

Confidence in the Connected World



Version 7.1

CIS Controls Internet of Things Companion Guide



Contents

| | |
|--|------|
| Acknowledgments | 2 |
| Introduction..... | 3 |
| Definition of Internet of Things | 3 |
| Methodology..... | 5 |
| Scope | 5 |
| Terminology..... | 5 |
| Applicability Overview | 6 |
| CIS Controls 1–20 (Version 7): Internet of Things Security | 7-63 |
| Acronyms and Abbreviations..... | 64 |
| Links and Resources..... | 66 |
| Closing Notes | 67 |

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for noncommercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (<http://www.cisecurity.org/controls/>) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of CIS® (Center for Internet Security, Inc.®).

Acknowledgments

CIS® (Center for Internet Security, Inc.®) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors:

Mary C. Yang, MITRE
Joshua M. Franklin, CIS

Contributors:

Vytautas Kuliesius, NRD Cyber Security
Staffan Huslid, Knowit Secure
Tony Krzyzewski, SAM for Compliance Ltd.
Karen Scarfone, Scarfone Cybersecurity
Emilio Grande-Garcia
Joseph M. DiPipi, Zoetis
Stephanie Domas, MedSec
Brian Russell, Cloud Security Alliance
Robin Regnier, CIS
Philippe Langlois, CIS

Introduction

The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth approach and best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, transport, education, government, defense, and others. While the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

The purpose of the CIS Controls Internet of Things Community is to develop best practices and guidance for implementing the CIS Controls in association with a variety of devices within the Internet of Things (IoT). Enterprise use of IoT presents unique and complex challenges for security professionals. IoT devices are being embedded into the enterprise across the globe and often cannot be secured via standard enterprise security methods, such as running a monitoring application on the device, as the devices can't support these types of applications. Yet for ease of use, enterprise IoT devices are often connected to the same networks that employees use day in and day out and are often directly connected to the internet via a variety of network protocols (e.g., Ethernet, Bluetooth, wireless fidelity [WiFi], cellular).

Definition of Internet of Things

There is no universally agreeable definition for IoT. The variety of perspectives from industry, academia, governments, and others across the world have led to different definitions, each focused on the needs of their sector, business, or area of interest. Each definition has relevant strengths and weaknesses, and they do not act to invalidate each other. Instead these definitions work within their desired context, and others may choose to use and apply them as they see fit for the systems that will be procured and implemented.

- In [The Internet of Things: An Overview](#), a 2015 report from The Internet Society, IoT is defined as: “...scenarios where network connectivity and computing capability extends to objects, sensors, and everyday items not normally considered computers, allowing these devices to generate, exchange, and consume data with minimal human intervention.”
- A 2015 report from the Institute of Electrical and Electronics Engineers Incorporated (IEEE) titled [Towards a Definition of the Internet of Things](#), defines IoT as “A network of items — each embedded with sensors — which are connected to the Internet.”
- IoT has been defined within a recommendation from the International Telecommunication Union as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”
- [Gartner's IT Glossary](#) defines IoT as “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”

Regardless of which definition an organization chooses to use, there are certain common features:

- Communications – Whether this is via a local medium, such as radio frequency identification (RFID), Bluetooth, WiFi, or via a wide area network (WAN) protocol, such as cellular, IoT devices can communicate with other devices.
- Functionality – IoT devices have a core function as well as some additional functionality but they do not do everything. Most IoT devices do one thing and do it well.
- Processing capability – IoT devices have sufficient processing capability to make their own decisions and act on inputs received from outside sources, but not enough intelligence to do complex tasks. For instance, they generally cannot run a rich operating system designed for a traditional desktop or mobile device.

The lack of a consistent, agreed-upon definition is actually part of the challenge within the IoT arena. IoT is a large, complex space and common issues include:

- Ubiquity – There are a large number of overall devices.
- Uniqueness – Devices are developed by different manufacturers with varying version numbers.
- Ecosystem – Multiple vendors are involved in creating each device, including hardware, firmware, and software.

Examples of IoT devices that might be included within an enterprise include smart speakers, security cameras, door locks, window sensors, thermostats, headsets, watches, power strips, and more—basically any device that may be integrated into a typical business IT environment.

Methodology

A consistent approach is needed for analyzing the CIS Controls in the context of IoT. For each of the 20 CIS Controls, the following information is provided in this document:

- Applicability – This assesses the degree to which a CIS Control functions or pertains to IoT.
- Challenges – These are unique issues that make implementing any of the relevant CIS Controls, or Sub-Controls, for IoT devices difficult.
- Additional Discussion – This is a general area for any guidance that also needs to be noted. For instance, relevant tools, products, or threat information that could be of use can be found here.




Scope


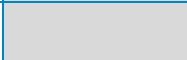


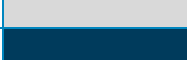

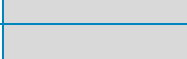





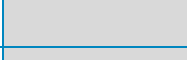





The objective of this document is to have broad applicability across sectors. IoT affects all areas of computing across multiple sectors, such as healthcare, aviation, public safety, and energy. This has led to sector-specific IoT security guidance, but this document is purposefully sector-agnostic. As such, this guide focuses on purchasing, deploying, and monitoring commercially available IoT devices. This document does not provide guidance on how to design, develop, and manufacture secure IoT devices, such as the secure system development process noted within NIST Special Publication (SP) 800-160 Revision 1.

Terminology

As noted earlier, there are many definitions of IoT. Below are basic descriptions of IoT components and terminology that we use throughout this document. Devices are the *thing* within IoT and are the primary focus of this guide. Gateways are devices that multiple things connect to in order to receive instructions, transfer data, etc. Multiple devices are often connected to a single gateway, or a gateway may solely passively monitor IoT devices. A gateway has an internet connection, whereas not all IoT devices will, and may only support local wireless protocols such as RFID, WiFi, Bluetooth, and Zigbee. Gateways are one way to help reduce the attack surface of legacy IoT devices that cannot be properly secured. Many consumer IoT devices are associated with complex cloud platforms that can control the behavior of IoT devices and access and store data.

Applicability Overview

-  More than 60% of CIS Sub-Controls apply
-  Between 60% and 0% of CIS Sub-Controls apply
-  0% of CIS Sub-Controls apply

| Control | CIS Control Title | Applicability |
|---------|---|---|
| 1 | Inventory and Control of Hardware Assets |  |
| 2 | Inventory and Control of Software Assets |  |
| 3 | Continuous Vulnerability Management |  |
| 4 | Controlled Use of Administrative Privileges |  |
| 5 | Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers |  |
| 6 | Maintenance, Monitoring and Analysis of Audit Logs |  |
| 7 | Email and Web Browser Protections |  |
| 8 | Malware Defenses |  |
| 9 | Limitation and Control of Network Ports, Protocols and Services |  |
| 10 | Data Recovery Capabilities |  |
| 11 | Secure Configuration for Network Devices, such as Firewalls, Routers and Switches |  |
| 12 | Boundary Defense |  |
| 13 | Data Protection |  |
| 14 | Controlled Access Based on the Need to Know |  |
| 15 | Wireless Access Control |  |
| 16 | Account Monitoring and Control |  |
| 17 | Implement a Security Awareness and Training Program |  |
| 18 | Application Software Security |  |
| 19 | Incident Response and Management |  |
| 20 | Penetration Tests and Red Team Exercises |  |

CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

IoT Applicability

It is important to track which devices have access to the network and are accessing data and organizational resources. IoT devices are no different and this Control is considered extremely important. Traditional MAC (media access control) and IP (internet protocol) addresses can be used for device identifiers. Unfortunately, not all IoT devices will have these identifiers present (e.g., MAC address, IP address). For instance, while Zigbee devices support physical layer MAC address, they use a Zigbee network address in lieu of an IP address. Very simple sensors and devices used for location tracking may only beacon identifiers for RFID. When using devices that do not support network-based authentication, network segmentation can be considered as a possible way to mitigate risk. Additional information on segmentation is available in CIS Control 12 (*Boundary Defense*) and CIS Control 15 (*Wireless Access Control*).

IoT Challenges

Organizations must deploy technology that tracks the myriad of IoT devices that can be deployed across their enterprise. Understanding which device types and, in some cases, which specific device instances are authorized to connect to the network is the starting point to adapting this Control for IoT. For devices without traditional identifiers, physical tags can be placed onto the devices themselves that integrate with asset management systems. For IoT devices with an externally accessible physical interface, cellular devices can be inserted into that interface with cloud-based asset management systems.

Some IoT devices are designed to work in relative isolation and never connect to an enterprise network. These devices still may be network-connected though, as they can communicate with a back-end cloud platform that the enterprise neither controls nor manages. Wireless IoT gateways can also be used to monitor wireless traffic from IoT devices, which can then be relayed to an asset management system, either in the cloud or physically hosted at the enterprise. Another challenge can be using digital certificates in IoT devices. Finally, global positioning system (GPS) can also be an effective way to monitor the location of IoT devices distributed outside the enterprise.

IoT Additional Discussion

Typical asset tracking tools may not work out of the box with IoT devices. Network scans for legacy and nontraditional devices may be dangerous to device, network, and system stability, potentially leaving IoT endpoints in an error state. Before purchasing devices and using them within an organization, it is worthwhile to understand how a device will respond to an asset discovery tool, and how well it will integrate with any asset management tools being utilized by an enterprise. The conventional approach of using ping responses, transmission control protocol synchronization (TCP SYN) or acknowledge (ACK) scans can disrupt communications, or, in some cases, even impact device operations. Passive methods are preferred and are less likely to impact system availability or to interact with vendor systems in a manner that could cause warranty issues. Where practical, non-intrusive methods should be leveraged, including media

access control-address resolution protocol (MAC-ARP) tables, domain name system (DNS), active directory (AD), or a variety of IoT-specific tools employed to control and collect data in these systems for the express purpose of locating the variety of connected assets.

