Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Implementing and Auditing the Critical Security Controls - In-Depth (Security 56)" at http://www.giac.org/registration/gccc
Abstract

Consumers need better home network security guidance for taking stock of the hardware and software applications installed on their network and devices. The primary sources of information security advice for the average person are TV, magazines, newspapers, websites and social media. Unfortunately, these sources typically repeat the same advice, provide limited guidance and miss key areas of security that should be taken into consideration when securing home networks. On the other hand, enterprises receive comprehensive, prioritized guidance such as the Critical Security Controls from The Center for Internet Security. Unfortunately, these controls were not designed with securing home networks in mind. The wide gap between consumer-media advice columns and highly professional corporate security controls needs to be bridged. This can be done by using the Critical Security Controls as a comprehensive foundation from which to craft an authoritative yet easy-to-understand set of home network security recommendations for individuals. The first step is distilling the guidance for inventorying hardware and software applications.
1. Introduction

Consumers need better home network security guidance for managing the inventory of devices on their home network as well as the apps installed on the many devices attached to their network. The United States government has a treasure trove of special publications from NIST. The Center for Internet Security has provided a similar, more digestible set of Critical Security Controls for industry. Yet consumers do not have a similar set of guidelines to reference and assess their networks against.

Just what exactly do they have? The primary sources of consumer security advice are television, print media like magazines and the Internet, including Google searches, blogs and social media. But these sources typically repeat the same, often incomplete or outdated advice and provide limited guidance while missing key areas of security.

Using the Center for Internet Security’s Critical Security Controls as the basis and distilling from it the necessary home network security guidance solves this problem. The first two Critical Security Controls (Center for Internet Security, 2015) are foundational and can be used to generate consumer guidelines for a Cybersecurity Inventory at Home. These controls are:

- CSC 1: Maintain a list of devices on your network.
- CSC 2: Maintain a list of all software/apps installed on your devices.

2. How to Inventory Network Devices

CSC 1: Maintain a list of devices on your network

Network security, like all security controls and safeguards, is best and most cheaply applied proactively (Tipton, 2010). One of the most fundamental proactive tasks for securing a home network is making a list that includes all devices on the network or that could later join the network. A simple spreadsheet can be created to document a comprehensive inventory of these devices.

Why should components that are not even connected to a network be inventoried? Devices that are off a network still need to be managed to keep them protected, up-to-
date and backed up. Having a complete inventory is also helpful when investigating unknown devices that show up on the home network. All devices must be listed because even if a device is not on the network at the moment, an attacker at some point could still use it in the future.

Steps for inventorying network devices:
1. Create a hardware inventory list.
2. Scan the network for devices.
4. Create a network diagram.
5. Maintain hardware inventory list.

2.1. Create a Hardware Inventory List

Creating and populating a hardware list for the first time takes a lot of time and effort. Fortunately, there are multiple tools available to make the process as efficient and stress-free as possible. One such tool is the Hardware Inventory List template (Excel spreadsheet) located in the Appendix. In the template, the information fields are ready to be populated with the documentation for each device.

Steps for creating a hardware inventory list:
1. Determine what program you will use (e.g. Excel, Sheets).
2. Identify all device types that will be inventoried.
3. Identify all relevant information fields associated with the devices to be inventoried.
4. Create the list template in the chosen program with relevant fields created and ready for input.

Suggested device types to be captured by the inventory process:
- Desktop
• Laptop
• Phone-Mobile
• Phone-IP
• Tablet
• Printer
• Scanner
• Server
• Virtual machine
• Access point: SSID
• Modem
• Modem-Wireless AP
• Firewall
• Router
• Switch
• TV
• Streaming device (e.g. Apple TV, Chromecast, Amazon Fire, Roku)
• Gaming Console (e.g. Xbox, PlayStation, Nintendo)
• Cable box
• DVR
• IP security camera
• Photo camera
• Electronic thermostat
• Electronic refrigerator
• Storage system
• Removable media containing sensitive data (e.g. CD-R, DVD-R, USB Flash Drive)
• Electronic Photo Frame
• Uninterruptable Power Supply (UPS)
• Other Internet of Things (IoT) device

