Best Practices for Keeping Your Home Network Secure

The cyber threat is no longer limited to your office network and work persona. Adversaries realize that targets are typically more vulnerable when operating from their home network since there is less rigor associated with the protection, monitoring, and maintenance of most home networks. Home users need to maintain a basic level of network defense and hygiene for both themselves and their family members when accessing the Internet.

Host-Based Recommendations

Windows Host OS

1. Migrate to a Modern OS and Hardware Platform

Both Windows 7 and Vista provide substantial security enhancements over earlier Windows workstation operating systems such as XP. Many of these security features are enabled by default and help prevent many common attack vectors. In addition, implementing the 64-bit mode of the OS on a 64-bit hardware platform substantially increases the effort of an adversary to attain a system or root compromise. For any Windows-based OS, verify that Windows Update is configured to provide updates automatically.

2. Install a Comprehensive Host-Based Security Suite

A comprehensive host-based security suite provides support for anti-virus, anti-phishing, safe browsing, Host-based Intrusion Prevention System (HIPS), and firewall capabilities. These services work collaboratively to provide a layered defense against most common threats. Several security suites today provide access to a cloud-based reputation service for leveraging corporate knowledge and history of malware and domains. Remember to enable any automated update service within the suite to keep signatures up-to-date.

3. Limit Use of the Administrator Account

The first account that is typically created when configuring a Windows host for the first time is the local administrator account. A non-privileged "user" account should be created and used for the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and reconfigure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host. Within Vista or Windows 7, administrative credentials can be easily accessed by right clicking on any application, selecting the "Run as Administrator" option, then providing the appropriate administrator password. Furthermore, all passwords associated with accounts on the host should be at least 10 characters long and be complex (include upper case, lower case, numbers, special characters).

4. Use a Web Browser with Sandboxing Capabilities

Several currently available third party web browsers now provide a sandboxing capability that can contain malware during execution thereby insulating the host operating system from exploitation. Most of these web browsers also provide a feature to auto-update or at least notify you when updates are available for

download. Also, promising approaches that move the web browser into a virtual machine (VM) are starting to appear on the market but are not yet ready for mass consumer use.

5. Update to a PDF Reader with Sandboxing Capabilities

A sandbox provides protection from malicious code that may be contained in a PDF file. PDF files have become a popular technique for delivering malicious executables. Several commercial and open source PDF readers now provide sandboxing capabilities as well as block execution of embedded URLs (website links) by default.

6. Migrate to Microsoft Office 2007 or Later

If using Microsoft Office products for email, word processing, spreadsheets, presentations, or database applications, upgrade to Office 2007 or later and its XML format for storing documents. By default, the XML file formats do not execute embedded code when opened within Office 2007 or later products thereby protecting the user from malicious code delivered via Office documents. The Office 2010 suite also provides "Protected View" mode which opens documents in read-only mode thereby potentially minimizing the impact of a malicious file.

7. Keep Application Software Up-to-Date

Most home users do not have the time or patience to verify that all applications installed on their workstation are fully patched and up-to-date. Since many applications do not have an automated update feature, attackers frequently target these applications as a means to exploit a targeted host. Several products exist in the market which will quickly survey the software installed on your workstation and indicate which applications have reached end-of-life, require a patch, or need updating. For some products, a link is conveniently provided in the report to download the latest update or patch.

8. Implement Full Disk Encryption (FDE) on Laptops

Windows 7 Ultimate as well as Vista Enterprise and Ultimate provide support for Bitlocker Full Disk Encryption (FDE) natively within the OS. For other versions of Windows, third party FDE products are available that will help prevent data disclosure in the event that a laptop is lost or stolen.

Apple Host OS

1. Maintain an Up-to-Date OS

Configure any Mac OS X system to automatically check for updates. When notified of an available update, provide privileged credentials in order to install the update. The Apple iPad should be kept up-to-date as well and requires a physical connection (e.g., USB) to a host running iTunes in order to receive its updates. A good practice is to connect the iPad to an iTunes host at least once a month or just prior to any travel where the iPad will be used.

2. Keep Third Party Application Software Up-to-Date

Periodically check key applications for updates. Several of these third party applications may have options to automatically check for updates. Legacy applications may require some research to determine their status.

3. Limit Use of the Privileged (Administrator Account)

The first account that is typically created when configuring a Mac host for the first time is the local administrator account. A non-privileged "user" account should be created and used for

the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and reconfigure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host.

4. Enable Data Protection on the iPad

The data protection feature on the iPad enhances hardware encryption by protecting the hardware encryption keys with a pass code. The pass code can be enabled by selecting "Settings," then "General", and finally "Pass code." After the pass code is set, the "Data protection is enabled" icon should be visible at the bottom of the screen. For iPads that have been upgraded from iOS 3, follow the instructions at: http://support.apple.com/kb/HT4175.

5. Implement FileVault on Mac OS Laptops

In the event that a Mac laptop is lost or stolen, FileVault (available in Mac OS X, v10.3 and later) can be used to encrypt the contents of a user's home directory to prevent data loss.

