Computer Security Orientation for Graduate Students
Campus Security Environment

- 65,000 internet addresses
  - Most open to the Internet
  - 13,000 “Office Workers” (faculty and staff)
  - 40,000 undergrads
    - 10,000 students in dorms
    - 10,000 grad students
  - High Performance Computing
A lot of Traffic

'UIUCNet' Network Traffic Summary

bps

TOTAL IN OUT MULTICAST

Thu 10/22 Fri 10/23 Sat 10/24 Sun 10/25 Mon 10/26 Tue 10/27

illinois.edu
Exceptionally Broad Usage Pattern

<table>
<thead>
<tr>
<th>Key</th>
<th>Bytes</th>
<th>bps</th>
<th>Percent</th>
<th>Service Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/80</td>
<td>1.98 T</td>
<td>183.54 Mbps</td>
<td>64%</td>
<td>HTTP</td>
</tr>
<tr>
<td>TCP/443</td>
<td>235.14 G</td>
<td>21.77 Mbps</td>
<td>8%</td>
<td>HTTPS</td>
</tr>
<tr>
<td>TCP/25</td>
<td>90.50 G</td>
<td>8.38 Mbps</td>
<td>3%</td>
<td>SMTP</td>
</tr>
<tr>
<td>TCP/135</td>
<td>73.19 G</td>
<td>8.78 Mbps</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>TCP/88</td>
<td>50.00 G</td>
<td>5.19 Mbps</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>TCP/445</td>
<td>50.18 G</td>
<td>4.65 Mbps</td>
<td>2%</td>
<td>SFTP</td>
</tr>
<tr>
<td>TCP/22</td>
<td>45.01 G</td>
<td>4.17 Mbps</td>
<td>1%</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP/5001</td>
<td>33.04 G</td>
<td>3.06 Mbps</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>GRE</td>
<td>28.13 G</td>
<td>2.60 Mbps</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>TCP/1500</td>
<td>24.86 G</td>
<td>2.28 Mbps</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Other (52,784 k services)</td>
<td>488.65 G</td>
<td>45.24 Mbps</td>
<td>16%</td>
<td></td>
</tr>
</tbody>
</table>
There are bad people in the world.
And they’re looking at us
Security Trends

• Five years ago
  – 750,000 legitimate emails per day
  – 750,000 spam emails per day
  – 180,000 email viruses

• Today
  – 750,000 legitimate emails per day
  – 6-7 million spam emails (peaks > 60 million)
  – 1,500-3000/day email viruses with spikes
CITES Spam Control

- http://www.cites.illinois.edu/antispam/overview.html
Security Trends

- Web based malware
  - Facebook
  - Phishing
- Traditional viruses and Trojans delivered through the web

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Number of Threat Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>CnsMin</td>
<td>552</td>
</tr>
<tr>
<td>W32/Rontokbro.gen@MM</td>
<td>487</td>
</tr>
<tr>
<td>FakeAlert-XPsecCenter</td>
<td>205</td>
</tr>
<tr>
<td>MWS</td>
<td>102</td>
</tr>
<tr>
<td>GameVance</td>
<td>42</td>
</tr>
<tr>
<td>Generic.dx</td>
<td>40</td>
</tr>
<tr>
<td>Generic!atr</td>
<td>37</td>
</tr>
<tr>
<td>JS/NRClick</td>
<td>35</td>
</tr>
<tr>
<td>W32/Mydoom.a.eml!zip</td>
<td>29</td>
</tr>
<tr>
<td>Generic PUP.x</td>
<td>28</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1557</strong></td>
</tr>
</tbody>
</table>
Tossed Up Websites

- phpBB
- Drupal
- Media Wiki
- Just say no to anonymous posting
Google Alerts

• Google Web Alert for:

[1] Illinois, University of Illinois
viagra for sale viagra buy viagra buy viagra online viagra canada buy viagra in the best pharmacy online viagra canada prescription buy sildenafil buy ...

This as-it-happens Google Alert is brought to you by Google.


--------------------------------------------------------

Graduate Students

- Sometimes you’re a
  - Student
  - IT Professional
  - Teacher
  - Researcher
  - Gopher
Information Technology at UIUC

• Unit IT
  – Most services and support
  – userhelp@cs.illinois.edu (computer science support)

• CITES
  – Campus central IT
  – Core services (network, email, etc…)
  – Service Desk: http://www.cites.illinois.edu/help/
  – consult@illinois.edu

• AITS
  – System-level IT
  – Banner (payroll, registration, etc…)
Policies to know

- What is permitted on campus
  - Appropriate Use Policy
  - Information Security Policy
Appropriate Use

• Nothing illegal
• No political use
• Cannot use for commercial use
• Respect copyright
  – If found sharing files, you will be disciplined and can be terminated.
• Limited personal use ok
• Limited personal publishing ok
  – no commercial sites
Passwords

• You may have multiple passwords
• CITES provided passwords can be simultaneously sync’d at
  – https://passwords.cites.uiuc.edu/index.html
• NetID Password is your ‘master password’
• Unit passwords are not under our control
• “North of Green Street” effect
• Password Entropy
  – http://en.wikipedia.org/wiki/Password_strength#Entropy.2C_or_bit_strength
• Number one source of compromised accounts on campus: ex’s.
Working remotely

- VPN – always a good idea
- Remote Desktop – safer than recognized
- SSL – If it touches sensitive data use SSL
- SSH – most common ‘serious’ compromise
  - [http://www.ncsa.illinois.edu/UserInfo/Resources/Software/ssh/openssh_ncsa.html](http://www.ncsa.illinois.edu/UserInfo/Resources/Software/ssh/openssh_ncsa.html)
Sensitive Data

- Creating
  - Access vs. copy
  - Secured location
  - Need for copies

- Transferring
  - Authorization for transfer
  - Secured transfer
  - Receiver authorized?

- Storing
  - Password protect
  - Secured
  - Encrypted

- Deleting
  - Shred or securely erased
Hand-me-downs

- You are responsible for data on your machine - even if you didn’t put it there
- Know what data you leave behind
- Closet zombies
Student Data

• ALL student data is protected by Federal Legislation known as FERPA
  – http://registrar.illinois.edu/staff/ferpa_tutorial/index.html
• Posting grades or other sensitive data online is forbidden
• Stolen/lost laptops with student data = get to know your University Administrators
When you get Compromised (and you will)

• Prepare for it (encrypt, encrypt, encrypt)
• Let us know (research and student data) security@illinois.edu
• Your machine will be removed from the network if it has a detectable compromise
• Sensitive data complicates matters – minimize it and secure it
Research Problems I

- Wire speed grows faster than deep packet inspection capability
- Network generated data is overwhelming – huge signal to noise problem
- All crypto is too complicated for typical end-user
  - The average IQ is 100
The Future of IT is not on Campus

- Campus will provide a diminishing percentage of e-services over time
  - Authentication
    - Who is taking a test online?
  - Shared data storage?
    - How do I access Google docs from campus apps?
  - Persistent data storage?
  - What does this mean for ‘integration’?
Research Problem II

• In a fundamentally distributed computing architecture how does one do intrusion detection? e.g., recognize malware in bit torrent streams?

• How can I characterize user behavior to enable detection of compromised accounts?