Best Practices for Keeping Your Home Network

Narrator: The Internet is a great tool that many households use daily in today's society. It gives us the capability to instantly send emails to friends and family, read the latest news, research a subject for school, or check out the score of a game. Additionally, the Internet allows us to perform bank transactions, purchase products from stores thousands of miles away, modify our stock portfolios, apply for credit cards, or file our taxes. But while you're typing in your credit card number, do you ever wonder if someone can see everything you're typing? Do you fear your sensitive information can be obtained to steal your identity, max out your credit card on exotic purchases, or obtain personal information about yourself? All of these concerns are common issues faced by every day home users. Attackers target home users for many reasons, including credit card fraud, identity theft, denial of service, or simply to target their employer for those who work from home. The battle to protect that information can be won by securing your home network.

Narrator: The National Security Agency's Information Assurance Directorate, or IAD, released a fact sheet of recommendations for securing your home network called "Best Practices for Keeping Your Home Network Secure". Whether you own a Mac or PC, these tips can help maintain a basic level of network defense for both you and your family members accessing the Internet.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 1. Migrate to a Modern OS and Hardware Platform]

Narrator: 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.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 2. Install a Comprehensive Host-Based Security Suite]

Narrator: A comprehensive host-based security suite provides support for anti-virus, anti-phishing, safe browsing, Host-based Intrusion Prevention System, or 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.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS] UNCLASSIFIED//FOR OFFICIAL USE ONLY 2 UNCLASSIFIED//FOR OFFICIAL USE ONLY

[sub-Title: 3. Install Limit Use of the Administrator Account]

Narrator: The first account that is typically created when configuring a Windows host for the first time is the local administrator account. A nonprivileged "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 or editing. The privileged administrator account should only be used to install updates or software, and reconfi gure 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 including upper case, lower case, numbers, and special characters.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 4. Use a Web Browser with Sandboxing Capabilities]

Narrator: 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 are starting to appear on the market but are not yet ready for mass consumer use.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 5. Update to a PDF Reader with Sandboxing Capabilities]

Narrator: 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, or website links, by default.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 6. Migrate to Microsoft Office 2007 or Later]

Narrator: 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.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 7. Keep Application Software Up-to-Date]

Narrator: 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.

[TITLE: WINDOWS OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 8. Implement Full Disk Encryption (FDE) on Laptops]

Narrator: Windows 7 Ultimate as well as Vista Enterprise and Ultimate provide support for Bitlocker Full Disk Encryption, or 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.

[TITLE: Apple OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 1. Maintain an Up-to-Date OS]

Narrator: 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 and can receive its updates wirelessly or through a physical connection, for example, USB, to a host running iTunes. 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.

[TITLE: Apple OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 2. Keep Third Party Application Software Up-to-Date]

Narrator: 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.

[TITLE: Apple OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 3. Limit Use of the Privileged (Administrator Account)]

Narrator: 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 or 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.

[TITLE: Apple OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 4. Enable Data Protection on the iPad]

Narrator: 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 the following URL:

[subtitle] http://support.apple.com/kb/HT4175.

[TITLE: Apple OS HOST-BASED RECOMMENDATIONS]

[sub-Title: 5. Implement FileVault on Mac OS Laptops]

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

[TITLE: NETWORK RECOMMENDATIONS]

[sub-Title: 1. Home Network Design]

Narrator: The Internet Service Provider, or 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 that connects to the ISP provided router or cable modem.

[graphic: Typical SOHO Configuration graphic]

Narrator: 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.

[TITLE: NETWORK RECOMMENDATIONS]

[sub-Title: 2. Implement WPA2 on Wireless Network]

Narrator: The wireless network should be protected using Wi-Fi Protected Access 2, or WPA2, instead of Wired Equivalent Privacy, or WEP. 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.

[TITLE: NETWORK RECOMMENDATIONS]

[sub-Title: 3. Limit Administration to Internal Network]

Narrator: 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.

[TITLE: NETWORK RECOMMENDATIONS]

[sub-Title: 4. Implement an Alternate DNS Provider] Narrator: The Domain Name Servers, or 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.