Author Name, email@address
Suggested hardware inventory list fields:

- Name
- IP Address
- MAC Address
- Device Type
- Manufacturer
- Make
- Model Number
- Serial Number
- Purchase Date
- Warranty Expiration Date
- Firmware
- Operating System
- OS Version
- Primary User
- Function
- Location
- On Network?
- Mobile

2.2. Scan the Network for Devices

One of the easiest ways to begin documenting the devices on a home network is to conduct a scan. There are several options for scanning a network. A Mac, PC or even a mobile device can be used to perform the scan and the software options range from easy-to-use (e.g. IP Scanner, Fing) to complex (e.g. Nmap, Wireshark). Whatever scanning solution is selected, it must have a good reporting function. Any security tool is only as useful as the output it generates (Lyon, 2008).

2.2.1. Network Scanning from a Computer

Whether or not the devices on the home network are wired or wireless, a scan can be completed using software installed on a computer. Here is an example that shows how...
to perform a wireless scan on a Mac using an app called IP Scanner (10base-T Interactive, 2015), which can be downloaded from the Apple App Store:

Step 1: Download and open the IP Scanner app.

![IP Scanner app](image)

Step 2: Perform the scan.

![Scan results](image)

Step 3: Export the results and update the software application inventory list with the IP addresses, MAC addresses and device types.
Note: The IP Scanner app has several other features to explore including labeling components, sending alert notifications if a new device joins the network and whitelisting devices on the network that have been confirmed to be authorized. Whitelisting can be a timesaver on subsequent inventory reviews.

2.2.2. Wireless Scanning from Your Mobile Device

It has become increasingly convenient to use mobile devices for just about everything and network scanning is no different. Scanning from a mobile phone or tablet, an inventory of wireless devices can be created. While useful, the inventory will need to be supplemented using a wired computer and manual discovery to inventory non-wireless components. Here is an example that shows how to perform a wireless scan on an iPhone.

Author Name, email@address
or iPad using an app called Fing (Overlook Soft., 2015), which can be downloaded from the Apple App Store:

Step 1: Download and open the Fing App.

Step 2: Perform the scan.
Step 3: Export the results and update the hardware inventory list with the IP addresses, MAC addresses and device types.

2.3. Perform a Manual Network Discovery

Even after performing scans, many devices that should be on the hardware inventory list must be manually added. This could be due to a weak wireless signal or the device may be off the network for some other reason such as being powered off or taken away from the residence. Perform a manual discovery and to add devices not covered by the scan and fill in all gaps on the list. Include anything on the network as well as anything that could get on the network. Consider adding off-network storage such as thumb drives and backup DVD-Rs. Here are the steps for performing a manual network discovery.

Step 1: Walk all rooms, including outdoor living spaces.

Step 2: Identify components that are off the network or need to be added to the hardware inventory list.

Author Name, email@address
Step 3: For all devices on the hardware inventory list, finish populating all fields to complete the list.

2.4. Create a Network Diagram

A natural add-on to the inventory list is a visual diagram of the home network showing all devices and how they are connected, or not. This could be as simple as a hand-drawn diagram or it could be a diagram created using a tool like Visio or xDiagram. A network diagram can prove invaluable for memory refreshes about how the home network is configured and can also aid in troubleshooting network issues.

Here is an example of a home network diagram produced in xDiagram:
2.5. Maintain Hardware Inventory List

Hardware inventories should be updated at least once per quarter. The hardware inventory process is a great way to identify unknown devices that may represent a threat to security. Here are the steps to take to ensure your hardware inventory list is kept up-to-date:

Step 1: Do a complete hardware inventory.
Step 2: Compare current inventory to previous inventory to find additional devices.
Step 3: Determine if the added devices are authorized or if they should be removed from the network.
Step 4: Update hardware inventory list with any changes that need to be made.