Network Recommendations

1. Home Network Design

The Internet Service Provider (ISP) may provide a cable modem with routing and wireless capabilities as part of the consumer contract. To maximize the home user's administration control over the routing and wireless device, deploy a separate personally-owned routing device (a) that connects to the ISP provided router/cable modem. Figure 1 depicts a typical home network configuration that provides the home user with the network infrastructure to support multiple systems as well as wireless networking and IP telephony services (b).

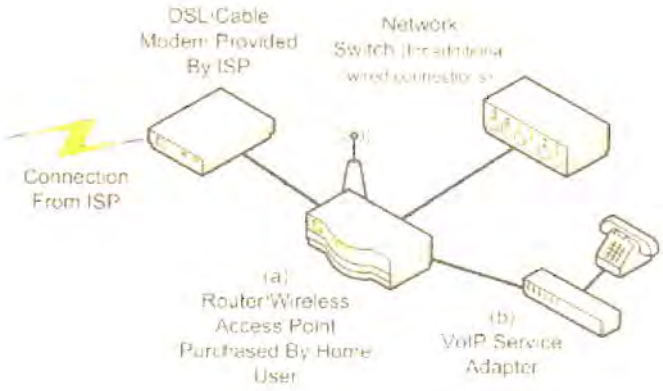

Figure 1: Typical SOHO Configuration

2. Implement WPA2 on Wireless Network

The wireless network should be protected using Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy). Using current technology, WEP encryption can be broken in minutes (if not seconds) by an attacker, which afterwards allows the attacker to view all traffic passed on the wireless network. It is important to note that older client systems and access points may not support WPA2 and will require a software or hardware upgrade. When researching for suitable replacement devices, ensure that the device is WPA2-Personal certified.

3. Limit Administration to Internal Network

Administration of home networking devices should be from the internal-facing network. When given the option, external remote administration should be disabled for network devices. Disabling remote administration prevents an attacker from changing and possibly compromising the home network.

4. Implement an Alternate DNS Provider

The Domain Name Servers (DNS) provided by the ISP typically don't provide enhanced security services such as the blocking and blacklisting of dangerous and infected web sites. Consider using either open source or commercial DNS providers to enhance web browsing security.

5. Implement Strong Passwords on all Network Devices

In addition to a strong and complex password on the wireless access point, a strong password needs to be implemented on any network device that can be managed via a web interface. For instance, many network printers on the market today can be managed via a web interface to configure services, determine job status, and enable features such as email alerts and logging.

Operational Security (OPSEC)/Internet Behavior Recommendations

1. Traveling with Personal Mobile Devices

Many establishments (e.g., coffee shops, hotels, airports, etc.) offer wireless hotspots or kiosks for customers to access the Internet. Since the underlying infrastructure is unknown and security is often lax, these hotspots and kiosks are susceptible to adversarial activity. The following options are recommended for those with a need to access the Internet while traveling:

a. Mobile devices (e.g., laptops, smart phones) should utilize the cellular network (e.g., mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.

b. Regardless of the underlying network, users can setup tunnels to a trusted VPN service provider. This option can protect all traffic between the mobile device and the VPN gateway from most malicious activities such as monitoring.

c. If using a hotspot is the only option for accessing the Internet, then limit activities to web browsing. Avoid accessing services that require user credentials or entering personal information.

Whenever possible, maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time. If a laptop must be left behind in a hotel room, the laptop should be powered down and have Full Disk Encryption enabled as discussed above.

2. Exchanging Home and Work Content

Government maintained hosts are generally configured more securely and also have an enterprise infrastructure in place (email filtering, web content filtering, IDS, etc.) for preventing and detecting malicious content. Since many users do not exercise the same level of security on their home systems (e.g., limiting the use of administrative credentials), home systems are generally easier to compromise. The forwarding of content (e.g., emails or documents) from home systems to work systems either via email or removable media may put work systems at an increased risk of compromise. For those interactions that are solicited and expected, have the contact send any work-related correspondence to your work email account.

3. Storage of Personal Information on the Internet

Personal information which has traditionally been stored on a local computing device is steadily moving to the Internet cloud. Examples of information typically stored in the cloud include webmail, financial information,

and personal information posted to social networking sites. Information in the cloud is difficult to remove and governed by the privacy policies and security of the hosting site. Individuals who post information to these web-based services should ask themselves "Who will have access to the information I am posting?" and "What controls do I have over how this information is stored and displayed?" before proceeding. Internet users should also be aware of personal information already published online by periodically searching for their personal information using popular Internet search engines.

4. Use of Social Networking Sites

Social networking sites are an incredibly convenient and efficient means for sharing personal information with family and friends. This convenience also brings some level of risk; therefore, social network users should be cognizant of what personal data is shared and who has access to this data. Users should think twice about posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you. If available, consider limiting access to posted personal data to "friends only" and attempt to verify any new sharing requests either by phone or in person. When receiving content (such as third-party applications) from friends or new acquaintances, be wary that many recent attacks have leveraged the ease with which content is generally accepted within the social network community. This content appears to provide a new capability, when in fact there is some malicious component that is rarely apparent to the typical user. Also, several social networking sites now provide a feature to opt-out of exposing your personal information to Internet search engines. A good recommendation is to periodically review the security policies and settings available from your social network provider to determine if new features are available to protect your personal information.

5. Enable the Use of SSL Encryption

Application encryption (also called SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit. SSL also prevents people who can see your traffic (for example at a public WiFi hotspot) from being able to impersonate you when logging into web based applications (webmail, social networking sites, etc.). Whenever possible, web-based applications such as browsers should be set to force the use of SSL. Financial institutions rely heavily on the use of SSL to protect financial transactions while in transit. Many popular applications such as Facebook and Gmail have options to force all communication to use SSL by default. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser.

6. Email Best Practices

Personal email accounts, either web-based or local to your host, are common attack targets. The following recommendations will help reduce your exposure to email-based threats:

a. In order to limit exposure both at work and home, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.

b. Setting out-of-office messages on personal email accounts is not recommended, as this can confirm to spammers that your email address is legitimate and also provide awareness to unknown parties as to your activities.

c. Always use secure email protocols if possible when accessing email, particularly if using a wireless network. Secure email protocols include Secure IMAP and Secure POP3. These protocols, or "always use SSL" for web-based

email, can be configured in the options for most email clients. Secure email prevents others from reading email while in transit between your computer and the mail server.

d. Unsolicited emails containing attachments or links should be considered suspicious. If the identity of the sender can't be verified, consider deleting the email without opening. For those emails with embedded links, open your browser and navigate to the web site either by its well-known web address or search for the site using a common search engine. Be wary of an email requesting personal information such as a password or social security number. Any web service that you currently conduct business with should already have this information.

7. Password Management

Ensure that passwords and challenge responses are properly protected since they provide access to large amounts of personal and financial information. Passwords should be strong, unique for each account, and difficult to guess. A strong password should be at least 10 characters long and contain multiple character types (lowercase, uppercase, numbers, and special characters). A unique password should be used for each account to prevent an attacker from gaining access to multiple accounts if any one password is compromised. Disable the feature that allows programs to remember passwords and automatically enter them when required. Additionally, many online sites make use of password recovery or challenge questions. The answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.

8. Photo/GPS Integration

Many phones and some new point-and-shoot cameras embed the GPS coordinates for a particular location within a photo when taken. Care should be taken to limit exposure of these photos on the Internet, ensure these photos can only be seen by a trusted audience, or use a third-party tool to remove the coordinates before uploading to the Internet. These coordinates can be used to profile the habits and places frequented for a particular individual, as well as provide near-real time notifications of an individual's location when uploaded directly from a smart phone. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Enhanced Protection Recommendations

The following recommendations require a higher level of administrative skills to implement and maintain on home networks than the previous recommendations. These recommendations provide additional layers of security but may impact your web browsing experience or require some iteration to adjust settings to the appropriate thresholds.

1. Enhanced Wireless Router Configuration Settings

Additional protections can be applied to the wireless network to limit access. The following security mechanisms do not protect against the experienced attacker, but are very effective against a less experienced attacker.

a. MAC address or hardware address filtering enables the wireless access point to only allow authorized systems to associate with the wireless network. The hardware address

for all authorized hosts must be configured on the wireless access point.

b. Limiting the transmit power of the wireless access point will reduce the area of operation (signal strength) of the wireless network. This capability curtails the home wireless network from extending beyond the borders of a home (e.g., parking lot or adjacent building).

c. SSID cloaking is a means to hide the SSID, the name of a wireless network, from the wireless medium. This technique is often used to prevent the detection of wireless networks by war drivers. It is important to note that enabling this capability prevents client systems from finding the wireless network. Instead, the wireless settings must be manually configured on all client systems.

d. Reducing the dynamic IP address pool or configuring static IP addresses is another mechanism to limit access to the wireless network. This provides an additional layer of protection to MAC address filtering and prevents rogue systems from connecting to the wireless network.

2. Disable Scripting Within the Web Browser

If using third party web browsers such as Firefox or Chrome, use NoScript (Firefox) or NotScript (Chrome) to prevent the execution of scripts from untrusted domains. Disabling scripting can cause usability issues, but is an effective technique to reduce web bourne attacks.

3. Enable Data Execution Prevention (DEP) for all Programs

By default, DEP is only enabled for essential Windows programs and services. Some third party or legacy applications may not be compatible with DEP, and could possibly crash when run with DEP enabled. Any program that requires DEP to execute can be manually added to the DEP exemption list, but this requires some technical expertise.

Additional Published Guidance

Social Networking
http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf

Mitigation Monday #2 – Defense Against Drive By Downloads
http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf

Mitigation Monday – Defense Against Malicious E-mail Attachments
http://www.nsa.gov/ia/_files/factsheets/MitigationMonday.pdf

Mac OSX 10.6 Hardening Tips
http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

Data Execution Prevention
http://www.nsa.gov/ia/_files/factsheets/I733-TR-043R-2007.pdf