Please Silence All Electronic Devices

Tom, what is that annoying ringing noise?

Mike, turn off your cell phone!
Cyber Risks

DANGER

WILL ROBINSON!
How to stay completely safe
Exploit (or Attack)

An action taken against a vulnerability to harm a computer or data

Hackers exploit vulnerabilities to achieve a goal – to gain control of, damage, or bring down a device or network
Why should we care?

Why would anyone want to get into my computer?

I don’t have any important information.

Many attackers take advantage of home computers to mount their attacks
Countermeasures
Defense in Depth
Anti-Malware
Best Practice #1
Use anti-malware software

Software installed on a computer to prevent the introduction of malware. It will also detect the presence of malware and repair or remove many infected files

• Run an AV scan on a regular basis
• Make sure the program is configured properly and runs all file types
• Keep the signatures up-to-date
Any type of **malicious software** that is designed to cause damage, steal information or act in an unexpected or undesirable manner

**Virus** – Self-replicating malware requiring a host file, that depends on human action to spread it

**Worm** - Self-contained malware, needing no host file, that spreads automatically through networks

**Trojan horse** - An apparently useful and innocent application containing a hidden malicious program

**Spyware** - A general term for programs that secretly monitor your actions.
Virus: I Love You…

You replied on Thursday, May 04, 2000 9:13 AM.

From: [name removed to protect sender]                   Sent: Thu 5/4/00 8:39 AM
To: [Victim]
Cc: 
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.
Trojan Horse: Sub Seven
The SQL Slammer worm affected large networks in several large companies and municipalities on Saturday, January 25, 2003.

<table>
<thead>
<tr>
<th>Company</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank of America</td>
<td>Many ATMs unavailable on Saturday, some other financial services affected</td>
</tr>
<tr>
<td>Continental Airlines</td>
<td>Some flights delayed or cancelled because of online ticketing and electronic check-in problems</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows XP can't be activated, gamers have trouble connecting to Asheron's Call 2 and Microsoft Network access is spotty</td>
</tr>
<tr>
<td>City of Seattle</td>
<td>Emergency 911 network wasn't working</td>
</tr>
<tr>
<td>Washington Mutual</td>
<td>ATMs unavailable until Monday; other financial services affected</td>
</tr>
<tr>
<td>David-Besse Ohio Nuclear Power Plant</td>
<td>Disabled safety monitoring system for over five hours.</td>
</tr>
</tbody>
</table>
The original MSBlaster infected 1,000,000 machines and inundated networks worldwide.

Designed as a DDoS attack against Microsoft, was released less than a month after a patch was made available.

Jeffrey Lee Parson, 18, released the first "variant," which gave him remote access to 7,000 infected machines.

He included code that told the worm to send system information back to t33kid.com.

*He was caught because T33kid.com was registered in his own name at his home address.*
You May Be Infected If…

• Your computer has less memory available:
  – Operates very slowly
  – Locks up or freezes
• Your screen displays strange, unexpected graphics or text
• Your computer performs actions on its own
• Disc access light stays on
• Computer reboots itself
• Contacts tell you they have received a virus from you
K-State Antivirus Software

K-State Antivirus Software

K-Staters are required to use the university's antivirus software. This software is provided free to students, faculty, and staff.

Trend Micro OfficeScan 8.0 for Windows

All computers running a supported Windows operating system must have Trend Micro OfficeScan installed before connecting to the K-State network.

On-Campus Users
The following situations are considered a direct connection to K-State's network and require running managed security software:

- Any university-owned Windows computer
- Student-owned computers in the residence halls
- Customers of K-State's dial-up Internet service
- Users of K-State's Virtual Private Network (VPN) service
- Personal computers owned by K-State employees or students using K-State's wireless network
- Personal computers owned by K-State employees or students using K-State's wired network.

Home Users
Home users include all other windows computers connecting to the K-State network for personal use and those that use a third party Internet Service Provider.

Symantec Antivirus for Mac

On-Campus and home Mac users running Mac OS X or higher should continue to use Symantec Antivirus for the Mac.

Mac Users

Linux Workstations
Currently, Trend Micro does not have a version of the OfficeScan client software for Linux, but they are working on one. K-State will offer it as soon as it is available. Until then, Linux workstations (i.e., those functioning as a personal computer, not a server) must run an antivirus software. SIRT recommends using the freeware product ClamAV.
Mobile Use Policy

• Must use K-State provided software if you use your computer on K-State’s network

This includes:
  – Carrying a laptop onto campus
  – Connecting through VPN
  – Dial-up access to K-State
http://www.free-av.com/

(Also available free for Linux)
http://free.avg.com
Patches
Best Practice #2

Maintain up-to-date patches

Install software patches as soon as they become available

A patch is a piece of code that is inserted into a program to fix a vulnerability or to increase the functionality of the product
Why isn’t software perfect?

• Modularity
• Failure of testing
• Nobody can think of everything

The more complex the product, the bigger the risk
Turning on automatic updates

Right-click

Open
Explore
Search...
Manage
Map Network Drive...
Disconnect Network Drive...
Create Shortcut
Delete
Rename
Properties
Go to
Start >
Control Panel >
System >
Welcome to Windows Update

Get the latest updates available for your computer’s operating system, software, and hardware.

Windows Update scans your computer and provides you with a selection of updates tailored just for you.