3. How to Inventory Software Applications

CSC 2: Maintain a list of all software/apps installed on your devices

Consumers need to maintain a list of the software applications installed on the devices in their hardware inventory. Limiting app installs to the devices on the authorized hardware inventory list reduces the risk of malware on the network. For most families, the ability to install software applications should be limited to a parent who also maintains a software application inventory list.

Steps for inventorying software applications:
1. Create a software application inventory list.
2. Query computers for software applications.
3. Query mobile devices for software applications.
4. Maintain software application inventory list.

3.1. Create a Software Application Inventory List

Creating and populating a software application list, like the hardware inventory list, is time-consuming. Using the same tool for tracking both the software and hardware inventories can make the process more efficient. There is a Software Application Inventory List template (Excel spreadsheet) located in the Appendix that can be leveraged as well.

Author Name, email@address
Steps for creating a software application inventory list:

1. Determine what program you will use (e.g. Excel, Sheets).
2. Identify all device types whose software applications will be inventoried.
3. Identify all relevant information fields associated with the software applications to be inventoried.
4. Create the list template in the chosen program with relevant fields created and ready for input.

Suggested software application inventory list fields:

- Manufacturer
- Software Application Name
- Software Type (e.g. Desktop, Mobile, Firmware)
- Function (Productivity, Game, Operating System, Hypervisor)
- Installed Version (including patch level)
- Current Version
- License Number
- Serial Number
- Devices Installed On
- Purchase Date
- Activation Date
- Warranty Expiration Date
- License Expiration Date

### 3.2. Query Computers for Software Applications

Getting a solid list of applications installed on a computer depends on the type of computer in question. In addition, user preference may dictate how the list should be displayed. In the sections below, instructions for listing software are provided for both Mac OS X and Windows PCs using two methods: the GUI and scripting.
3.2.1. Mac Software Applications

There are a couple of easy ways to get a list of all the applications installed on a Mac. One way is by using the operating system GUI and the other way is to run a script that outputs to a file. The information needed for the inventory list can be retrieved using either method so it is just a matter of personal preference.

GUI Method for Listing Apps on a Mac:
Step 1: Click the Apple icon on the menu bar and select About This Mac.

Step 2: Click the System Report button.

Step 3: On the left pane of the System Report, select Software, and then select Applications. This will show all the applications installed on the Mac.
Scripting Method for Listing Apps on a Mac:

Step 1: Open the Terminal

Step 2: Copy/Paste this script into the Terminal and hit Enter:

```
system_profiler -detailLevel full SPApplicationsDataType > apps.txt
```
Step 3: Open the file created by the script to retrieve information on the installed software applications.

3.2.2. Windows PC Software Applications

Just as there are multiple ways to list applications on a Mac, Windows offers a couple of convenient methods for doing the same. These methods include using the Control Panel and using PowerShell scripting.

**Control Panel Method for Listing Apps on a Windows PC:**

```bash
Last login: Sun Dec 20 07:38:35 on ttyS000
You have mail.
Yong:~ gwilliams> system_profiler -detailLevel full SPAApplicationsDataType > apps.txt
```

<table>
<thead>
<tr>
<th>IP Scanner Home:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version:</strong> 3.42</td>
</tr>
<tr>
<td><strong>Obtained From:</strong> Mac App Store</td>
</tr>
<tr>
<td><strong>Last Modified:</strong> 12/16/15, 6:44 AM</td>
</tr>
<tr>
<td><strong>Kind:</strong> Intel</td>
</tr>
<tr>
<td><strong>64-Bit [Intel]:</strong> Yes</td>
</tr>
<tr>
<td><strong>Signed by:</strong> Apple Mac OS Application Signing, Apple Worldwide Developer Relations Certification Authority, Apple Root CA</td>
</tr>
<tr>
<td><strong>Location:</strong> /Applications/IP Scanner Home.app</td>
</tr>
<tr>
<td><strong>Get Info String:</strong> IP Scanner Home 3.42</td>
</tr>
</tbody>
</table>

