Beginning Open-Source/Free Solutions for Home and Small Business Owners

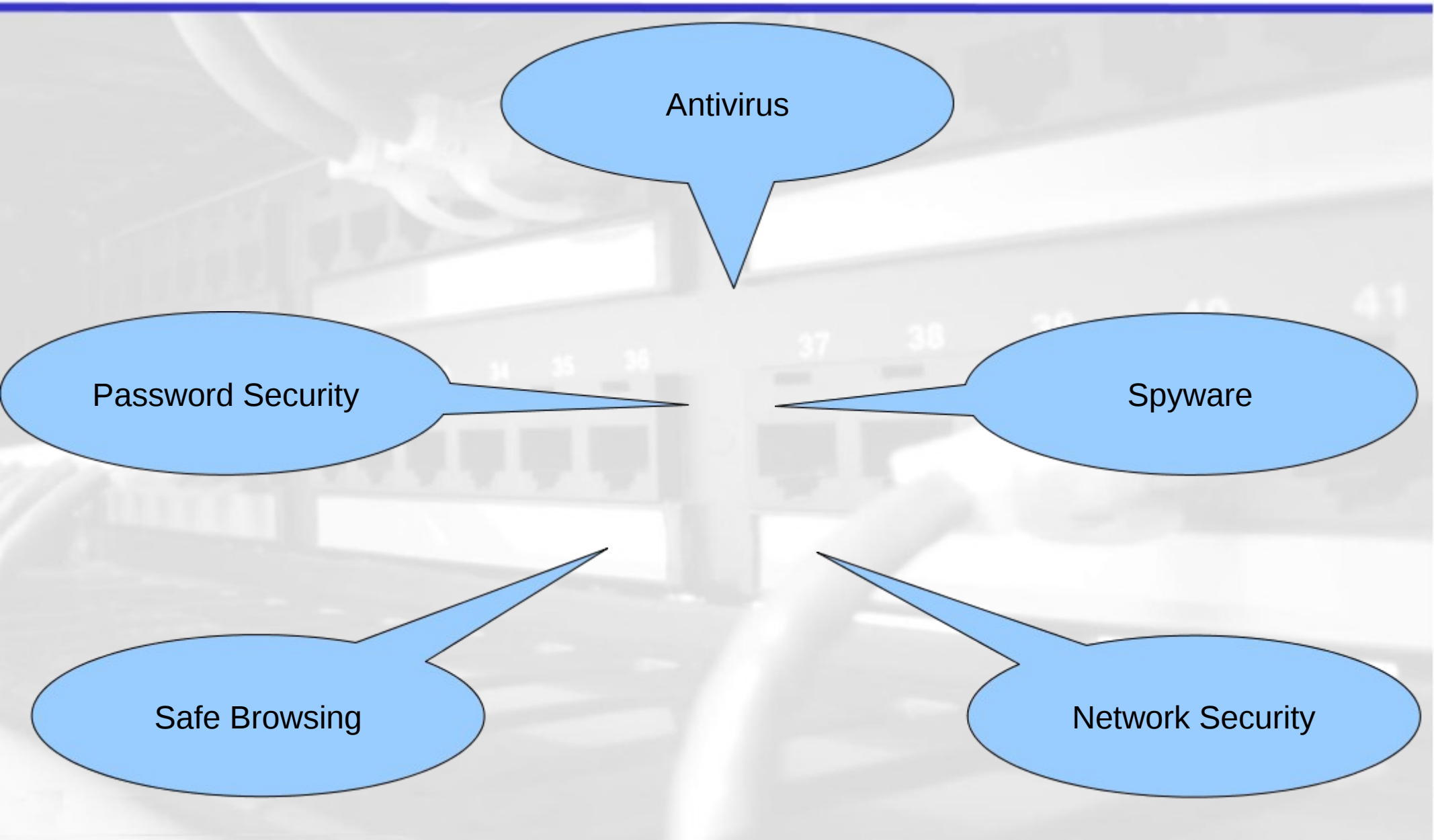
Robert Baldi, CISSP-ISSEP
Robert Clauff




Open source….Efficient ….Secure




TOPICS


Antivirus
Password Security
Spyware
Safe Browsing
Network Security

ANTIVIRUS

- It is a good start to have antivirus on every computer in your network to keep you virus free
- Growing numbers of viruses and new definitions of viruses are being released everyday
- If you choose to go to a Enterprise edition you may have to pay for a license, but depending on the number of computers in the network it should still be affordable
- There are more than a couple free antivirus applications to keep your network free of viruses
- Antivirus is only one piece of the puzzle when you are securing either your home or office network

Avast Antivirus

- Great free home edition antivirus
- Free signature updates
- Real time protection
- Web and P2P Protection
- Anti-spyware and anti-rootkit tools
- Available for linux as well for free
- Professional and small business versions for a small fee, but still affordable

http://www.avast.com

AVG Antivirus

- Real time protection and web surfing protection
- Spyware protection
- Compatible for Windows 7, Vista, and XP
- Just like others this is only for home use and not commercial.

http://free.avg.com

Clamwin or Clamav

- Features include integration with Outlook and internet explorer
- Schedule automatic scans
- Automatically updates virus databases
- Easy to update to newer versions with just one click
- Compatible with both Windows and Linux

http://www.clamwin.com/

Clamwin

http://www.clamwin.com/

SECURED BROWSING

- The first step to securing yourself from viruses and spyware is to avoid it in the first place
- By making yourself secure during browsing you add another layer to your security
- There are applications to secure your browser as well as plugins for your browser directly

