
Paul's Top Ten Security Tips

Important Terminology

Virus - A program that is installed and run on your computer without your knowledge typically for malicious purposes.

Worm - A Virus that uses the infected computer to replicate itself across the network usually performing malicious actions.

Trojan - A Virus that disguises itself as a benign application

Backdoors - An undocumented way of gaining access to a program, online service or an entire computer system.

Vulnerability – A programming or design flaw in software that allows for a security exposure. A bug.

Exploit – Software that that takes advantage of some vulnerability in other software. Usually used to gain unauthorized access to computer(s).

Port – In the context of TCP/IP networking, a port is nothing more than an integer that uniquely identifies a path for data to travel across, or an application to listen on.

Class Information

Presentation: <http://www.pauldotcom.com/toptensecurityv33.pdf>

Instructor Email: Paul_Asadoorian@brown.edu

Instructor Web Site: <http://www.pauldotcom.com>

Course Evaluation: <http://comped.brown.edu/myevent/results.php?eventID=1016>

Exercise 1 - Patch Your Machine

Windows

- 1) Set windows update to run automatically:

Start → Control Panel → System → Automatic Updates Tab

Select “Automatic (Recommended)”, set to run at 12:00PM (or other time when you think your computer will be turned on) and click okay.

- 2) Run Windows Update manually:

Start → All Programs → Windows Update

If there are critical updates (See left hand side of the screen (, install them (click “Express Updates”)

If there are no critical updates look at optional updates and apply the ones that relate to the software installed or used on your computers (i.e. if you use Windows Media player, apply the upgrades and/or patches)

NOTE: Reboot after applying any patches!

- 3) Verify patches have installed and check for other problems by downloading the Microsoft Baseline Security Analyzer at:

<http://www.microsoft.com/technet/security/tools/mbsahome.msp>

Download and install the software, accepting the defaults during the installation and then run the MS Baseline Analyzer (Start → All Programs → MS Baseline Security Analyzer 2.1).

Click “Scan Computer” then on the next screen click “Start Scan”. Follow the recommendations for all critical items found (missing patches, running services, etc...).

Mac

- 1) Go to System Preferences → Software Update
- 2) Make certain “Check for updates” is checked and is set to “Daily”
- 3) Check “Download Updates in the background”
- 4) Click “Check Now” to be certain you are up to date

5) Close all windows

- * If you have Adobe Acrobat or WinZip installed note which version is installed. Use the web to determine if you need your software updated, and if so, update it.
- * Configure you security center to monitor Auto updates, Anti-Virus Software, and Firewall. Disable these services and see how it reacts.

Exercise 2 – Use a Firewall

1) Check the status of your windows XP firewall, make certain its “On”

Windows

- a) Start → Control Panel → Network Connections
- b) Right click on “Local Area Connection” and go to properties, advanced tab
- c) In the “Windows Firewall” section click “Settings...”
- d) Click the radio button next to “ON”, click okay

Mac

- a) Go to System Preferences → Sharing → Firewall
- b) Be certain it says firewall is “On”
- c) Make certain that no boxes are checked unless you specifically allow that service (port).
- d) BONUS: Using the following command, view your firewall rules in a terminal window:

```
paimel:~ root# ipfw list
02000 allow ip from any to any via lo*
02010 deny ip from 127.0.0.0/8 to any in
02020 deny ip from any to 127.0.0.0/8 in
02030 deny ip from 224.0.0.0/3 to any in
02040 deny tcp from any to 224.0.0.0/3 in
02050 allow tcp from any to any out
02060 allow tcp from any to any established
02070 allow tcp from any to any 22 in
02080 allow tcp from any to any 5900-5902 in
```

```
12190 deny tcp from any to any
65535 allow ip from any to any
```

NOTE: You must have system privileges to run this command. Open a terminal window and type the following:

```
paimei:~ username$ sudo -s
Password:
paimei:~ root#
```

Your instructor will provide the password to you. The prompt should change from a "\$" to a "#" as seen above.

2) Test your firewall

- a) Go to <https://grc.com/x/ne.dll?bh0bkyd2> and click "Proceed".
 - b) On this page click the "All Services & Ports" link.
 - c) If your firewall is configured properly you will see all "Green".
- * Download and install Zone Alarm. Notice what happens every time an application attempts to use the network.
 - * Open a port in your firewall and see if the test in question 3 produces different results.

