Securing Your Home Network

Part I

How a Home Network Works
Threats to Your Devices and Information
Managing Vulnerabilities & Threats

Cyber Security Month Presentation,
October 4th, 2012
Curtis McNay - Director, IT security
How To Understand the Risk

- **Example Drive-By-Download Infection**
  - Forensic breakdown of an actual attack
    - User Browses to malicious site
    - User is manipulated to take an action: could have been responding to a informational dialogue box.
    - User has admin rights on the system
    - Insecure browser setting allows java code to be run with full access
The Vulnerabilities & Threats (V&T)

- **The Threat**
  - **Who are the Hackers**
    - Sophisticated, resourceful crime organization primarily in Eastern Europe, Russia, and Asia
    - State or Nation Sponsored industrial or governmental espionage
    - Someone who has taken a persona interest in you
    - Property thief
  - **What Motivates Hackers**
    - Financial gain, financial gain and financial gain
    - Occasionally industrial or governmental espionage is motivation
    - Occasionally the motivation is personal
    - For physical theft the motivation can be data theft, access and resale of hardware
  - **Vulnerabilities**
    - Your behavior online
    - Unpatched or unknown operating system, software or device vulnerabilities
    - Insecure Configuration
    - unprotected Sensitive Data
    - Exposure to physical theft
Assessing & Mitigating the Risk

- What is the easiest way for the hackers to get what they most desire. What do you have that they Want.
  - The Weakest Link
    - Exploiting Human Behavior
    - Exploiting System Vulnerability
    - Physical Theft
  - The Valuables
    - Information: Credit Card, SSN #, Identity, Contact Lists
    - Access: Your financial, social, cloud storage accounts
    - The reuse of your computer or device to target someone else.
    - The hardware and it’s resale value.
Your Home Network

The Internet or The New Wild Wild West

Internet Service Provider

Internet Provider Modem

Your ISP is providing a valid internet Address to your Modem

Home Multifunction Wireless Access Point (WAP)

All of these devices are getting Internal (IP) addresses

IP Phone

Wireless Printer

Windows PC

Android or IOS Tablet

IMAC

IOS or Android Smartphone

Apple or Windows Laptop

Wireless Storage Device
The Pieces that Stay at Home

- **ISP Modem/Wireless Access Point (WAP)**
  - Provide Internet connection and internal addresses
  - Provides Wireless Access (WEP, WPA2, SSID)
  - Provide logical separation between home net and Internet
  - V&T: Wardriving, exploiting unpatched vulnerability, theft of encryption key, resulting in home network access & control

- **Windows or Apple Workstation**
  - Stays at home, it’s fixed in place
  - V&T: Drive-by-Download, unpatched vulnerability, infected removable media resulting in data theft, access, system control

- **Wireless Printer**
  - Usually is running Web server, it may also have vulnerabilities
  - V&T: Unpatched vulnerability, default admin access resulting in data theft, device control

- **Wireless Storage**
  - Usually an appliance network file server device
  - Usually Linux, may be proprietary.
  - V&T: Unpatched vulnerability, default admin access, resulting data theft.

- **IP Phone**
  - Voice over IP (VoIP): Provide traditional telephone like service over the internet
  - V&T: Unpatched hardware or software, resulting in capture and replay of communication
The Pieces that Can Travel

- **Windows or Apple Laptop**
  - It will be exposed to multiple external networks
  - Physical theft risk increases information theft risk.
  - V&T: Drive-by-Download, unpatched vulnerability, infected removable media, exposure to insecure networks resulting in data theft, access, system control, physical theft

- **Apple or Android Tablet**
  - Like a laptop may move to exposed networks
  - Simpler, less secure operating systems
  - Same theft risk as a laptop.
  - V&T: Drive-by-Download, unpatched vulnerability, infected removable media, exposure to insecure networks resulting in data theft, access, system control, physical theft

- **Apple or Android Smartphone**
  - Same threat profile as a tablet
  - Same or greater theft risk as a laptop.
  - V&T: Drive-by-Download, unpatched vulnerability, infected removable media, exposure to insecure networks resulting in data theft, access, system control, physical theft
Mitigating Risk: What Can You Do

- Migrate to a Modern Operating System and Hardware
  - Window 7 or latest Mac OS X build
    - 64 bit OS on hardware that supports 64 bit
  - At this time, android and Apple iOS tablets and smartphones do not have significant security at the OS layer
- Install a comprehensive Host-Based Security Suite
  - Firewall, Host Intrusion Prevent, and Antivirus
- Limit Use of the Administrator Account- Create a standard user account and use it for most of what you do
Account & Password Management

- Use a secure password
  - Length first, then complexity
    - At least 10 characters,
    - Mixed alphanumeric, upper/lower and special characters
- Use a password safe to store your passwords.
- Use different passwords for different accounts
  - Mitigates threat of chain link attacks
Web Browser Security

• **Understand what risky behavior is**
  • What is an untrusted web sites
  • Don’t click that button-FakeAV
  • Downloading plugins and add-ons

• **Learn how to secure your internet browser**
  • Manage plugins
  • Keep plugins patched
    • 40 percent of drive-by-downloads exploit unpatched vulnerabilities in Adobe Flash and PDF reader
  • Disable Java, JavaScript and ActiveX
    • Or, for browsers that support it, enable for web sites that you trust
Email and “Other” Security

- Identifying Malicious Email
  - If the email is from your mom and the subject is “Topless photos of Kate Middleton”. Context is important.
  - Know what a phishing attack is and how to identify it.
  - Don’t open the email, don’t respond to the email
  - Disable scripts in email client

- Any application that allows for downloading files
  - Instant Messaging, Social Media, BitTorrent, etc.
    - Downloading untrusted files is a high risk behavior
Questions? Thanks!

- Securing your home network Part II,
  - How to actually put the controls in place and
  - How to recover from an event.