Wireless monitoring may be necessary to identify devices as many IoT devices lack wire-line physical connections. Many newer IoT devices support integration into IoT management systems via application programming interfaces (APIs). At the very least, organizations can make a listing of device MAC address, device type, serial number, and other relevant information. "Smarter" IoT devices can utilize digital certificates to enhance identity and access management.

| CIS Control 1: Inventory and Control of Hardware Assets | | | | Applicability |
|---|--|--|---|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 1.1 | Utilize an Active Discovery Tool | Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. | <ul style="list-style-type: none"> • | Active discovery tools should be implemented to identify IoT devices, although some types of scans could leave devices in a nonfunctional state. The types of scans run against high-value or critical IoT assets should be contemplated before they are run, with the outcomes known beforehand. |
| 1.2 | Use a Passive Asset Discovery Tool | Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory. | <ul style="list-style-type: none"> • | A passive asset discovery tool may not identify all IoT devices but is a solid step forward to understanding the devices on the network. |
| 1.3 | Use DHCP Logging to Update Asset Inventory | Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory. | <ul style="list-style-type: none"> • | This Sub-Control should be applicable to IoT devices using Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). |

| CIS Control 1: Inventory and Control of Hardware Assets | | | | Applicability |
|---|---|---|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 1.4 | Maintain Detailed Asset Inventory | Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not. | • | This Sub-Control helps to ensure that IoT devices that are never intended to be connected to the enterprise network, or only connected to an internal network, are still properly tracked. |
| 1.5 | Maintain Asset Inventory Information | Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. | • | This can present a variety of challenges for IoT devices, as the hardware asset information can drastically change from manufacturer to manufacturer. It can be difficult to standardize field formats as well. Broadly, it is best to collect whatever hardware asset information is available. |
| 1.6 | Address Unauthorized Assets | Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner. | • | Unknown IoT devices connected to enterprise networks and systems should be quickly investigated and removed. |
| 1.7 | Deploy Port Level Access Control | Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. | • | It is unlikely that this will be possible for most IoT devices, but if the capability is available, it should be enabled. Note that 802.1x does not work on many IoT devices that do not support supplicant software. Network-level authentication can cause reliability issues if not strictly maintained. |
| 1.8 | Utilize Client Certificates to Authenticate Hardware Assets | Use client certificates to authenticate hardware assets connecting to the organization's trusted network. | • | It is unlikely that this will be possible for many IoT devices, but if the capability to store and utilize certificates within an authentication protocol is available, it should be enabled. |

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

IoT Applicability

Network scanning and agent-based approaches are typical methods for software asset management. As mentioned in CIS Control 1, network scanning can leave many IoT devices in an unsafe or unusable state. Agent-based approaches will be ineffectual for IoT devices as there is not a common platform for the agent to be built to and installed on. Manual and procedural methods can be used for asset tracking, such as a spreadsheet.

IoT Challenges

Identifying the versions of software and firmware of IoT devices within the enterprise is a challenge. It may be possible to leverage central command and control systems, which are aware of device firmware versions. However, custom and restricted operating systems may limit remote query capability. In general, IoT device software is not patchable, but is loaded onto the device as a new complete image. To obtain the listing of software applications on an embedded device, it may be necessary to work with the device developer/manufacturer. Manual sampling or firmware extraction via on-board direct maintenance ports (e.g., joint test action group [JTAG]) using proprietary software and hardware tools may be required.

IoT Additional Discussion

In some cases, firmware must be delivered over the network to IoT devices. In these situations, utilize best practices for securing firmware images, which often includes applying digital signatures that are evaluated by the device before loading. The user or the device may check the signature. This may require a secured space within the device to store credentials used for signature validation.

Tracking versions of Bluetooth and WiFi in devices can be quite difficult and may not be possible using traditional scanning methods. Applications like Airodump-ng for WiFi devices and hcitool or ubertooth-scan for Bluetooth devices will provide broadcast advertisements and MAC addresses. Note that for Bluetooth devices, MAC addresses do not conform to typical conventions and are oftentimes represented as the device WiFi MAC address incremented by 1 bit. The information available from WiFi and Bluetooth advertisements will allow enterprises to identify which versions of wireless protocols are supported.

Whitelisting is generally not available on IoT devices. Whitelisting can occur at the application layer, or specific libraries or scripts can be whitelisted. A more common capability is for devices to perform *command whitelisting*, which only specifies a subset of commands that a device would accept. This will more likely be available with IoT vendors that engage within a security engineering process over the lifecycle of the product.

| CIS Control 2: Inventory and Control of Software Assets | | | | Applicability |
|---|---|---|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 2.1 | Maintain Inventory of Authorized Software | Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system. | • | At minimum, a listing of the software versions associated with the IoT device can be noted. |
| 2.2 | Ensure Software Is Supported by Vendor | Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. | • | Enterprises should check the period of time for which a device will be supported before purchase. Additional support may be available for purchase, but this is uncommon. |
| 2.3 | Utilize Software Inventory Tools | Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems. | • | Not all IoT devices will be able to integrate or be inventoried by an automated tool, but those that have this capability should use it. |
| 2.4 | Track Software Inventory Information | The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization. | • | Tracking this level of detail may be difficult, and some systems may only allow you to track real-time inventory data, not historical information. |

| CIS Control 2: Inventory and Control of Software Assets | | | | Applicability |
|---|--|--|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 2.5 | Integrate Software and Hardware Asset Inventories | The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location. | • | The lack of information available for software and hardware assets will likely prevent the combination of these two inventories from being particularly helpful. |
| 2.6 | Address Unapproved Software | Ensure that unauthorized software is either removed or the inventory is updated in a timely manner. | | Enterprises are often unable to control the software that is running on an IoT device.. |
| 2.7 | Utilize Application Whitelisting | Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. | | This capability is unavailable on most IoT devices, many of which will lack the processing power or security architecture to perform whitelisting. |
| 2.8 | Implement Application Whitelisting of Libraries | The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process. | | Whitelisting individual libraries is typically not available on IoT devices. |
| 2.9 | Implement Application Whitelisting of Scripts | The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system. | | Whitelisting individual scripts is typically not available on IoT devices. |
| 2.10 | Physically or Logically Segregate High Risk Applications | Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization. | | IoT devices are generally embedded devices, meaning that an enterprise will not have the ability to identify what applications are running on the IoT device. Additionally, they will not be able to isolate applications from one another. |

CIS Control 3: Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

IoT Applicability

Vulnerability monitoring and management are applicable to IoT devices, but it is a much more difficult challenge in this context than with traditional systems or even mobile devices. Just as with other devices on a network, regularly scheduled vulnerability assessments should be conducted to determine non-secure configurations that lead to elevated threats to the enterprise. These security holes should be remediated quickly, and the processes used for remediation should be fed back into the organization's best practices for secure IoT device deployment.

IoT Challenges

Active vulnerability assessments of IoT devices in an operational environment may be dangerous, as they can lead to system instability or failure. Ideally, how the device will behave when scanned will be known before it is scanned. As an alternative, passive vulnerability assessment can be one way to get the vulnerabilities identified without the risk of harming the operational environment. These assessments can be done manually or with automated tools sold by a third-party vendor. Although many IoT devices will be deployed internally, and not directly exposed to the internet, it may be a worthwhile exercise to routinely scan your organization using tools like Shodan or Censys. These tools can detect externally exposed devices and help administrators either remove or properly configure them.

IoT Additional Discussion

For the subset of IoT devices that receive security patches from their vendor, they should be kept up-to-date. Outdated firmware and software often contain exploitable vulnerabilities that an attacker could leverage to access enterprise data.

A laboratory test environment may be appropriate for regularly scheduled assessments against new threats and new IoT software configurations. Collaborative threat laboratories (e.g., sponsored by an Information Sharing & Analysis Center [ISAC] or other industry body) and IoT vendor laboratories may be the best venues for implementing this Control. As with other hardware and software vulnerabilities, these new vulnerabilities should also be evaluated against the organization's risk appetite to determine when a particular device or device class can no longer be supported on the network, or when it must be isolated in some fashion.

| CIS Control 3: Continuous Vulnerability Management | | | Applicability | |
|--|--|--|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 3.1 | Run Automated Vulnerability Scanning Tools | Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems. | • | Vulnerability assessment tools can be utilized in an automated manner for IoT systems, although how a device will respond should be known beforehand, especially if the system undergoing scan is critical to operations and needs to be available. |
| 3.2 | Perform Authenticated Vulnerability Scanning | Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. | | Accounts for these types of scans are unavailable on typical consumer-grade IoT devices. Authenticated accounts are generally associated with managing configurations and settings on the device. On-device vulnerability scanning applications are not generally available for IoT. |
| 3.3 | Protect Dedicated Assessment Accounts | Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. | • | Accounts used within vulnerability scanning tools for IoT devices need to be protected in a manner similar to other high-value administrative accounts. |
| 3.4 | Deploy Automated Operating System Patch Management Tools | Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. | | Many IoT devices cannot be updated via a centralized tool. If updates are available at all, they generally need to be individually updated. It is often difficult to separate operating system level patches from the application providing the device's primary function. |

| CIS Control 3: Continuous Vulnerability Management | | | Applicability | |
|--|--|---|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 3.5 | Deploy Automated Software Patch Management Tools | Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. | | Many IoT devices cannot be updated via a centralized tool. If updates are available at all, they generally need to be individually updated. It is often difficult to separate operating system level patches from the application providing the device's primary function. |
| 3.6 | Compare Back-to-Back Vulnerability Scans | Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. | • | Enterprises using IoT devices will benefit from checking current IoT vulnerabilities within a network against historical data and vulnerability trends. |
| 3.7 | Utilize a Risk-Rating Process | Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. | • | Administrators and security professionals will benefit from rating IoT device vulnerabilities. The Common Vulnerability Scoring System (CVSS) does not differentiate between system types and is applicable to IoT devices and any management or administration systems. |

CIS Control 4: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

IoT Applicability

Very few IoT devices include administrative accounts for management of the system. In some situations, especially with enterprise or consumer-grade IoT devices, control or pseudo-administrative access can be obtained through management applications on mobile devices.

IoT Challenges

Ensure that when evaluating IoT components for use in the enterprise, you investigate the controls associated with administrative accounts, to include the type of authentication supported – which will most likely be passwords – and the strength of the authentication implementation. For administrator accounts, attempt to ensure that, at a minimum, strong password requirements are used, and account access is audited. In addition, when feasible, attach the IoT component to a directory, allowing for the use of domain administrator accounts when needed. This will allow for the ability to more easily restrict the use of administrative privileges.

Administrators should be extremely careful when first working with a completely unmanaged device.

IoT Additional Discussion

Many IoT devices are deployed in insecure areas (e.g., roadside units, or RSUs, in the transportation sector). These devices are sometimes deployed with shared accounts that are used by technicians to manage the devices. Consider alternative methods for restricting administrative access to devices. For legacy devices without privileged access capability, a compensating control may be applied, such as additional physical security. Newly designed IoT devices and subsystems should integrate use of this Control.