Scan for updates

Note Windows Update does not collect any form of personally identifiable information from your computer. Read our privacy statement
### Apple Downloads

#### Mac OS X Update 10.5.1
- Delivers enhanced stability, compatibility, and security.
- [Download](www.Apple.com/SUPPORT/Downloads)

#### iPod + iTunes
- The latest iTunes and iPod software for Mac and Windows.
- [Download](www.Apple.com/SUPPORT/Downloads)

<table>
<thead>
<tr>
<th>Title/Description</th>
<th>Posted</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>iTunes 7.6 for Mac</td>
<td>01/15/2008</td>
<td>8.5MB</td>
</tr>
<tr>
<td>This is the best way to enjoy your digital music and video with your Mac, iPod, iPhone and Apple TV.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iTunes 7.6 for Windows</td>
<td>01/15/2008</td>
<td>8.5MB</td>
</tr>
<tr>
<td>This is the best way to enjoy your digital music and video with your Mac, iPod, iPhone and Apple TV.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Front Row 2.1.2</td>
<td>01/15/2008</td>
<td>16.8MB</td>
</tr>
<tr>
<td>This Front Row update provides for bug fixes and improved iTunes compatibility.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Movie 7.4.5</td>
<td>01/15/2008</td>
<td>16.8MB</td>
</tr>
<tr>
<td>This update addresses issues when publishing movies to a Mac Web Gallery, improves overall stability, and addresses a number of other minor issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuickTime 7.4 for Leopard</td>
<td>01/15/2008</td>
<td>55.8MB</td>
</tr>
<tr>
<td>This release is recommended for all QuickTime 7 users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuickTime 7.4 for Tiger</td>
<td>01/15/2008</td>
<td>51.8MB</td>
</tr>
<tr>
<td>This release is recommended for all QuickTime 7 users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuickTime 7.4 for Panther</td>
<td>01/15/2008</td>
<td>50.8MB</td>
</tr>
<tr>
<td>This release is recommended for all QuickTime 7 users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuickTime 7.4 for Windows</td>
<td>01/15/2008</td>
<td>22.8MB</td>
</tr>
<tr>
<td>This release is recommended for all QuickTime 7 users.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Software Updates


#### Featured Downloads

- **iTunes 7.5**
  - 45MB
  - 11/05/2007
- **IPod Reset Utility 1.0.2 for Windows**
  - 2.2MB
  - 7/06/2007
- **QuickTime 7.3 for Mac**
  - 50MB
  - 11/05/2007
- **Mac OS X 10.4.11 Combo Update (Total)**
  - 922MB
  - 11/14/2007
- **Mac OS X 10.4.11 Combo Update (PPC)**
  - 1.61MB
  - 11/14/2007
Windows vs. Mac

Mono-culturalism

- 91% Windows users
- 6% Mac users
- 3% others
Firewalls
Best Practice #3

Install hardware and software firewalls

Your network should be behind a hardware firewall, particularly with a high-speed connection. Install a personal firewall to block any content that the hardware may miss.
A combination of hardware and software, used to protect a network from unwelcome traffic by:

- Blocking hackers
- Blocking many worm based attacks
- Creating a single point of access to the internet
- Screening outgoing traffic
Firewalls are NOT good in preventing...

Attacks introduced through email
Internal attacks
Firewall Vendors

Software

Windows Firewall
C·O·M·O·D·O

Hardware
Connecting your new PC to the Internet without using a firewall ... is like leaving the keys in the ignition of your new, unlocked, sporty convertible – if you're lucky nothing will happen, but it's risky.

–McAfee Security
Best Practice #4
Create strong passwords

A strong password is one that has at least eight characters including letters, numbers, and other non-alphanumeric characters.

A strong password can’t be guessed and is very time-consuming to crack.
How Most Passwords Get Hacked

- Get you to tell them (social engineering)
- See it written down somewhere
- "Shoulder surfing"
- Guess (from what they know about you)
- Dictionary attacks
- Brute force hacking
Strong Password: Example

Example:

A&Bh3cnJ,P,&E.

Ann and Bob have three children named Jason, Paul, and Elizabeth.
Password Hints

If you can’t remember all your passwords, write down a HINT:

A&Bh3cnJ,P,&E. – “family”
Wireless Security
Best Practice #5
Secure your home wireless network

Ensuring that your wireless network is secure will keep prying eyes from accessing your data or using your network for nefarious means.

*By transmitting information through radio waves a Wireless LAN can make traditional security measure obsolete.*
Router

This device hooks multiple computers to one Internet connection by sending data between the Internet and the correct computer.

Consumer level routers have built in fire-walls and many act as Access Points for a Wireless LAN.
Service Set Identifier (SSID)

*The name you choose for your wireless network*

- Choosing a unique SSID and disabling the broadcast mode adds an extra level of security
- If your SSID is set to the default, that added level of security fails
Encryption

Changing the data into a form unreadable by anyone without a secret decryption key to keep the information from being intercepted

Encryption keeps intruders from eavesdropping or “sniffing” the traffic that is sent over your wireless network
Wi-Fi Protected Access 2

This latest security standard for wireless connections improves on and is expected to replace the original Wi-Fi security standard.

Newer APs are sold with WPA2 installed, while many older APs may offer a firmware update that will install WPA2.
Wardriving

Driving around with a laptop computer equipped with a wireless network card to find unsecured wireless networks
Warspamming

By logging into an unprotected wireless network, spammers can send their messages to millions of names while remaining completely anonymous.

This isn't the only way your unsecured wireless network can get you in trouble...
Does anyone have any questions about the presentation?

Yeah! Can I get the last hour of my life back?