Browser Plugins

- Browsers have hundreds of available plugins to increase your security during browsing
- Plugins are all free and have a large range of abilities
- New plugins are getting released everyday
- Since there are differences between browsers we will cover a few for firefox

http://www.microsoft.com/windows/internet-explorer/default.aspx

http://firefox.com

Mozilla Plugins

- NoScript – This prevents scripts in websites from running unless you allow them to

- Show MyIP – This shows you your current address

- Firebug – This plugin will troubleshoot code on the website

- Ghostery – Watches the scripts and cookies that are tracking you

https://addons.mozilla.org/en-US/firefox/

Sandboxie

- Secures web site browsing
- Creates a quarantine area on harddrive
- Privacy is assured by "sandboxing" all history, cookies, and temp files
- Malware infection is isolated from your host system
- Run programs securely as well

http://sandboxie.com

Sandboxie

SPYWARE

- Spyware is a growing problem on the internet today
- Spyware is very, very common and everyone gets a little bit
- These are gateways to worse problems then just slowing down a PC
- Spyware can open security holes, monitor your PC, and slow your PC to a standstill
- Getting rid of spyware is just another layer that you can add to secure your PC and your network
- Most free tools are as efficient if not more efficient than most paid applications

Malwarebytes

- Lightspeed scanning
- Works in tandem with other spyware applications
- Tools for manual, hard to remove malware
- Command line operability for faster scans
- Paid version offers Anti-malware, real-time
- Works with 32 and 64 bit Windows systems up through Vista

http://www.malwarebytes.org

Ad-Aware

- Basic integrated real-time protection
- Fully integrates with Windows security center
- Quick scan, remove, and clean
- Rootkit removal
- External drive scanability
- Very easy to use

http://www.lavasoft.com/products/ad_aware.php

Spybot Search & Destroy

- Stops spyware in real-time and “immunizes” all the ways spyware can enter your system
- Can prevent and will alert you if any programs are allowed to install or change the registry
- Removes spyware, adware, and hijacks that aren't sometimes covered by antivirus definitions
- Works with Windows Vista

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

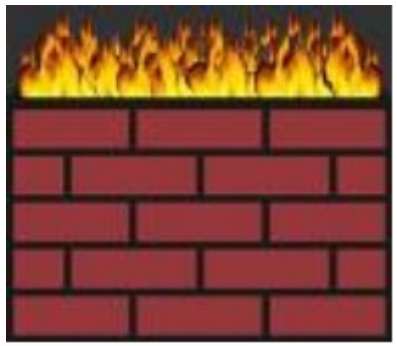
Spybot Search & Destroy

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

NETWORK SECURITY

- Keeping your network secure and monitored allows you to secure the biggest part of your network
- The main gateway to your security is through the outside of your network and keeping the network secure inside
- With an efficient firewall and quality network elements you should be able to keep a lock down on your network

FIREWALLS



- The most efficient way to secure a network is by putting a quality firewall at the edge of your network
- Firewalls are also a great way to secure other applications and the ability to remotely access your systems
- Despite what is said you do not need to spend a lot of money to get a quality firewall for your network

Pfsense

- Open source stateful firewall that is forked from the MoNowall project
- Several filtering options
- Plugins available for different applications
- Load balancing and VPN
- Available as a standalone install, image (for smaller hardware), or vmware appliance
- Real time monitoring and MORE
- Fantastic firewall, our personal favorite

http://www.pfsense.org

Untangle

- Open source network gateway
- Can be installed on top of a Windows machine
- Open source package available for firewall, spam-filtering, and more
- Can be setup as a router, transparent bridge, or a re-router
- Can run on bare metal install, XP, or as a vmware appliance
- More detailed apps with paid subscriptions

http://www.pfsense.org

NETWORK APPLICATIONS

- Good network applications inside of your network help you keep things secure and keep unwanted people out
- Some network applications will not only help secure the network, but make operations and administration easier
- There are numerous free applications to choose from if you go to sourceforge.net for both Linux and Windows

Wireshark

- Network protocol analyzer for both Linux and Windows
- Scans network collecting all packets to be later analyzed
- Supports hundreds of protocols
- TCPDUMP output can also be analyzed in wireshark
- Easily filterable and manipulated
- Great for troubleshooting network problems

http://www.wireshark.org

Lansweeper

- Inventory network clients including Active Directory integration
- Lansweeper allows you scan machines remotely without installing agents
- Locate non-compliant programs
- Track licenses and inventory or generate reports via SQL

http://www.lansweeper.com

Lansweeper

http://www.lansweeper.com

PASSWORD SECURITY

- One of the most common things that put a network at risk is not having secure passwords
- If you have a lot of passwords the worst thing you can do is save them in a browser or something else
- Having a way to securely log the passwords is a very good practice to have

KeePass

- A secure password manager
- Requires only one master password to open the database
- AES or Twofish Encryption

http://www.keepass.info

KeePass

http://www.keepass.info

Security

- This brief overview of the security concepts that we have covered today will drastically improve the security of your network
- All of the tools that we covered today will be distributed out on a DVD for you to use at your leisure (accept the OS firewalls)
- Hopefully the things we covered today were of interest to you and make you want to focus more on your security for you and your data
- The things we didn’t show tutorials on today do have great documentation at their websites as well.