**Installer:**

```bash
Version: 6.2.8
Obtained From: Apple
Last Modified: 12/18/15, 2:20 PM
Kind: Intel
64-Bit [Intel]: Yes
Signed by: Software Signing, Apple Code Signing Certification Authority, Apple Root CA
Location: /System/Library/CoreServices/Installer.app
```

**Wireshark:**

```bash
Version: 1.12.7
Obtained From: Identified Developer
Last Modified: 8/12/15, 1:42 AM
Kind: Intel
64-Bit [Intel]: No
Signed by: Developer ID Application: Wireshark Foundation, Inc. [7266810251], Developer ID Certification Authority, Apple Root CA
Location: /Applications/Wireshark.app
```

**NetSpot:**

```bash
Version: 1.3.41B
Obtained From: Mac App Store
Last Modified: 12/16/15, 5:08 AM
Kind: Intel
64-Bit [Intel]: Yes
Signed by: Apple Mac OS Application Signing, Apple Worldwide Developer Relations Certification Authority, Apple Root CA
Location: /Applications/NetSpot.app
```

**InSSIDer:**

```bash
Version: 6.2.13
Obtained From: Identified Developer
Last Modified: 12/19/15, 4:05 PM
Kind: Intel
64-Bit [Intel]: No
Signed by: Developer ID Application: MetaGeek, LLC [8082046039], Developer ID Certification Authority, Apple Root CA
Location: /Applications/InSSIDer.app
```

**WiFi Explorer:**

```bash
Version: 2.1
Obtained From: Mac App Store
Last Modified: 12/16/15, 5:42 AM
```
Step 1: Hit the Start button and select Control Panel from the pop-up menu.
Step 2: Click Programs and Features.

Step 3: Use installed application information to update software application inventory list.

Scripting Method for Listing Apps on a Windows PC:
Step 1: Click the Start button and select Run from the pop-up menu.
Step 2: Type “cmd” in the Open dialog box and hit OK to open the command prompt.

![Run dialog box with cmd selected](image)

Step 3: Type “powershell” in the terminal window and hit enter to invoke PowerShell.

Step 4: Copy/Paste the following script into the terminal window and hit Enter.

```powershell
get-wmiobject -class win32_product | select vendor, name, version | sort-object vendor, name | export-csv c:\apps.csv –notype
```

Step 5: Use the file that was just created to update the software application inventory list.
3.3. **Query Mobile Devices for Software Applications**

Mobile devices, in general, don’t make it very easy for consumers to inventory installed apps. Therefore, the first mobile inventory will involve a lot of scrolling and typing. For example, here are the steps required to get a detailed list of the apps installed on an iPhone or iPad:

Step 1: Tap the App Store.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>vendor</td>
<td>name</td>
</tr>
<tr>
<td>2</td>
<td>Microsoft Corporation</td>
<td>Microsoft .NET Framework 4.5.2</td>
</tr>
<tr>
<td>3</td>
<td>Microsoft Corporation</td>
<td>Microsoft Lync 2013</td>
</tr>
<tr>
<td>4</td>
<td>Microsoft Corporation</td>
<td>Microsoft Lync MUI (English) 2013</td>
</tr>
<tr>
<td>5</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office 64-bit Components 2013</td>
</tr>
<tr>
<td>6</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Access MUI (English) 2010</td>
</tr>
<tr>
<td>7</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Access Setup Metadata MUI (English) 2010</td>
</tr>
<tr>
<td>8</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Excel MUI (English) 2010</td>
</tr>
<tr>
<td>9</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Groove MUI (English) 2010</td>
</tr>
<tr>
<td>10</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office InfoPath MUI (English) 2010</td>
</tr>
<tr>
<td>11</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Office 64-bit Components 2010</td>
</tr>
<tr>
<td>12</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office OneNote MUI (English) 2010</td>
</tr>
<tr>
<td>13</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Outlook MUI (English) 2010</td>
</tr>
<tr>
<td>14</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office PowerPoint MUI (English) 2010</td>
</tr>
<tr>
<td>15</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Professional Plus 2010</td>
</tr>
<tr>
<td>16</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proof (English) 2010</td>
</tr>
<tr>
<td>17</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proof (French) 2010</td>
</tr>
<tr>
<td>18</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proof (Spanish) 2010</td>
</tr>
<tr>
<td>19</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proofing (English) 2010</td>
</tr>
<tr>
<td>20</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proofing (English) 2013</td>
</tr>
<tr>
<td>21</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proofing Tools 2013 - English</td>
</tr>
<tr>
<td>22</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Proofing Tools 2013 - Español</td>
</tr>
<tr>
<td>23</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Publisher MUI (English) 2010</td>
</tr>
<tr>
<td>24</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared 64-bit MUI (English) 2010</td>
</tr>
<tr>
<td>25</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared 64-bit MUI (English) 2013</td>
</tr>
<tr>
<td>26</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010</td>
</tr>
<tr>
<td>27</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2013</td>
</tr>
<tr>
<td>28</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared MUI (English) 2010</td>
</tr>
<tr>
<td>29</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared MUI (English) 2013</td>
</tr>
<tr>
<td>30</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared Setup Metadata MUI (English) 2010</td>
</tr>
<tr>
<td>31</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Shared Setup Metadata MUI (English) 2013</td>
</tr>
<tr>
<td>32</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Visio 2010</td>
</tr>
<tr>
<td>33</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Visio MUI (English) 2010</td>
</tr>
<tr>
<td>34</td>
<td>Microsoft Corporation</td>
<td>Microsoft Office Word MUI (English) 2010</td>
</tr>
</tbody>
</table>
Step 2: Tap Purchased.
Step 3: Tap My Purchases.
Step 4: Document app details (app name, manufacturer, version)

Note: The list shows all purchased applications including those that are not installed. The cloud icon indicates a particular app is not installed while the OPEN button appears next to apps that are installed.

3.4. Maintain Software Application Inventory List

Software application inventories should be updated at least once per quarter. The inventory process is a great way to identify unknown or unauthorized software that should be uninstalled. Here are the steps to take to ensure your software inventory is kept up-to-date:

Step 1: Do a complete software application inventory.
Step 2: Compare current inventory to previous inventory to find added apps.
Step 3: Determine if the added apps are authorized or if they should be removed.
Step 4: Update software inventory list with any changes that need to be made.
4. Conclusion

Having a good inventory list is the foundation for being able to identify unknown or unauthorized hardware and software. The Center for Internet Security’s Critical Security Controls provide a solid basis for consumers looking to create and maintain hardware and software inventories. These hardware and software inventory lists must be kept up-to-date as components are added to the network.
References


Appendix

Hardware Inventory List Template:

Hardware Inventory List Template.xlsx

Software Application Inventory List Template:

Software Application Inventory List Template.xlsx
# Upcoming Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London May 2020</td>
<td>London, United Kingdom</td>
<td>May 18, 2020 - May 23, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS vLive - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth</td>
<td>SEC566 - 202005,</td>
<td>May 19, 2020 - Jun 18, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANSFIRE 2020</td>
<td>Jacksonville, FL</td>
<td>Jun 22, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Silicon Valley - Cupertino 2020 - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Security Awareness Summit &amp; Training 2020</td>
<td>Austin, TX</td>
<td>Aug 03, 2020 - Aug 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020</td>
<td>Amsterdam, Netherlands</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Tampa-Clearwater 2020</td>
<td>Clearwater, FL</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain September 2020</td>
<td>Manama, Bahrain</td>
<td>Sep 12, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Ottawa SEC566</td>
<td>Ottawa, ON</td>
<td>Sep 14, 2020 - Sep 18, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020</td>
<td>San Antonio, TX</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>