Attackers may attempt to obtain administrator rights via operating system (OS) or firmware level vulnerabilities so they can hide themselves from the user. This entire CIS Control is difficult to enforce on a rooted device that has its security architecture broken. Although this may provide a user with root access, they often have default administrator credentials that do not frequently change. Furthermore, if an administrator is able to change their password, it is recommended they comply with the password requirements set forth by National Institute of Standards and Technology (NIST) SP 800-63-3. This means that memorized secrets (i.e., passwords) chosen by a subscriber (i.e., human) should be at least 8 characters long. To the extent practical in IoT, multifactor authentication (MFA) should always be used.

| CIS Control 4: Controlled Use of Administrative Privileges | | | Applicability | |
|--|---|--|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 4.1 | Maintain Inventory of Administrative Accounts | Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | If an IoT management system is available, which is rare, an inventory of the account accessing that system should be maintained. Local administrative accounts are often not available within IoT. |
| 4.2 | Change Default Passwords | Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. | • | All default passwords should be changed to prevent unauthorized access to the device. |
| 4.3 | Ensure the Use of Dedicated Administrative Accounts | Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities. | • | Where possible, administrative accounts or accounts controlling a device should use unique accounts with dedicated administrative passwords. |
| 4.4 | Use Unique Passwords | Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. | • | Administrative accounts for management applications should use unique passwords. |
| 4.5 | Use Multi-Factor Authentication for All Administrative Access | Use multi-factor authentication and encrypted channels for all administrative account access. | | Two-factor authentication (2FA) is not generally available when managing or using an IoT device. |

| CIS Control 4: Controlled Use of Administrative Privileges | | | | Applicability |
|--|---|---|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 4.6 | Use Dedicated Workstations for All Administrative Tasks | Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading email, composing documents, or browsing the Internet. | | This presents significant challenges as many IoT management consoles are publicly accessible web applications. |
| 4.7 | Limit Access to Scripting Tools | Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities. | | IoT environments do not commonly offer these types of capabilities. |
| 4.8 | Log and Alert on Changes to Administrative Group Membership | Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. | | Group memberships generally do not exist in IoT. |
| 4.9 | Log and Alert on Unsuccessful Administrative Account Login | Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account. | • | This may be an option within a management console. Where possible, it should be enabled to monitor breach attempts. |

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement, and actively manage (track/report on/correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

IoT Applicability

A majority of the time, resource constrained IoT devices lack the configuration and customization options provided by laptops or even mobile devices. Yet some devices can still be hardened in a limited fashion. This is true even of embedded IoT devices. A common example is changing default passwords. End users should familiarize themselves with the developer's or manufacturer's documentation for a device and also take advantage of other available resources (e.g., academic papers, conference proceedings) to understand what configuration options are available and whether a device can be sufficiently configured to meet your needs.

IoT Challenges

A device or application's configuration may drift over time, even if efforts are made to properly configure the device before or during deployment. This could be due to software updates, factory resets, or potentially even software errors. Some IoT device configurations, especially for consumer or typical enterprise use, are *solely* available within a corresponding mobile application. Users will need to first connect the device to the application before configuration is an option. Although this can make device configuration, monitoring, and maintenance easier, it also expands the overall attack surface of the device as now the mobile device (and mobile application) must also remain secure. Undocumented APIs and backdoors may offer original equipment manufacturers (OEMs) and potentially malicious parties access to the device, and subsequently consumer or enterprise information. For instance, many IoT devices run a web server with network troubleshooting tools installed (e.g., *ping*, *nslookup*) that can be used to profile any internal or external network to which the IoT device is connected.

IoT Additional Discussion

IoT devices sold and marketed as “appliances” with integrated software generally contain proprietary software components, limiting applicability of post-development hardening. When configuration options are available, cybersecurity professionals should review and decide if any particular configurations are untenable for your organization. Additionally, if a certain configuration setting is required to assure the security of the component on the network, then that should also be documented. Cybersecurity professionals should baseline these configurations and keep them documented as best practices. This information can be helpful as requirements when selecting future devices.

A subset of IoT devices support real-time operating systems (RTOSs) that allow for some amount of persistent storage. Oftentimes, this persistence comes in the form of startup scripts that can be modified to affect the configuration of the device at boot time. It is worthwhile to take the time to research if these configurations are written in a secure manner. When IoT devices support access control via user or administrator accounts and passwords, default accounts and passwords should be changed, and sound password update and strength guidelines promoted. If available, MFA should be used to protect administrator accounts.

| CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | | | | Applicability |
|--|--|--|---|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 5.1 | Establish Secure Configurations | Maintain documented security configuration standards for all authorized operating systems and software. | <ul style="list-style-type: none"> • | Secure configurations generally cannot be established in the same manner as traditional operating systems or applications. With that said, there may be certain configuration options available such as changing a default password or ensuring MFA is used to access any management functions. |
| 5.2 | Maintain Secure Images | Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates. | | This is not possible for IoT devices. |
| 5.3 | Securely Store Master Images | Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible. | | Maintaining secure images is generally unfeasible for IoT, and accordingly images for IoT devices cannot be securely stored. |
| 5.4 | Deploy System Configuration Management Tools | Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. | <ul style="list-style-type: none"> • | A select few IoT gateways or management platforms may be able to manage basic settings, but this is not commonly available. |
| 5.5 | Implement Automated Configuration Monitoring Systems | Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. | | This feature is unavailable for IoT management tools. |

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

IoT Applicability

Logs on IoT devices can take a variety of formats, and there are no uniform standards for how to store and transfer data. Each OEM is free to create their own format, making integrations from multiple vendors within the same network difficult. Furthermore, devices may not be configured to log events; they may store logs locally on the device; or they may be sending them off to a local gateway or cloud platform. Organizations should ensure that IoT devices create detailed logs and many IoT devices have this capability. Additionally, a trusted method of extracting and parsing audit logs from relevant components should be available. However, this may prove challenging in some instances where OS and application logs are not enabled or available. To the degree possible, the default stance should always be to attempt to collect these logs.

IoT Challenges

Having logs from IoT devices is one measure of success but means little to an organization's cybersecurity posture if they are not being reviewed on a regular basis. Another challenging area related to IoT security is how to integrate large security data from large quantities of components into an enterprise's Security Information and Event Management (SIEM) system. The creation of custom connectors should be investigated when IoT components do not provide standards-based log output. Just as important is a focus on how to make sense of the IoT log data when combined with standard network data captured by the SIEM. The establishment of rules that correlate this diverse data effectively will be an interesting challenge moving forward. Cloud-based analysis may be a potential solution to these challenges.

Additionally, many developers are worried about logging too often to flash memory, which can potentially lead to excessive wear on the flash memory modules. This is an open problem, and developers must attempt to strike their own balance based on customer need.

IoT Additional Discussion

Legacy IoT systems are designed for reliable operations and rapid recovery. Accordingly, some of these systems include the ability to generate logs, which may be sufficient. Command and control subsystems may use alternative, out-of-band logging of activities that should be considered when assessing the need for a separate control.

| CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs | | | | Applicability |
|---|---|---|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 6.1 | Utilize Three Synchronized Time Sources | Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent. | | Developers of IoT devices may be able to design individual applications to utilize additional time sources, but this is an extremely uncommon feature. |
| 6.2 | Activate Audit Logging | Ensure that local logging has been enabled on all systems and networking devices. | <ul style="list-style-type: none"> • | Where possible, IoT devices should have audit logging enabled. |
| 6.3 | Enable Detailed Logging | Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. | <ul style="list-style-type: none"> • | The level of detail offered by a platform is generally set in stone pending major updates from the device manufacturer. |
| 6.4 | Ensure Adequate Storage for Logs | Ensure that all systems that store logs have adequate storage space for the logs generated. | <ul style="list-style-type: none"> • | This is particularly important for IoT devices with constrained memory storage. It is difficult to ascertain before a purchase if a device contains sufficient local storage capacity for detailed event logs. If sufficient storage is not available, old logs may be written over. Another solution is to send the logs off-device to a gateway or cloud platform. |
| 6.5 | Central Log Management | Ensure that appropriate logs are being aggregated to a central log management system for analysis and review. | <ul style="list-style-type: none"> • | Log management at scale can provide useful information about the state and health of fielded devices. This information should be stored and processed via a single resource. |

| CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs | | | | Applicability |
|---|-----------------------------------|--|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 6.6 | Deploy SIEM or Log Analytic Tools | Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis | <ul style="list-style-type: none"> • | SIEMs can help to correlate security events occurring on IoT devices with mobile, server, network appliances, or other events within the enterprise network. |
| 6.7 | Regularly Review Logs | On a regular basis, review logs to identify anomalies or abnormal events. | <ul style="list-style-type: none"> • | Logging is one thing, and reviewing them is another. After an incident occurs, logs can provide some of the most valuable sources of information. SIEMs and other automated log analysis tools can also help to identify small issues before they become large problems. |
| 6.8 | Regularly Tune SIEM | On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise. | <ul style="list-style-type: none"> • | Customizing rules and alerts to your enterprise's unique needs is important. |

CIS Control 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

IoT Applicability

IoT devices generally do not use email or external web browser applications or interfaces, although some stand-alone IoT management systems may leverage standard web browser technologies for visualization and a common user experience. The majority of IoT devices will use email and browsers in a "headless" fashion.

IoT Challenges

Some devices will run a web server in order to support Representational State Transfer (RESTful) web services. It is uncommon to be able to apply hardening guidance (e.g., CIS Benchmarks) to these devices.

IoT Additional Discussion

IT equipment that is used to transfer or bridge data between an IoT network and an IT corporate or other non-IoT operational network may incorporate email or web browser functionality. These applications should be protected according to best practice. In cases where web browser technologies are incorporated in stand-alone IoT networks, a risk analysis should be performed to address the need to update the applications when patches and new versions are released.

| CIS Control 7: Email and Web Browser Protections | | | | Applicability |
|--|---|---|--|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 7.1 | Ensure Use of Only Fully Supported Browsers and Email Clients | Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. | <ul style="list-style-type: none"> | Although browsers and email clients should be kept up-to-date, it is difficult to do this for IoT devices. Enterprises should attempt to verify that updates are regularly applied to IoT devices. |
| 7.2 | Disable Unnecessary or Unauthorized Browser or Email Client Plugins | Uninstall or disable any unauthorized browser or email client plugins or add-on applications. | | Email client and browser plugins generally do not exist for IoT devices. |
| 7.3 | Limit Use of Scripting Languages in Web Browsers and Email Clients | Ensure that only authorized scripting languages are able to run in all web browsers and email clients. | | Obtaining this level of granularity is often not possible. |

| CIS Control 7: Email and Web Browser Protections | | | Applicability | |
|--|---|--|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 7.4 | Maintain and Enforce Network-Based URL Filters | Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. | <ul style="list-style-type: none"> • | Network-based proxies, firewalls, and other proxies can be configured for IoT devices, or specifically support capabilities to filter IoT traffic. Content blockers can be developed for certain applications. |
| 7.5 | Subscribe to URL-Categorization Service | Subscribe to URL-categorization services to ensure that they are up to date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. | | In order for this mitigation to be put into place, it would have to be done at the network level. |
| 7.6 | Log All URL Requests | Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems. | | In order for this mitigation to be put into place, it would have to be done at the network level. |
| 7.7 | Use of DNS Filtering Services | Use Domain Name System (DNS) filtering services to help block access to known malicious domains. | | In order for this mitigation to be put into place, it would have to be done at the network level. |
| 7.8 | Implement DMARC and Enable Receiver-Side Verification | To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards. | | Although DMARC is an important Sub-Control, there is little to be done specifically on IoT devices to enable this mitigation. |
| 7.9 | Block Unnecessary File Types | Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business. | | This is generally not possible with common IoT devices. |
| 7.10 | Sandbox All Email Attachments | Use sandboxing to analyze and block inbound email attachments with malicious behavior. | | Email is typically used as an egress data transfer method and receiving email attachments may not be possible. |

CIS Control 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

IoT Applicability

Malware most certainly affects IoT devices, as seen with recent, high-profile attacks utilizing distributed denial of service (DDoS) and explored in greater detail in the paper [DDoS in the IoT: Mirai and Other Botnets](#). Both malware and exploits are now tailored to affect IoT devices and platforms, which highlights the need for a robust strategy to defend against malware and malicious code.

IoT Challenges

Given the limited processing ability and limited power capacity of many IoT components, host-based malware protections may consume too many cycles and too much energy, necessitating alternative protections. Using commercial, network-based malware detection systems (e.g., in-line monitoring) may not be feasible due to latency requirements or the use of non-IP protocols, but this is changing. IoT-specific network monitoring devices are beginning to be available for both enterprises and consumers. Continuous monitoring at corporate or other gateways through which IoT device information (updates and/or data) flows may be used to detect adversary malware or to correlate observed activity with known, legitimate, and/or planned activity.

IoT Additional Discussion

Traditional anti-malware techniques are not feasible on IoT devices. At the very least, preventing your IoT devices from being publicly exposed to and facing the internet will act as a barrier of sorts.

A primary attack vector for malware against an IoT device is through maintenance action of a new IoT device software load (also known as the software or firmware update process). Supply chain risk management can help to address these risk factors. Additionally, periodic validation of IoT device operation via alternative information channels (e.g., analog records, operational anomaly detection through long-term analytics) may be possible but will require collection and long-term storage of what is normally perishable data.

In certain industries where availability is the overriding concern (e.g., healthcare, energy), IoT devices may be uniquely vulnerable to DDoS. Anti-malware tools and techniques should be properly regression-tested to ensure that availability and reliability of the system will not be adversely affected. Additionally, all anti-malware tools should be configured such that a false positive detection will not negatively impact the availability or reliability of any critical processes. Testing may need to occur whenever a change is made to the anti-malware software such as a configuration change, software hotfix, or repository update. It is important to understand the attack patterns used to affect IoT devices in your industry.

Another product category that can assist in defense against the threat of malware is threat intelligence focused on IoT devices. These services review Tactics, Techniques, and Procedures (TTPs) and provide a risk rating or threat score to analysts based on behavior and other factors.

Finally, whitelisting of software can provide malware protection by preventing malicious code from executing in the first place.

| CIS Control 8: Malware Defenses | | | Applicability | |
|---------------------------------|--|---|---|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 8.1 | Utilize Centrally Managed Anti-Malware Software | Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | <ul style="list-style-type: none"> • | It can be difficult to find anti-malware products that also integrate with solutions already being used within an enterprise. Regardless of whether the solution is centrally managed or not, a plan for dealing with malware, including incident response, should be in place prior to the introduction of IoT. |
| 8.2 | Ensure Anti-Malware Software and Signatures Are Updated | Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis. | <ul style="list-style-type: none"> • | As with other solutions, the ways in which malware behaves (e.g., initial infection vectors) may change over time. Updating centrally managed anti-malware software will keep the defenses up-to-date against new threats. |
| 8.3 | Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies | Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. | | These are either enabled by default on the operating system or they are not. Unfortunately, IoT devices typically do not have these features enabled. If these important anti-exploit technologies are necessary, verification of these features in IoT devices should be conducted before purchase and implementation. |
| 8.4 | Configure Anti-Malware Scanning of Removable Media | Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. | | IoT devices do not typically have physical ports for removable devices and cannot perform scanning activities. |

| CIS Control 8: Malware Defenses | | | Applicability | |
|---------------------------------|---|--|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 8.5 | Configure Devices to Not Auto-Run Content | Configure devices to not auto-run content from removable media. | | IoT devices typically do not have these features enabled. If this is necessary, verification of these features in IoT devices should be conducted before purchase and implementation. |
| 8.6 | Centralize Anti-Malware Logging | Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting. | • | Logs associated with IoT devices should be collected and analyzed to the degree possible. |
| 8.7 | Enable DNS Query Logging | Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains. | | If this capability exists within an enterprise's network, it should also work for IoT devices with the necessary networking protocols without a change from the enterprise. |
| 8.8 | Enable Command-Line Audit Logging | Enable command-line audit logging for command shells, such as Microsoft® PowerShell and Bash. | | Interacting with the device via a command line interface is often not supported for IoT. |

CIS Control 9: Limitation and Control of Network Ports, Protocols and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

IoT Applicability

Most IoT devices communicate via specific ports and protocols just as other IT assets, though some embedded devices and sensors are not fully *network aware*. Defining allowable ports, protocols, and services that may be used by IoT devices must be performed and then enforced. However, IoT devices may implement other communication protocols that do not ride over the corporate network. As an example, IoT devices that implement Bluetooth could be used as a jumping-off point for an attacker, and, once exploited, allow the attacker to move to a nearby target that does not have Bluetooth locked down. It is important to fully understand the protocols employed by each IoT device, which of those protocols are allowed within an enterprise, and then design an overarching security strategy that mitigates the risk associated with these implementations.

IoT Challenges

IoT network traffic is highly predictable and repetitious, in comparison with commodity enterprise traffic. Commercial and/or industrial IoT traffic generally leverages a private network or specific and unchanging ports, protocols, and services on a corporate network. IoT devices may be tested to assess their susceptibility to messaging that does not conform to expectations; related risks may be mitigated through application of this Control.

Vendors may require internet access to IoT devices or subsystems to support and verify licensing or maintenance agreements, or to perform maintenance or support; such access should be monitored and limited. Another challenge of securing IoT is related to employees, customers, or others bringing consumer IoT devices into the enterprise. Research has shown that employees often associate IoT software on their corporate assets (laptops or phones) with their personal IoT devices (e.g., fitness trackers), or bring their personal IoT devices directly into the network (e.g., smart speaker or digital assistant). This opens up command and control channels between the device's installed software or hardware and internet sites used for data collection or management. Organizations should monitor for personal IoT-related traffic and take actions to deny that traffic when necessary.

IoT Additional Discussion

A related concept to this Control is the management of various network interfaces, such as WiFi, Bluetooth, or Near Field Communications (NFC). These should be managed, as WiFi, Bluetooth, and cellular beacons/advertisements may broadcast the presence of any IoT device to the surrounding area. For example, specific mobile applications may be directly correlated to an open port on Android. Accordingly, removing superfluous applications on any mobile OS is an attack surface reduction approach. Additional attack surface reduction activities can likely be done in high-risk scenarios, specifically for Android, but this is not a traditional approach. Interfaces should be limited to only those required for the necessary purpose. Any management platforms used for administering IoT devices should be treated as regular servers and scanned accordingly alongside other enterprise systems.

| CIS Control 9: Limitation and Control of Network Ports, Protocols and Services | | | | Applicability |
|--|--|---|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 9.1 | Associate Active Ports, Services, and Protocols to Asset Inventory | Associate active ports, services, and protocols to the hardware assets in the asset inventory. | • | Although the ports that are listed may not be directly associated with services running on a device, it is worthwhile to understand which ports are considered baseline for any enterprise devices and monitor for changes. |
| 9.2 | Ensure Only Approved Ports, Protocols, and Services Are Running | Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system. | • | This can be impractical for many embedded IoT devices, but the usage of IoT gateways can act to firewall or segment IoT devices from the larger network and decrease overall exposure. |
| 9.3 | Perform Regular Automated Port Scans | Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system. | • | Just as with traditional systems, automated port and other types of network scans should be performed. |
| 9.4 | Apply Host-Based Firewalls or Port-Filtering | Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. | | The privileges to do such a thing are generally not available on mobile operating systems. |
| 9.5 | Implement Application Firewalls | Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged. | | Host-based application firewalls are generally not available on IoT products. |

CIS Control 10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

IoT Applicability

Many IoT devices may provide onboard storage for data and logs, though some IoT devices do not. Devices that store data may transfer it to dedicated network storage locations for near-term or permanent storage. This can be done periodically or in near real-time. When taking an inventory of the types of IoT devices to be used within an enterprise, it is important to understand whether data is at risk of being lost at any given point in the architecture and to devise a plan for ensuring that data can be recovered in case of component failure.

IoT Challenges

Backing up IoT data can be very difficult as traditional backup strategies simply will not work. For instance, even simple utilities such as `rsync` will not be available and are therefore not a valid option. However, native backup capabilities may be present, and those should be understood before purchase and be implemented accordingly. Native capabilities may automatically back up to the cloud or a phone, and enterprises should understand this before implementation.

IoT Additional Discussion

When IoT message traffic is perishable and temporary, the value of data recovery is limited to maintenance actions. Data recovery capabilities may be required for operational data at consolidation and action points for compliance or maintenance purposes. Security engineers should understand that some IoT devices maintain data until an online connection (e.g., via Bluetooth, WiFi, etc.) is established with a gateway application. In these instances, sensitive data may continue to be resident on the device and may require a recovery capability.

Organizations should verify and review backup settings from the device manufacturer, including any associated service within the IoT ecosystem, to make sure the proper information is backed up and that improper information is not backed up. Proper authentication mechanisms should be in place to protect any enterprise cloud backup. IoT devices may also unintentionally back up information to any desktop environment they are connected to, including gateways or mobile devices. The creation of these backups should be prevented unless specifically authorized by the enterprise.

| CIS Control 10: Data Recovery Capabilities | | | Applicability | |
|--|---|--|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 10.1 | Ensure Regular Automated Backups | Ensure that all system data is automatically backed up on a regular basis. | • | Users should regularly back up enterprise IoT data to approved backup locations. This includes backing up monitoring and administration-oriented data, such as logs that are stored on a system separate from the IoT device. |
| 10.2 | Perform Complete System Backups | Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system. | | IoT devices generally lack the notion of a system image, and information is often needed to be configured and backed up on a per-application basis. |
| 10.3 | Test Data on Backup Media | Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working. | • | Employees and administrators should regularly perform tests of restoring backed up data. An easy way of testing this is going through the motions of provisioning a new phone or application to a new device. |
| 10.4 | Protect Backups | Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services. | • | Some cloud-based services will do this automatically, but users and enterprises need to check on the mitigations in place before electing to use a service. Any removable media for the device, alongside desktop backups, also needs to be protected. |
| 10.5 | Ensure All Backups Have at Least One Offline Backup Destination | Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination. | | Ransomware and its related offshoots (e.g., destructive malware) typically perform malicious activities on the device itself. This includes preventing access to the device, yet it rarely affects third-party cloud storage providers. |

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Establish, implement, and actively manage (track/report on/correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

IoT Applicability

This Control is not directly applicable to IoT devices but is relevant for the security of certain types of IoT gateways (e.g., small office, home office [SoHo] routers used as IoT gateways) as well as for the secure usage of general network devices. There is guidance on WiFi security, but it applies to all computing devices and not necessarily IoT. When there is a plan to do a medium- to large-scale deployment of IoT devices within an enterprise, take the opportunity to review the configurations for firewalls, routers, and switches to ensure that additional vulnerabilities are not introduced through misconfiguration. Additionally, take care to revisit the guidance provided within CIS Control 9 (*Limitation and Control of Network Ports, Protocols and Services*).

IoT Challenges

Legacy IoT systems may favor proprietary byte-oriented protocols, but legacy systems that migrate to TCP/IP (e.g., Modbus TCP) are often fragile and insecure. The absence of commercially available network devices for legacy networks limits the value of this Control for those networks.

IoT Additional Discussion

Newer IoT devices often use RESTful APIs that require supporting web services be implemented securely. In addition, many IoT devices implement IPv6 communications and sometimes use protocols such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) to support the ability for constrained IoT devices to connect to the internet. The introduction of IPv6 opens a whole new set of security considerations across network devices for operation in a secure manner.

| CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches | | | Applicability | |
|---|---|--|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 11.1 | Maintain Standard Security Configurations for Network Devices | Maintain documented security configuration standards for all authorized network devices. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |
| 11.2 | Document Traffic Configuration Rules | All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |
| 11.3 | Use Automated Tools to Verify Standard Device Configurations and Detect Changes | Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |

| CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches | | | Applicability | |
|---|--|---|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 11.4 | Install the Latest Stable Version of Any Security-Related Updates on All Network Devices | Install the latest stable version of any security-related updates on all network devices. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |
| 11.5 | Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions | Manage all network devices using multi-factor authentication and encrypted sessions. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |
| 11.6 | Use Dedicated Workstations for All Network Administrative Tasks | Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |
| 11.7 | Manage Network Infrastructure Through a Dedicated Network | Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. | | See the <i>Applicability</i> statement above. This Control is not directly applicable to IoT. |

CIS Control 12: Boundary Defense

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

IoT Applicability

This is a particularly important control for IoT devices, and strategies for traditional boundary defense apply. Defenses and mitigations, such as network monitoring tools, email security, intrusion detection system (IDS) and intrusion prevention system (IPS) alerts, logging of events and alerts and virtual private network (VPN) concatenators, are all important and should be utilized to the extent possible. These can be implemented in segmented networks where IoT devices are utilized and routed instead of through the trusted enterprise network. Controlling the flow of information within a network is important.

IoT Challenges

IoT devices are increasingly being used in stand-alone scenarios or connected to cloud-based platforms. Full infrastructures dedicated to IoT may be needed that support capture, processing, and analysis of data from IoT endpoints in the cloud. In addition, IoT devices may share and collate information from many different organizations. For cloud-based systems that support IoT, consider cloud security best practices, and move to a data-centric security approach to support the sharing of IoT data across many different organizations. The [CIS Controls™ Cloud Companion Guide](#) offers additional guidance for securing cloud environments.

As discussed in other Controls within this guide, the use of segregation strategies is recommended to keep IoT components operating in their own zones or on their own separate networks. In cases where there must be a connection point between an IoT segment and the corporate network, boundary defense mechanisms must be put in place. Firewalls, IDS, and IPS can provide assurance that a compromise of the less-trusted IoT network will have limited effect on the more secure corporate network.

IoT Additional Discussion

In many instances, a decision will be made to place IoT devices outside of the trusted network boundary. Even with the few devices utilizing data-in-transit encryption with vetted algorithms and reasonable key sizes, certain types of traffic will be leaked. Examples of this type of information may include diagnostic information about the device, OS traffic back and forth with the ecosystem provider, and wireless traffic using WiFi, Bluetooth, and cellular networks. These types of information leaks allow passively sniffing malicious actors to fingerprint the device. Some devices may automatically attempt to access or connect to WiFi networks to which they have previously been associated. Blacklisting certain service set identifiers (SSIDs) on devices, such as those from major retailers and cafes, can help prevent an IoT device from accessing a rogue version of that network and sending sensitive enterprise data over it. Many enterprises will use a combination of network segmentation approaches for better vetted devices that provide critical enterprise functions.

| CIS Control 12: Boundary Defense | | | | Applicability |
|----------------------------------|---|--|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 12.1 | Maintain an Inventory of Network Boundaries | Maintain an up-to-date inventory of all of the organization's network boundaries. | <ul style="list-style-type: none"> • | Network boundaries with insecure, legacy, or untrusted devices should be inventoried and monitored. |
| 12.2 | Scan for Unauthorized Connections Across Trusted Network Boundaries | Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary. | <ul style="list-style-type: none"> • | IoT devices may be making connections to networks not approved by the enterprise. This could be due to malware, misconfiguration, or by design. |
| 12.3 | Deny Communications with Known Malicious IP Addresses | Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries. | | This is generally impractical to implement on an IoT device. This is more generally possible at the IoT gateway or network level. |
| 12.4 | Deny Communication Over Unauthorized Ports | Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries. | | Botnets and other malware distribution nodes that are specific to IoT should be administered at the organization level. This Sub-Control is better and more easily enforced when IoT devices are taking advantage of an IoT gateway. |
| 12.5 | Configure Monitoring Systems to Record Network Packets | Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries. | | Although this Sub-Control is quite useful, this is generally not an IoT-specific configuration, although some developer options may support this. |

| CIS Control 12: Boundary Defense | | | | Applicability |
|----------------------------------|--|--|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 12.6 | Deploy Network-Based IDS Sensors | Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries. | • | Enterprises can ensure that signatures and other information used by the IDS are IoT-specific, and that their IDS is "IoT aware." This Sub-Control is better and more easily enforced when an IoT gateway is in use or when devices route traffic through the enterprise. |
| 12.7 | Deploy Network-Based Intrusion Prevention Systems | Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. | • | Enterprises can ensure that any relevant IPS is "IoT aware." This Sub-Control is better and more easily enforced when an IoT gateway is in use or when devices route traffic through the enterprise. |
| 12.8 | Deploy NetFlow Collection on Networking Boundary Devices | Enable the collection of NetFlow and logging data on all network boundary devices. | | This is a useful Sub-Control yet there is nothing specific to IoT within its scope. |
| 12.9 | Deploy Application Layer Filtering Proxy Server | Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections. | | Although this Sub-Control is quite useful, there is nothing specific to IoT about it. |
| 12.10 | Decrypt Network Traffic at Proxy | Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic. | • | This is most easily done when an IoT gateway is in use or when devices route traffic through the enterprise. |
| 12.11 | Require All Remote Logins to Use Multi-Factor Authentication | Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication. | • | VPN applications and their back-end components can integrate with external authentication services and identity providers. |
| 12.12 | Manage All Devices Remotely Logging Into Internal Network | Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices. | • | Administrators should attempt to obtain some degree of control over the security and configuration of any IoT devices accessing an internal network. |

CIS Control 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

IoT Applicability

Protecting the security of data being stored, transmitted, and manipulated on IoT devices can be critical depending on use case or sector. Certain industries may not contain any sensitive data in the traditional sense. In other instances, certain IoT devices will be dedicated to environments that have an informal set of standards and norms, or their usage may be directly regulated (e.g., Payment Card Industry Data Security Standard [PCI DSS], Health Insurance Portability and Accountability Act [HIPAA], General Data Protection Regulation [GDPR]). The level of data protection needed is often specific to the use case at hand, depending on factors such as data sensitivity and likelihood of exposure.

Some IoT devices will process and transmit complex enterprise or customer information in modern formats, whereas other devices will read and transmit physical attributes such as temperature or pressure. This latter information is sometimes not deemed to be especially sensitive or proprietary on its own, though it may become more sensitive when coupled with other data points, such as location. In some cases, these “simple” IoT use cases can be absent of any particular protections in the way it is collected, transferred, stored, and analyzed.

IoT Challenges

Detecting and preventing the flow of data out of IoT devices is a difficult task, as is preventing unauthorized disclosure. IoT devices will often have a diverse supply chain, utilizing numerous hardware manufacturers alongside cloud services. This makes data protection that much more difficult. If possible, data-in-transit security, through protocols such as IPsec or Transport Layer Security (TLS), must be implemented to guard against eavesdropping on data flowing between IoT and other enterprise components. This is difficult as most IoT devices will ship with a set of security protocols that are supported, and this may never change over the lifetime of the device.

Protections must also be implemented for the data stored on any cloud platform or the device itself, including integrated memory or removable storage media. This is another area typically outside of enterprise control and may need to be screened for pre-purchase if it is a necessary enterprise security control, as does any IoT device's ability to manage cryptographic keys.

IoT Additional Discussion

Legacy or low-end IoT devices often do not encrypt data in transit or in storage. Typically, IoT traffic is perishable, near real-time, of limited historical value, and tolerant of loss. Sophisticated attacks looking to manipulate data often require deep system knowledge and serious mission benefit to justify the cost of technique and exploit development. In cases where actual threats or observed threat intelligence indicates the need, methods such as multi-path redundancy, cross-sensor correlation, or a custom in-line device may be put into place. Many IoT devices will attempt to store data in the cloud by default without enterprise approval. This may also include storing data on any mobile devices used to control a device. This makes data protection hard, as enterprises may not have visibility into what information is being transmitted.

Traditional enterprise data loss protection (DLP) systems can be helpful for email and network stored data. It is important to perform methodical threat modeling for every new IoT system being

implemented. Consider the value of, and the threats to, data when determining whether encryption should be applied to protect that data. In some instances, the need to support near real-time communications outweighs the need to apply an encryption layer to the data. The output of a threat analysis will provide the foundation for an effective data protection strategy.

| CIS Control 13: Data Protection | | | | Applicability |
|---------------------------------|---|---|-----------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 13.1 | Maintain an Inventory of Sensitive Information | Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider. | • | Sensitive information on IoT devices should be recorded and inventoried. |
| 13.2 | Remove Sensitive Data or Systems Not Regularly Accessed by Organization | Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed. | • | These could include unused IoT devices, third-party cloud services, or unnecessary management systems or gateways. The implementation of this Sub-Control will depend on how the IoT devices are used. |
| 13.3 | Monitor and Block Unauthorized Network Traffic | Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals. | | Although an important Sub-Control, this is not specific to IoT. |
| 13.4 | Only Allow Access to Authorized Cloud Storage or Email Providers | Only allow access to authorized cloud storage or email providers. | • | This will often need to be decided before IoT device purchase. |
| 13.5 | Monitor and Detect Any Unauthorized Use of Encryption | Monitor all traffic leaving the organization and detect any unauthorized use of encryption. | | This can be extremely difficult for IoT, especially if the network is not "IoT aware." |

| CIS Control 13: Data Protection | | | Applicability | |
|---------------------------------|--|--|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 13.6 | Encrypt Mobile Device Data | Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices. | | This Control is specific to mobile. CIS provides the CIS Controls™ Mobile Companion Guide to assist with deploying mobile devices in the enterprise. |
| 13.7 | Manage USB Devices | If universal serial bus (USB) storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained. | | This generally does not affect IoT devices as USB storage devices are not utilized for IoT. |
| 13.8 | Manage System's External Removable Media's Read/Write Configurations | Configure systems not to write data to external removable media, if there is no business need for supporting such devices. | | In most cases this cannot be managed. |
| 13.9 | Encrypt Data on USB Storage Devices | If USB storage devices are required, all data stored on such devices must be encrypted while at rest. | • | IoT devices do not commonly utilize USB storage; however, other removable storage media (such as SD cards) might be used. Based on the sensitivity of stored data, encryption should be used to mitigate risks related to data theft and disclosure. |

CIS Control 14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

IoT Applicability

Authentication to IoT devices is sometimes not a built-in capability. This can cause significant problems for controlling access to enterprise data stored on IoT devices. Access control mechanisms should be in place for all entities accessing any IoT device, alongside any associated cloud service, web application, or mobile application. Sub-Controls relating to private VLANs may not be applicable, as are those relating to sensitive information or data.

IoT Challenges

Legacy IoT systems often lack automated access control functionality. If this is the case, organizations should still consider developing policies around secure usage of IoT devices, especially regarding which networks legacy IoT devices can access. Manual or physical security solutions that are consistent with an assessed risk profile can also be created. Similarly, determinations for enterprise data access should be made for all users, applications (including mobile applications), IoT devices, and any requisite management infrastructure. Plans should be in place to permanently remove or render device data inaccessible for all devices outside the physical perimeter of the enterprise.

IoT Additional Discussion

Organizations should look to purchase IoT devices that require, at a minimum, password protections and should ensure that passwords and authentication mechanisms should be able to be changed from their default setting. Additionally, passwords should be able to be set to a sufficient strength for a modern threat environment. In addition, organizations should work to integrate IoT component authentication with an enterprise authentication capability such as lightweight directory access protocol (LDAP) or active directory (AD) where practical. As a design goal for new IoT systems, IoT components should authenticate themselves to the network when joining.

Although traditional network security mitigations apply, holistic approaches to IoT security may need to include cellular security if a cellular modem is present. CIS provides the [CIS Controls™ Mobile Companion Guide](#) to assist with deploying mobile devices in the enterprise. Cellular networks are not always properly encrypted and authenticated, and, as the security of these networks is difficult to independently validate, enterprises can elect to use devices that can establish an authenticated and encrypted session back to the cloud service or enterprise. Although 3G universal mobile telecommunications system (UMTS) networks perform mutual authentication, the improvements made within 4G long-term evolution (LTE) systems are worthwhile to ensure that device and network properly authenticate each other. Enterprises should not count on 2G global system for mobile communication (GSM) networks for device authentication or encryption.

| CIS Control 14: Controlled Access Based on the Need to Know | | | | Applicability |
|---|---|--|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 14.1 | Segment the Network Based on Sensitivity | Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs). | • | Organizations should look to segment legacy IoT devices from modern IoT devices and all enterprise networks handling sensitive information. |
| 14.2 | Enable Firewall Filtering Between VLANs | Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. | | This is generally outside the scope of an IoT device. |
| 14.3 | Disable Workstation-to-Workstation Communication | Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as private VLANs or micro segmentation. | | The typical workstation does not fall within the scope of IoT. CIS Control 15 discusses the need for peer-to-peer (P2P) communication in certain use cases. |
| 14.4 | Encrypt All Sensitive Information in Transit | Encrypt all sensitive information in transit. | • | This is an important Sub-Control for IoT devices, but enterprises will need to verify if this capability is available for the specific device before device purchase. |
| 14.5 | Utilize an Active Discovery Tool to Identify Sensitive Data | Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory. | | This is not specific to IoT devices or their management platforms. |

| CIS Control 14: Controlled Access Based on the Need to Know | | | Applicability | |
|---|--|--|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 14.6 | Protect Information Through Access Control Lists | Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | | This is not specific to IoT devices. |
| 14.7 | Enforce Access Control to Data Through Automated Tools | Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when the data is copied off a system. | | This feature is generally not available on IoT systems. |
| 14.8 | Encrypt Sensitive Information at Rest | Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information. | • | This is an important Sub-Control for IoT devices, but enterprises will need to verify if this capability is available for the specific device before device purchase. |
| 14.9 | Enforce Detail Logging for Access or Changes to Sensitive Data | Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). | | This feature is generally not available on IoT systems. |

CIS Control 15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

IoT Applicability

Many IoT devices will make use of a variety of wireless communication protocols, although some rely on wired mediums, such as Ethernet, for functions like building automation controls and other use cases. Devices may use the global and ubiquitous highway addressable remote transducer (HART) protocol, while others use proprietary solutions with built-in access control.

Geographically distributed systems may use elements of cellular stacks. WiFi is a very common communication protocol for IoT devices, and controls can be implemented within the device and at the network level. Vulnerabilities may exist within the protocols being used or within the firmware used to connect and maintain a network connection.

IoT Challenges

Disabling wireless network interfaces can be a challenge as it is not normally a user-customizable option in off-the-shelf IoT devices. If there is a concern around the usage of wireless, it may be possible to perform radio frequency (RF) environment characterization and continuous RF monitoring to see if any pertinent interfaces are in use. IoT devices in the enterprise may implement several protocols, such as Zigbee, Z-Wave and Bluetooth Low Energy (BLE). To the extent possible, security engineers should ensure that only needed protocols are allowed within the organization. Regardless, proper network segmentation will be an ongoing challenge for IoT devices used within an enterprise.

IoT Additional Discussion

For wireless IoT devices, ensuring that only authorized devices/components connect to an enterprise wireless network is a first step in meeting the objectives of this Control. In order to accomplish this, an organization must first define the types of devices that are allowed to be connected to the enterprise network and which protocols are allowed to be used. IoT devices are susceptible to network-level man-in-the-middle attacks, such as TLS stripping and address resolution protocol (ARP) poisoning. These attacks can allow an attacker to sniff unencrypted traffic or reroute traffic to insecure websites, leading to potential credential theft. Some mobile threat defense (MTD) on-device agents can detect these attacks and notify a user and/or administrator. Developers can implement certificate pinning to help stop these types of network-based attacks as well. Traditional guidance on WiFi security applies, such as using strong credentials and restricting unauthorized device connectivity. If WiFi Protected Access 2 Pre-Shared Key (WPA2-PSK) is used, a strong password is necessary, although 802.1x is preferred.

| CIS Control 15: Wireless Access Control | | | Applicability | |
|---|--|---|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 15.1 | Maintain an Inventory of Authorized Wireless Access Points | Maintain an inventory of authorized wireless access points connected to the wired network. | • | The wireless access points used by enterprises will not be within scope for this Sub-Control, but any IoT gateways acting as a gateway for wireless IoT traffic will need to be inventoried. |
| 15.2 | Detect Wireless Access Points Connected to the Wired Network | Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network. | | Although important, there is nothing specific to IoT within this Sub-Control. |
| 15.3 | Use a Wireless Intrusion Detection System | Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network. | | Traditional IDS technology has not necessarily caught up with IoT yet, although this is an actively researched topic within academia and industry. IoT gateways may be the best place to deploy this type of technology. |
| 15.4 | Disable Wireless Access on Devices if Not Required | Disable wireless access on devices that do not have a business purpose for wireless access. | | IoT devices will likely rely upon some form of wireless as their primary communication mechanism. |
| 15.5 | Limit Wireless Access on Client Devices | Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks. | | IoT devices will likely rely upon some form of wireless as their primary communication mechanism. |
| 15.6 | Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients | Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients. | | Some enterprises may deem it necessary to limit P2P functionality, yet many IoT devices are specifically designed to utilize machine-to-machine (M2M) communication. Disabling this functionality would significantly reduce the utility of the device. |

| CIS Control 15: Wireless Access Control | | | Applicability | |
|---|--|---|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 15.7 | Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data | Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit. | • | This is an important capability that is not always available for IoT. Enterprises will need to verify this before purchase, but this is possible to determine with online research. |
| 15.8 | Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication | Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) that requires mutual, multi-factor authentication. | | This protocol is not supported on most IoT devices. Enterprises will need to verify this before purchase. |
| 15.9 | Disable Wireless Peripheral Access to Devices | Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose. | | IoT devices will likely rely upon some form of wireless peripheral as their primary communication mechanism. |
| 15.10 | Create Separate Wireless Network for Personal and Untrusted Devices | Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly. | • | This Sub-Control is one of the most critical for IoT devices, especially when insecure devices utilizing legacy protocols with aging software/firmware need to function on an enterprise network. |

CIS Control 16: Account Monitoring and Control

Actively manage the lifecycle of system and application accounts — their creation, use, dormancy, deletion — in order to minimize opportunities for attackers to leverage them.

IoT Applicability

The need exists to manage accounts on IoT devices and associated platforms throughout their lifecycle. IoT devices will have a series of accounts already created and in use when the device is purchased and shipped. Account management is also applicable to mobile applications, IoT management platforms, and cloud platforms. Additionally, enterprises and potentially individual users may also create new accounts. All of these accounts need to be actively managed.

IoT Challenges

It can be challenging to manage accounts on a single system with different user accounts developed by different vendors. Realistically, it may not be possible to manage all accounts on a device from all of the companies involved in development. Still, though all accounts may not be properly documented upon receipt of a device, creating as thorough an inventory of these accounts as possible is important. It is difficult to identify all root accounts that a developer may use, and it may be preferable to use devices that can disable all accounts that the organization has not explicitly approved.

IoT Additional Discussion

Registering devices within an enterprise directory system such as AD or LDAP may be a valid method for restricting access and for effectively monitoring who has authenticated to the devices. However, this is only applicable for those devices that can be configured for AD. Organizations should ensure that IoT implementation plans include strategies for authentication and monitoring the accounts used to access devices. This data should then be fed back to the organization's SIEM for monitoring and control. Administrators should regularly review user accounts on all systems utilized by the enterprise. Privileges should be adjusted accordingly on a regular basis with over-privileged users addressed and accounts deactivated when necessary.

Legacy IoT systems with stand-alone consolidating or command and control hosts should leverage system tools, augmenting them with manual recording and audit processes as required, to enable this Control. Cloud-based applications supported by the enterprise should be monitored and have their credentials disabled during employee separation. Enterprise applications should be analyzed and reviewed for proper authentication techniques. Special attention should be paid to areas where integration occurs between third-party services and when identities are federated. Logging should be enabled within back-end management services to monitor activity, with the logs regularly reviewed.

| CIS Control 16: Account Monitoring and Control | | | Applicability | |
|--|--|--|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 16.1 | Maintain an Inventory of Authentication Systems | Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider. | | Although an important Sub-Control, IoT-specific authentication systems are not commonplace. |
| 16.2 | Configure Centralized Point of Authentication | Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems. | | A majority of IoT devices do not allow for a centralized point of authentication. For instance, IoT devices utilizing a cloud platform will not allow enterprises to insert themselves into the authentication process. |
| 16.3 | Require Multi-Factor Authentication | Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider. | | Although most IoT devices will not support this capability, where possible it should be set up and utilized. |
| 16.4 | Encrypt or Hash All Authentication Credentials | Encrypt or hash with a salt all authentication credentials when stored. | | This is typically a feature that will need to be built-in to the device and verified by the enterprise before purchase. |
| 16.5 | Encrypt Transmittal of Username and Authentication Credentials | Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. | | This feature will need to be built into the device beforehand, but IoT devices should be cryptographically protecting authentication data using modern means. <ul style="list-style-type: none"> |
| 16.6 | Maintain an Inventory of Accounts | Maintain an inventory of all accounts organized by authentication system. | | This is an important Sub-Control but will need to be accomplished via technical and procedural means. To accomplish it, enterprises must be aware of all the cloud platforms and user accounts associated with an IoT device. <ul style="list-style-type: none"> |

| CIS Control 16: Account Monitoring and Control | | | | Applicability |
|--|---|--|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 16.7 | Establish Process for Revoking Access | Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails. | • | In addition to typical workstations and servers, administrators should define this process specifically for IoT devices and gateways. |
| 16.8 | Disable Any Unassociated Accounts | Disable any account that cannot be associated with a business process or business owner. | • | Just as with traditional systems, accounts that are not linked to an approved user should be disabled. |
| 16.9 | Disable Dormant Accounts | Automatically disable dormant accounts after a set period of inactivity. | • | In a manner similar to traditional systems, dormant accounts should be disabled after a pre-defined time of inactivity. |
| 16.10 | Ensure All Accounts Have An Expiration Date | Ensure that all accounts have an expiration date that is monitored and enforced. | • | To the extent possible on IoT devices and within applications, accounts should not be created to be used in perpetuity. |
| 16.11 | Lock Workstation Sessions After Inactivity | Automatically lock workstation sessions after a standard period of inactivity. | | IoT devices are often "headless" embedded devices that do not directly interact with users. |
| 16.12 | Monitor Attempts to Access Deactivated Accounts | Monitor attempts to access deactivated accounts through audit logging. | • | Attempts to access disabled or deactivated accounts should be logged to the extent possible. |
| 16.13 | Alert on Account Login Behavior Deviation | Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration. | • | When abnormal behavior for an account occurs, the necessary parties are properly notified. |

CIS Control 17: Implement a Security Awareness and Training Program

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

IoT Applicability

Administrators and any potential employees interacting with IoT devices should be trained on risks and threats specific to IoT platforms. The deployment of IoT components brings with it new operational capabilities as well as new system and security management requirements. Security awareness training should be tailored to all employees regularly using these devices.

IoT Challenges

Ensuring that administrators and employees understand the threats IoT devices pose to their networks can be a challenging task. Special notice should be taken regarding the connection of insecure legacy devices to enterprise networks handling sensitive enterprise information. Consumer IoT devices are often cheaply available and becoming ubiquitous in daily living, and employees will likely bring unapproved devices into the office to use. This could include connecting enterprise systems to these devices, or connecting the IoT devices directly to the network. Employees need to understand the security policies surrounding these actions.

IoT Additional Discussion

It is important that organizations understand if a skills gap exists for current staff and work toward identifying appropriate training to fill those gaps. Specifically, training related to the new threats that an organization may be exposed to as they implement aspects of IoT would prove valuable to those charged with protecting the enterprise. Legacy operators that migrate to remote operations or reporting capabilities that leverage commodity IT solutions for remote situational awareness or command and control need to ensure their remote operators have the skills and training to address the additional risks of leveraging internet-facing IoT devices for their work.

Additionally, IoT introduces new concepts that include a heavy focus on RF communications, with a range of purpose-built protocols. Security engineering teams must understand the intricate details of these protocols to be able to configure devices in a secure manner. In many cases, IoT subsystems must also be integrated into the larger enterprise through cloud-based APIs. This requires that security engineering teams be well versed in the cloud-based technologies that support IoT.

| CIS Control 17: Implement a Security Awareness and Training Program | | | | Applicability |
|---|--|--|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 17.1 | Perform a Skills Gap Analysis | Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap. | <ul style="list-style-type: none"> • | Understanding the habits of employees using enterprise-approved IoT devices can help focus future cybersecurity awareness training. It can also be beneficial to analyze the list of IoT devices used in the organization and plan specific training for staff with administrative privileges for those IoT devices. |
| 17.2 | Deliver Training to Fill the Skills Gap | Deliver training to address the skills gap identified to positively impact workforce members' security behavior. | <ul style="list-style-type: none"> • | Once a gap analysis has been performed, specific training should be provided to those users. |
| 17.3 | Implement a Security Awareness Program | Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner. | <ul style="list-style-type: none"> • | A strategy should be developed to address and educate users on security concerns surrounding the use of IoT devices. |
| 17.4 | Update Awareness Content Frequently | Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements. | <ul style="list-style-type: none"> • | Consistent updates to user awareness training can help ensure employees know the latest threats. |
| 17.5 | Train Workforce on Secure Authentication | Train workforce members on the importance of enabling and utilizing secure authentication. | <ul style="list-style-type: none"> • | Secure authentication is different on IoT platforms, and employees should know the security risks and implications of insecurely connecting IoT devices to corporate networks. |

| CIS Control 17: Implement a Security Awareness and Training Program | | | | Applicability |
|---|--|---|---|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 17.6 | Train Workforce on Identifying Social Engineering Attacks | Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls. | <ul style="list-style-type: none"> • | This is important as IoT devices may purport to perform one purpose (e.g., Bluetooth speaker) but be configured to record information about a user and send it back to a malicious actor. |
| 17.7 | Train Workforce on Sensitive Data Handling | Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information. | <ul style="list-style-type: none"> • | Users should understand what data is sensitive on their IoT devices and how to prevent commingling alongside personal information. |
| 17.8 | Train Workforce on Causes of Unintentional Data Exposure | Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to <i>autocomplete</i> in email. | <ul style="list-style-type: none"> • | This can be tailored to IoT-specific needs, such as what can happen if an insecure IoT device is connected to an enterprise network. |
| 17.9 | Train Workforce Members on Identifying and Reporting Incidents | Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident. | <ul style="list-style-type: none"> • | Employees can be trained on what successful attacks on IoT devices look like and to whom they should be reported. |

CIS Control 18: Application Software Security

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

IoT Applicability

This CIS Control can be applied in a few distinct ways as application software security can apply to 1) creating IoT devices; 2) deploying cloud-based applications that IoT devices utilize; 3) writing mobile or other applications that govern the usage of an IoT device; and 4) creating an application that integrates with a device in some way, such as leveraging an API. Note that this guide is not focused on the development and manufacturing of IoT devices and instead guides enterprises on their usage of IoT.

IoT Challenges

Most enterprises will not be provided with the source code used to run and operate IoT devices on their networks. This also includes the associated mobile applications and cloud platforms. In many instances, those responsible for application security for IoT devices would have to perform analysis on compiled binaries pulled from the devices, which can be an arduous and time-consuming task. Mobile applications may be more easily acquired, but again the analysis would not be directly on the source, which limits the benefit somewhat. But this can still be a valuable effort. For instance, privileged credentials for accessing an IoT device have been found inside of its corresponding mobile application. Or, in another instance, credentials can be shared between distinct devices from the same manufacturer.

IoT Additional Discussion

Enterprises may like some level of assurance that device manufacturers of IoT components practiced software assurance fundamentals when developing the firmware/software that powers these devices. There will also likely be a number of proprietary applications (e.g., cloud service, mobile application) that communicate with the IoT components and devices located throughout the enterprise. For procured IoT devices, enterprises should understand which security best practices were employed by the manufacturer and help to push vendors toward secure software development methodologies. This should also be a part of acquisition requirements and evaluation.

Software being developed by enterprises to connect to IoT components should follow the same secure development standards that the organization is already using for other internally developed applications. The [IoT Security Testing Guide](#) from the Open Web Application Security Project (OWASP) can be a useful resource for IoT device software security.

| CIS Control 18: Application Software Security | | | Applicability | |
|---|--|--|---|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 18.1 | Establish Secure Coding Practices | Establish secure coding practices appropriate to the programming language and development environment being used. | <ul style="list-style-type: none"> • | The OWASP IoT Project provides helpful guidance for secure IoT coding practices. |
| 18.2 | Ensure That Explicit Error Checking Is Performed for All In-House Developed Software | For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. | <ul style="list-style-type: none"> • | Error checking is an important software assurance concept and is still necessary in the languages used to develop software that integrates with IoT devices. |
| 18.3 | Verify That Acquired Software Is Still Supported | Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations. | <ul style="list-style-type: none"> • | The use of unsupported software/firmware and applications for IoT devices to conduct enterprise tasks is dangerous and potentially exposes sensitive enterprise data via application-level vulnerabilities and misconfigurations. |
| 18.4 | Only Use Up-to-Date and Trusted Third-Party Components | Only use up-to-date and trusted third-party components for the software developed by the organization. | <ul style="list-style-type: none"> • | All of the libraries and development kits used for device development should be supported. |
| 18.5 | Use only Standardized and Extensively Reviewed Encryption Algorithms | Use only standardized, currently accepted, and extensively reviewed encryption algorithms. | <ul style="list-style-type: none"> • | As with any device, only standardized cryptographic algorithms with sufficient key sizes should be utilized. Specialized lightweight crypto is available and undergoing standardization for resource constrained use cases. |

| CIS Control 18: Application Software Security | | | Applicability | |
|---|---|--|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 18.6 | Ensure Software Development Personnel Are Trained in Secure Coding | Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. | <ul style="list-style-type: none"> • | Classes and training materials are easily available online and in-person to educated developers on the common pitfalls of secure software development. |
| 18.7 | Apply Static and Dynamic Code Analysis Tools | Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software. | <ul style="list-style-type: none"> • | Many companies offer these types of services for IoT applications. There is no single tool that will operate with 100% efficiency and correctness, necessitating a toolbox approach of various tools good at performing different types of analysis. |
| 18.8 | Establish a Process to Accept and Address Reports of Software Vulnerabilities | Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group. | <ul style="list-style-type: none"> • | Enterprises should set up processes for vulnerability disclosure associated with IoT software. |
| 18.9 | Separate Production and Non-Production Systems | Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments. | <ul style="list-style-type: none"> • | Non-production systems should not be exposed to untrusted parties, as they commonly store sensitive data, but are often not hardened or running up-to-date software. |

| CIS Control 18: Application Software Security | | | Applicability | |
|---|--|--|---------------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 18.10 | Deploy Web Application Firewalls | Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed. | • | Web application firewalls (WAFs) are not an appropriate control within the context of embedded IoT devices. With that said, many IoT devices use a web portal to display IoT data or to manage an IoT device. |
| 18.11 | Use Standard Hardening Configuration Templates for Databases | For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested. | | Enterprises generally have little say in the methodologies and standards used to harden IoT devices. The device manufacturer can provide such information before procurement. |

CIS Control 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

IoT Applicability

Traditional incident response guidance applies and can be tailored to IoT. This includes the need for planning, defining roles and responsibilities, and having an escalation path. Like with traditional computer systems, the need to identify, investigate, respond, and recover from incidents involving IoT devices is important.

IoT Challenges

Just as security professionals establish incident response plans to react to the compromise of a traditional IT asset, response plans should be tailored to address the course of action to take when one or more IoT components are compromised. This should include taking into account the need to perform forensics on the compromised component as well as the need to quickly ensure that the device is taken offline to limit the spread of the incident. It should be noted that IoT forensics requires specialized knowledge and can be difficult to perform. When considering data forensics for IoT devices, there are a wealth of different types of data available to support the objective of the acquisition, be it eDiscovery, misuse, or evidence collection to support a criminal case.

IoT Additional Discussion

IoT systems are generally operational and come with a complete maintenance-oriented incident response and management subsystem of technology and business processes. Cybersecurity incident response and management controls should be integrated into these maintenance operations. Operations personnel and incident responders need to be trained on what unusual behavior looks like for an IoT device. As IoT extends to support new business processes, perform a mapping of IoT systems to those business processes. This will aid in determining the continuity of operations planning (COOP) approach to maintaining IoT operations. As with traditional incident response processes, this part of the response process should be tested or exercised regularly.

| CIS Control 19: Incident Response and Management | | | | Applicability |
|--|--|---|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 19.1 | Document Incident Response Procedures | Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management. | <ul style="list-style-type: none"> • | Written plans for IoT and supporting system breaches are key to IoT incident response. |
| 19.2 | Assign Job Titles and Duties for Incident Response | Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution. | <ul style="list-style-type: none"> • | Especially if an enterprise is supporting an in-house application that integrates with an IoT device that is critical to business operations, personnel should be dedicated to IoT incident response. |
| 19.3 | Designate Management Personnel to Support Incident Handling | Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles. | <ul style="list-style-type: none"> • | Management and backup personnel should be specifically appointed for IoT incident response. |
| 19.4 | Devise Organization-wide Standards For Reporting Incidents | Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. | <ul style="list-style-type: none"> • | Standards for reporting IoT incidents should be put in place that are mandated across the enterprise. This should include time to report, types of anomalous events, and details of any relevant incident. |
| 19.5 | Maintain Contact Information For Reporting Security Incidents | Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners. | <ul style="list-style-type: none"> • | Contact information for specific individuals and external organizations regarding IoT security incidents should be maintained. |
| 19.6 | Publish Information Regarding Reporting Computer Anomalies and Incidents | Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities. | <ul style="list-style-type: none"> • | Information regarding IoT breaches and other incidents should be made available to internal employees. This information can be fed back into awareness training. |

| CIS Control 19: Incident Response and Management | | | Applicability | |
|--|---|--|---------------|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 19.7 | Conduct Periodic Incident Scenario Sessions for Personnel | Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responder's technical capabilities using tools and data available to them. | | <ul style="list-style-type: none"> IoT devices can be periodically assessed in order to test IoT incident response procedures. This also helps to keep the necessary individuals aware of the IoT procedures. |
| 19.8 | Create Incident Scoring and Prioritization Schema | Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures. | | <ul style="list-style-type: none"> Depending on their criticality to the organization, a security incident affecting IoT systems may be more or less important to the enterprise. |

CIS Control 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

IoT Applicability

Using traditional penetration testing exercises, such as scanning to identify what ports are open and what services are running to find vulnerable or exploitable versions doesn't apply. Legacy devices may need to be omitted from these activities, especially if they are supporting an important business function. IoT typically expands the threat model facing an organization in unique ways that sometimes cannot be easily rectified or mitigated.

IoT Challenges

Many IoT systems do not have mature IP stacks (or any IP stacks) to scan. Errors in scanning may severely impact business operations. All such tests and scans should be tested thoroughly in a non-operational testbed (including code review or architecture review), preferably under simulated practical load-in operations. Strict rules of engagement must be applied that preclude any possibility of unintended, unexpected, or unwanted operational impact. A good example is a realistic, offline, threat-driven scenario. The usage of automated penetration (pen) testing tools with offline configurations can give a hint as to how the real environment will perform.

Penetration testers and red team members should pay extra care in securing authorization to perform vulnerability assessment and pen testing activities on cloud-based services supporting IoT devices and any mobile devices with an application supporting an IoT device. Specific user or service-level approval may be necessary, more so than what is typically provided by the enterprise.

IoT Additional Discussion

Areas of focus for penetration testing could include sniffing wireless communications, reverse engineering firmware, and scanning for unknown services. The use of a test lab and devices for more thorough hardware examination is relevant to IoT. The [Attify IoT Penetration Testing Guide](#) can be a useful starting point to begin IoT penetration testing exercises. The use of IoT components within an enterprise should result in a tailoring of pen tests and red team exercises to focus specifically on methods to gain access to the network by leveraging weaknesses in the design, configuration, or deployment of those IoT components.

| CIS Control 20: Penetration Tests and Red Team Exercises | | | | Applicability |
|--|--|--|---|--|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 20.1 | Establish a Penetration Testing Program | Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks. | <ul style="list-style-type: none"> • | A penetration testing program geared toward IoT will include any relevant IoT devices, applications, cloud services, and gateways. |
| 20.2 | Conduct Regular External and Internal Penetration Tests | Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. | <ul style="list-style-type: none"> • | The frequency of testing can be difficult to determine, but changes or updates to firmware are a reasonable place to level-set a frequency. |
| 20.3 | Perform Periodic Red Team Exercises | Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively. | <ul style="list-style-type: none"> • | Red team exercises focused on IoT will include any relevant IoT devices, applications, cloud services, and gateways. |
| 20.4 | Include Tests for Presence of Unprotected System Information and Artifacts | Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation. | <ul style="list-style-type: none"> • | Red team tests should look for passwords, digital certificates, and other artifacts that will allow them to access devices and cloud services. |
| 20.5 | Create a Test Bed for Elements Not Typically Tested in Production | Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems. | <ul style="list-style-type: none"> • | This will likely include purchasing additional devices and services. |
| 20.6 | Use Vulnerability Scanning and Penetration Testing Tools in Concert | Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts. | <ul style="list-style-type: none"> • | Although this can be done in a manner similar to normal desktop systems, it may not be as effective for IoT. |

| CIS Control 20: Penetration Tests and Red Team Exercises | | | | Applicability |
|--|--|--|-----------|---|
| Sub-Control | Control Title | Control Description | Included? | Justification |
| 20.7 | Ensure Results From Penetration Test Are Documented Using Open, Machine-Readable Standards | Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time. | | <p>IoT results can be documented in a similar manner as traditional systems. The Mobile version of ATT&CK can also provide value for helping to explain test results to outside parties. Although it's not directly applicable to IoT, it is focused on embedded devices that often contain wireless communication capabilities.</p> <ul style="list-style-type: none"> |
| 20.8 | Control and Monitor Accounts Associated With Penetration Testing | Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over. | | <ul style="list-style-type: none"> Any tools designed to penetrate IoT devices should be monitored and routinely audited. |

Acronyms and Abbreviations

| | |
|---------|---|
| 2FA | Two-Factor Authentication |
| 2G | 2 nd Generation |
| 3G | 3 rd Generation |
| 4G | 4 th Generation |
| 6LoWPAN | IPv6 over Low-Power Wireless Personal Area Network |
| ACK | Acknowledge |
| AD | Active Directory |
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| ASLR | Address Space Layout Randomization |
| ATT&CK | Adversarial Tactics Techniques and Common Knowledge |
| BLE | Bluetooth Low Energy |
| CIS | Center for Internet Security |
| COOP | Continuity of Operations Planning |
| CVSS | Common Vulnerability Scoring System |
| DDoS | Distributed Denial of Service |
| DEP | Data Execution Prevention |
| DHCP | Dynamic Host Configuration Protocol |
| DLP | Data Loss Protection |
| DNS | Domain Name System |
| DSS | Data Security Standard |
| EAP-TLS | Extensible Authentication Protocol-Transport Layer Security |
| GDPR | General Data Protection Regulation |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communication |
| HART | