



Wireless Security

Bill Clayton

**IEEE Senior Member
Region 3 Communications Committee**

Disclaimer

Sophisticated attacks possible

Social engineering happens

Day Zero attacks possible

Not intended for high value targets

Government

Medium – Large Business

Outline

Why?

Computer Security

Home Wireless

Wireless Hotspots

Sources and Resources

<http://www.ieee.org/hrs/>

Why Computer Security?

Why my computer?

How can they do it?

How long does it take?

Why Wireless Security?

Why my wireless access point?

How can anyone get to my access point?

What about public hot spots?

Computer Security

Firewalls

Strong passwords

Security patches.

**Share files
correctly**

Antivirus software

Spyware scanner

Minimize services

Limit Admin

Backup often

**Analyze your
security**

Analyze Your Security

Shields Up

<https://grc.com/x/ne.dll?bh0bkyd2>

Microsoft Baseline Security Analyzer

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

Home Wireless

Turn off SSID broadcast

Unique SSID

Use Encryption

WAP w/ TKIP

Use a strong key

26 Characters

Turn off when inactive

Wireless Hotspots

Use a personal firewall

Turn off all shares

Do not auto-connect

Encrypt your session

Do not accept untrusted certificates

Sources

Virginia Tech <http://www.security.vt.edu/>

Microsoft Security <http://www.microsoft.com/>

Stanford University <http://pangea.stanford.edu/>

Duke University <http://www.oit.duke.edu/>

Gibson Research <http://grc.com/>

Network World Fusion <http://www.nwfusion.com/>

Greg Sherrock, TDS

James Bohling, USJFCOM

Resources

NIST CSRC

<http://csrc.nist.gov/pcig/cig.html>

SANS Reading Room

<http://www.sans.org/rr/>



Questions

Backup Slides

Firewalls

XP Firewall

Passwords

Patches

File Shares

AV Software

Spyware

Services

Limit Admin

Backup

Firewalls.

Home style Firewall – Router

Network Address Translation

Blocks inbound ports

Personal Firewall

Controls access to ports by applications

Use carefully

Windows XP Internet Connection Firewall

You MUST have administrator access to your computer

- 1. Click on the Start button.**
- 2. Select Settings then Network Connections.**
- 3. Inside the Network Connections window, right-click on one network connection.**
- 4. Select Properties.**
- 5. Select the Advanced tab and check the box about protecting my computer.**
- 6. Click OK and return to step 3 until all connections are fire walled.**

Additional detailed instructions are at:

<http://www.microsoft.com/security/protect/windowsxp/firewall.asp>

Windows 2000

No windows ICF

If not using hardware firewall (e.g. Linksys Router), download one of the following products:

BlackICE PC Protection

<http://blackice.iss.net/microsoft.php>

McAfee Security

<http://us.mcafee.com/root/campaign.asp?cid=8437>

Symantec <http://www.symantecstore.com/BlasterProtect>

Tiny Software: Tiny Personal Firewall

<http://www.tinysoftware.com/home/tiny2?la=EN>

ZoneAlarm

<http://download.zonelabs.com/bin/promotions/microsoftsecurity/>

Strong passwords!

Minimum 8 characters

Increase character entropy

Mix lower and upper case

Use numbers and punctuation

Hard to guess – use pass phrase

Ti1rgpw!

Ti1rgpw!

Security patches.

Install critical security patches often.
New security bugs discovered daily.
Software out-of-date when you get it
Becomes increasingly less secure over time
Vendors provide patches to fix security bugs
You download and install

Windows Update

Login as "Administrator", or administrative privileges,
Internet Explorer to connect to the Windows Update web
site: <http://windowsupdate.microsoft.com>
Other vendors have similar services.

Share files correctly.

Enabled shares require accounts and passwords.

Not the Windows default setting.

Takes work to set up.

Need synchronize the account names and passwords on both the 'server' Windows computer and the 'client' Windows computer

OR

Turn Off File Sharing (see below).

Disable 'File and Printer Sharing' in Windows 98/ME:

- 1. Right-click on the Network Neighborhood icon on your desktop.**
- 2. Select Properties from the pop-up menu.**
- 3. Click the File and Print Sharing button.**
- 4. If I want to be able to give others access to my files is checked, you have enabled file sharing. Uncheck it.**
- 5. If I want to be able to allow others to print to my printer(s) is checked, you have enabled print sharing. Uncheck it.**
- 6. Click OK.**
- 7. Insert your Windows CD if prompted.**
- 8. Click OK.**
- 9. Restart your computer.**
- 10. File and print sharing is now off.**

Disable 'File and Printer Sharing' in Windows 2000/NT:

- 1. Right-click on My Network Places on your desktop and select Properties.**
- 2. Right-click on Local Area Connection and select Properties.**
- 3. Under Components checked are used by this connection, look for File and Printer Sharing for Microsoft Networks. If it is not listed, you are not sharing. If it is in the list:**
 - 1. Click in the check box next to File and Printer Sharing for Microsoft Networks to unselect it.**
 - 2. Click OK.**

Note: File and Printer Sharing will not be enabled when you restart your computer. In order to re-enable it, you must go back and click in the check box next to File and Printer Sharing to select it.

Disable 'File and Printer Sharing' in Windows XP:

- 1. Open Control Panels from the Start menu**
- 2. Double-Click Network Connections (under Network and Internet Connections in XP Category View).**
- 3. Right-click on Local Area Connection and select Properties. In the middle of the properties window, you will see the list of networking components used by this connection.**
- 4. If File and Printer Sharing for Microsoft Networks is listed, uncheck the item and click OK. This change goes into effect immediately.**

Antivirus software.

Symantec <http://symantec.com/>

McAfee <http://us.mcafee.com/>

Trend Micro

<http://www.trendmicro.com/>

Spyware scanner.

Ad-aware

<http://www.lavasoftusa.com/software/adaware>

Not Windows 95 compatible

Spybot <http://security.kolla.de/>

Be sure these programs stay updated.

Minimize services

No unnecessary network.

Every additional service = possible security hole for a hacker to find.

Key examples:

Windows Messenger / WinPopUp

Internet Information Server (IIS)

Universal Plug and Play

Messenger¹ Service on

Windows 2000 or XP

Open the list of services running on your computer.

1. Open Control Panels from the Start menu (under Settings in Windows 2000).
2. Double-click on Administrative Tools (inside Performance and Maintenance in Windows XP),
3. Double-click on Services.

Scroll down the list of services on the right until you find Messenger.

1. Double-click Messenger; a Messenger Properties window opens.
2. The General tab window should be selected.
3. Click the Stop button under Service Status if the service is currently running.

In the center of the window, there is a Startup Type drop-down menu. By default, the menu is set to Automatic. Instead, Select Disabled so the service will never start again.

1. Click the OK button in the Messenger Properties window.
2. Close the Services window.

Windows 95/98 WinPopUP

Add/Remove programs Control Panel to see if WinPopUp is installed; if so, remove it.

Note 1: This is not MSN Messenger

Remote Registry Service

Windows 2000 and XP users should also disable the built-in Remote Registry Service. This service can allow hackers to modify your registry remotely.

To disable this Remote Registry Service on Windows 2000 or XP, follow these steps:

Open the list of services running on your computer.

- 1. Open Control Panels from the Start menu (under Settings in Windows 2000).**
- 2. Double-click on Administrative Tools (inside Performance and Maintenance in Windows XP),**
- 3. Double-click on Services.**

Scroll down the list of services on the right until you find Remote Registry Service.

- 1. Double-click Remote Registry Service; a Remote Registry Service Properties window opens.**
- 2. The General tab window should be selected.**
- 3. Click the Stop button under Service Status if the service is currently running.**

In the center of the window, there is a Startup Type drop-down menu. By default, the menu is set to Automatic. Instead, Select Disabled so the service will never start again.

- 1. Click the OK button in the Remote Registry Service Properties window.**
- 2. Close the Services window.**

Additional Information

Disable file sharing.

Remove or harden Microsoft's Internet Information Services (IIS)

FTP

Web server

Windows NT, 2000, or XP

Disable Windows XP Universal Plug and Play

UnPlug and Pray <http://grc.com/unpnp/unpnp.htm>

Limit Admin

Separate Admin and User accounts

User should not be able to install software

Windows 2000, XP

“Run as” command to install software from user account

Backup often.

Nothing is fool proof

Sophisticated attacks

Social Engineering

Day Zero attacks

Back up data

Reinstall software applications from CD

Don't forget license keys

Store in a safe place

Physically secure

Air conditioned / heated