Exercise 3 – Use Anti-Virus Software (Symantec Anti-Virus version 9.0)

Windows (Only):

- 1) Enable automatic updates as often as possible
 - a) In the system tray portion of the Taskbar (typically on the lower right of your screen), you can right-click the Norton/Symantec Antivirus icon (which looks like a shield) and select Open Norton/Symantec Antivirus....
 - b) From the File menu, choose Schedule Updates....
 - c) Make sure the box labeled "Enable scheduled automatic updates" is checked. Click Schedule... .
 - d) You can now schedule a specific time for updates to occur. UITS recommends setting the "Frequency" to Daily and choose a time when your computer is most likely to be turned on. Click OK when done.

- 2) Schedule a nightly virus scan
 - a) Launch NAV/SAV as described above.
 - b) From the Edit menu, choose New Scheduled Scan.
 - c) In the field labeled "Name:", type the name of this scan (for example, Daily Scan). Click Next.
 - d) Make sure that the box labeled Enable scan is checked. You can now schedule how often and at what time of the day you want the scan to occur. Choose a time when your computer is most likely to be turned on. Click Next when done.
 - e) You can now select what drives you want to scan. Check the box next to each drive you want to scan (preferably all). The Options... button will allow you to configure what file types you wish to scan and what actions you wish to take upon finding a virus, quarantining all the viruses is a good option.
 - f) Click Save to finish scheduling your virus scan.
- * Go to <http://securityresponse.symantec.com/> and read the top 5 latest virus descriptions. Note the threat level, and what it does to your computer. Rest easier tonight knowing you've installed and updated your anti-virus client.

Exercise 4 – Use Good Passwords

- 1) Think of a new, good password (Do not enter any of your current passwords!). Go to <http://www.securitystats.com/tools/password.php> and see how it ranks. Never use this password again.
- 2) Where is the best place to store your password?
 - a) On a sticky note
 - b) On paper under the mousepad
 - c) In your head
 - d) On paper in your wallet
 - e) Written on your whiteboard
- 3) True/False – If someone claiming to be a network administrator asks you for your password you should give it to them?
- 4) True/False – Your password should contain your pet names, family members, birthdays, and nicknames so they are easy to remember.

Exercise 5 – Use An Alternate Web Browser

Windows (Only):

Create a shortcut to open a web site in IE:

- 1) Right click on IE Icon, click copy, then paste it somewhere (desktop, quick launch bar)
 - 2) Right click on the new icon and click properties. In the target field append the web site after "explorer.exe", using a space in between.
 - 3) Click the Change Icon button and choose a new icon
 - 4) Go to the general tab and enter a new name then click OK.
 - 5) Double click on the icon and enjoy!
- * Download an alternate browser and import your bookmarks. Bonus: If you downloaded Firefox (<http://www.mozilla.org/firefox>), install any of the four plug-ins mentioned and test them out.

Exercise 6 – Share Your Resources Responsibly

Windows:

- 1) Open Windows Explorer (Start → All Programs → Accessories → Windows Explorer)
- 2) Go to My Computer, C Drive.
- 3) Create a new folder called "Shared Files"
- 4) Right click on the new "Shared Files" folder and go to properties, Sharing Tab
- 5) Click "Share this folder on the network", type a name for the share in the box, click OK
- 6) Note the icon for the folder changes
- 7) Go back into the properties for the "Shared Files" folder, and go to sharing.
- 8) Remote sharing from this folder by unchecking the "Share this folder on the network"
- 9) Click okay
- 10) Notice that the icon changes yet again

11) Delete the folder (right click, delete)

Mac

1) Open a terminal window and type the following command:

```
$ smbclient -I localhost -L `hostname` -N
```

View the results. Note if you are sharing anything you don't want to.

2) Go to System Preferences → Sharing

3) Note any of the sharing options that you have checked. These include "Windows Sharing", "Personal File Sharing", and "Printer Sharing". Do you really want to share stuff? If not, uncheck these boxes.

Exercise 7 – Secure Your Wireless

Make certain you are not an access point

Windows:

- 1) Start → Control Panel → Network Devices
- 2) Right click on your wireless adapter and go to properties
- 3) Go to the advanced tab
- 4) Make certain that the checkbox labeled "allow other network users to connect through this computer's Internet connection" is UNCHECKED.

Mac:

- 1) In the wireless pulldown menu be certain never to "Create Network..."
- * Download NetStumbler or MacStumbler
 - <http://www.netstumbler.com/>
 - <http://www.macstumbler.com/>
 - Note access points in your area
 - Do they have encryption enabled?
 - How is the signal?
 - What is the SSID?

All:

Configuring WPA:

<http://www.brown.edu/Facilities/CIS/itsecurity/news/05-002.html>

Exercise 8 – Use Anti-Spyware tools

Download, install, and run MS Anti-Spyware Tool

1) Go to:

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

and follow the instructions to download the software

2) Install the software, following the prompts (accept all the defaults)

3) Run the tool and have it find spyware on the system