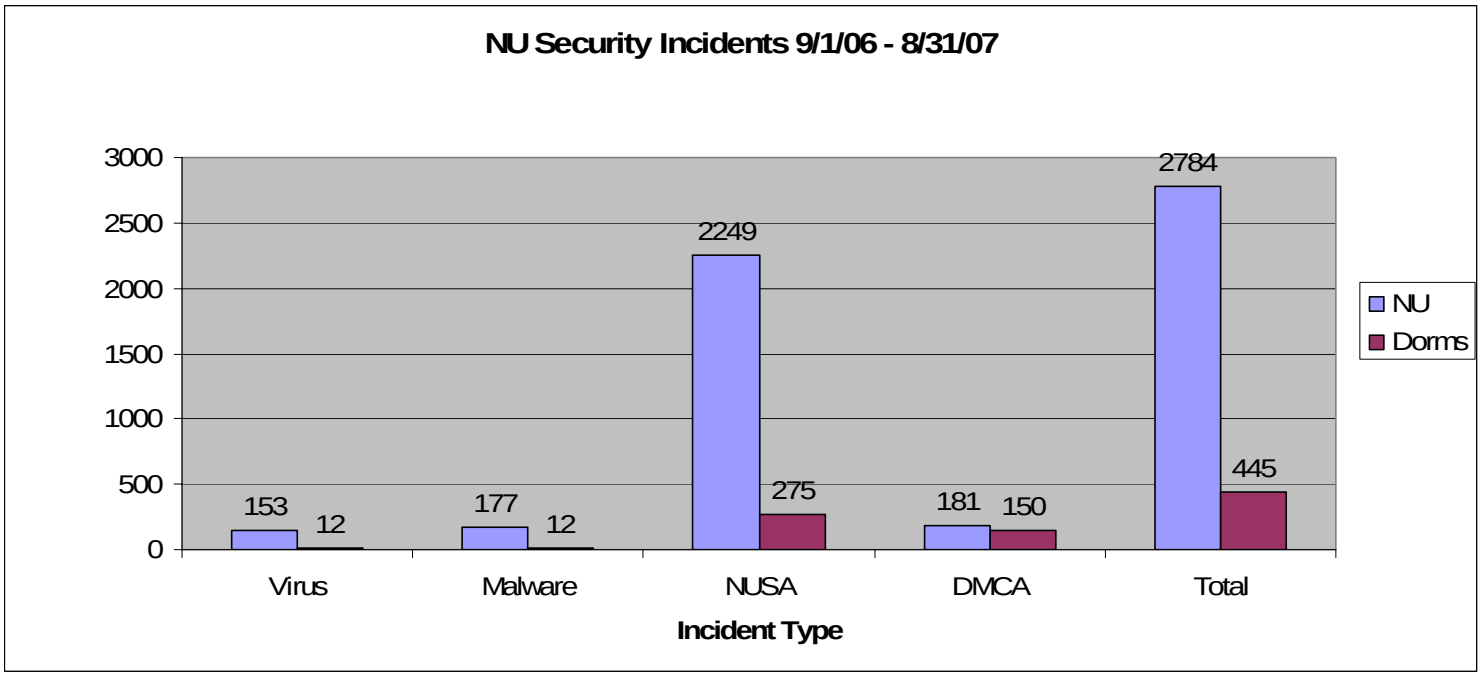
About Me

- 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



Security Statistics (cont'd)



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

Information Security

YOU are the *KEY*
to reducing these numbers

Why These 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 These Incidents Occur (cont'd)

- Updates not applied
  - Ensure Windows update runs automatically
  - Don't forget about layered products
- Network use
  - P2P
  - Be careful when clicking on links

Why These Incidents Occur (cont'd)

- Instant Messaging
  - Be careful of links in messages
  - Don't add extensive plugins
- Out of date anti-viral software
  - Ensure you install the NU supplied software
  - Set to update automatically EVERY day

Why These Incidents Occur (cont'd)

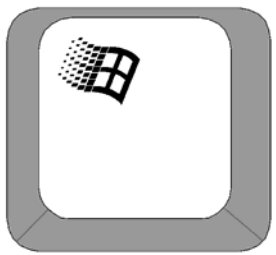
- Lack of firewall
  - Even if user has one they don't understand it
    - Sometimes blamed for problems
      - Then removed
  - Often installed after the infection
    - Not a good idea

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**



+ 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

Pass*phrases*

- 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
  - http://www.zonealarm.com/
  - 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 plugins 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 any penalty

Routers, Wireless & Modems

- 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

Recomendations

- 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
  - http://www.hijackfree.com/en/

Tools I Use (cont'd)

- Baseline Security Analyzer
  - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- Malicious Software Removal Tool
  - http://www.microsoft.com/security/malwareremove/default.mspx
- Windows Defender – Beta 2
  - http://www.microsoft.com/downloads/details.aspx?FamilyId=435BFCE7-DA2B-4A6A-AFA4-F7F14E605A0D&displaylang=en

Tools I Use (cont'd)

- 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
  - http://www.safer-networking.org/en/download/index.html

Tools I Use (cont'd)

- Trend Micro
  - scans for virus and spyware
  - http://www.trendmicro.com/en/home/us/enterprise.htm
- Sophos Anti-Rootkit
  - http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html
- Symantec Web Site
  - http://www.symantec.com/enterprise/security_response/threatexplorer/threats.jsp

Tools I Use (cont'd)

- Internet Storm Center
  - http://isc.sans.org/
- Active Ports
  - http://www.protect-me.com/freeware.html
- Microsoft Power Toys
  - http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx
    - Tweak UI
- Task Manager

Tools I Use (cont'd)

- Virginia Tech – Find_SSNs
  - http://filebox.vt.edu/users/rtilley/public/find_ssns/index.html
- Cornell – Spider
  - http://www.ats.cornell.edu/security/tools/
- TrueCrypt
  - http://www.truecrypt.org/

Tools I use (Cont'd)

- NU Sensitive Data Search Web Page
  - http://www.it.northwestern.edu/policies/datasearch.html
    - http://www.it.northwestern.edu/bin/docs/character_string_search.pdf

Tools I Use (cont'd)

- 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 (cont'd)

- 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”
- Not checking that the admin account has a strong passphrase

Things NOT To Do (cont'd)

- Rebuilding a machine, while it's on the network
- Put infected machine on the network to download updates and fixes
- Install a firewall to limit malware already on an infected machine
- Knowingly working with pirated software

More Help

NUIT Web info

- 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
- Copy of this presentation available online at
  - http://www.it.northwestern.edu/learning/techtalks/datasecurity.pdf

Contact Information

- Roger Safian
  - (847) 491-4058
  - security@northwestern.edu
  - r-safian@northwestern.edu
- NUIT Support Center
  - (847) 49**1-HELP** (4357)
  - consultant@northwestern.edu
- Northwestern Network Operations Center
  - (847) 467-6662 (staffed 24 hours per day)

Questions?

Fall Quarter Tech Talks

- *Are You Software Savvy? – October 30*
- *What's New with Windows Vista – November 27*
- *Prevent Security Incidents with New Symantec Protection - November 29*

More Information: www.it.northwestern.edu