[TITLE: NETWORK RECOMMENDATIONS]

[sub-Title: 5. Implement Strong Passwords on all Network Devices]

Narrator: 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.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 1. Traveling with Personal Mobile Devices]

Narrator: Many establishments, such as coffee shops, hotels, or airports, 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:

[sub-title: a. Use cellular network instead of hotspots for mobile devices]

Narrator: Mobile devices such as laptops, smart phones, and tablets, should utilize the cellular network, like 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.

[sub-title: b. Setup tunnels to a trusted VPN service provider]

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

[sub-title: c. Limit activities to web browsing at hotspots]

Narrator: 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. Narrator: 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 earlier.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 2. Exchanging Home and Work Content]

Narrator: Government maintained hosts are generally configured more securely and also have an enterprise infrastructure in place, such as email filtering, web content filtering or intrusion detection systems, for preventing and detecting malicious content. Since many users do not exercise the same level of security on their home systems, for example limiting the use of administrative credentials, home systems are generally easier to compromise. The forwarding of content like 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.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 3. Storage of Personal Information on the Internet]

Narrator: 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 before posting "Who will have access to the information I am posting?" and "What controls do I have over how this information is stored and displayed?" Internet users should also be aware of personal information already published online by periodically searching for their personal information using popular Internet search engines.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 4. Use of Social Networking Sites]

Narrator: 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.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 5. Enable the Use of SSL Encryption]

Narrator: Secure socket layer, or SSL encryption, protects the confidentiality of sensitive information while in transit over the Internet. SSL also prevents people who can see your traffic, for example at public WiFi hotspots, from being able to impersonate you when logging into web based applications, like webmail or social networking sites. 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 like 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.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 6. Email Best Practices]

Narrator: 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:

[sub-title: Use different usernames for home and work email addresses]

Narrator: 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.

[sub-title: Avoid using out-of-office messages on personal email accounts]

Narrator: 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.

[sub-title: Use secure email protocols]

Narrator: 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 your email while in transit between your computer and the mail server.

[sub-title: Be cautious around unsolicited emails with attachments and/or links]

Narrator: 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.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 7. Password Management]

Narrator: 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, such as 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.

[TITLE: Operational Security (OPSEC)/Internet Behavior Recommendations]

[sub-Title: 8. Photo/GPS Integration]

Narrator: Many phones and some new point-and-shoot cameras embed the GPS coordinates of the camera 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 by 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.

[CAUTION tape picture]

Narrator: 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.

[TITLE: Enhanced Protection Recommendations]

[sub-Title: 1. Enhanced Wireless Router Configuration Settings]

Narrator: 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.

[sub-Title: MAC address or hardware address filtering]

Narrator: MAC address or hardware address filtering enables the wireless access point to only allow authorized systems to associate with the wireless network. The hardware addresses for all authorized hosts must be configured on the wireless access point.

[sub-Title: Limit wireless access point transmit power]

Narrator: Limiting the transmit power of the wireless access point will reduce the area of operation or usable signal strength, of the wireless network. This capability curtails the home wireless network from extending beyond the borders of a home for example, into a parking lot or adjacent buildings.

[sub-Title: SSID Cloaking]

Narrator: Service Set Identifier, or 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.

[sub-Title: Reducing dynamic IP address pool / Configuring Static IP addresses]

Narrator: 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.

[TITLE: Enhanced Protection Recommendations]

[sub-Title: 2. Disable Scripting Within the Web Browser]

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

[TITLE: Enhanced Protection Recommendations]

[sub-Title: 3. Enable Data Execution Prevention (DEP) for all Program]

Narrator: By default, Data Execution Prevention, or 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.
Narrator: For more information, visit the following URLs:

[TITLE: Additional Published Guidance Social Networking https://nsagov.web.nsa.ic.gov/ia/_fi les/factsheets/I73- 021R-2009.pdf Mitigation Monday #2 â€“ Defense Against Drive By Downloads https://nsagov.web.nsa.ic.gov/ia/_fi les/factsheets/I733-011R-2009.pdf Mitigation Monday â€“ Defense Against Malicious E-mail Attachments https://nsagov.web.nsa.ic.gov/ia/_fi les/factsheets/MitigationMonday.pdf Mac OSX 10.6 Hardening Tips https://nsagov.web.nsa.ic.gov/ia/_fi les/factsheets/macosx_10_6_hardeningtips.pdf Data Execution Prevention https://nsagov.web.nsa.ic.gov/ia/_fi les/factsheets/I733- TR-043R-2007.pdf]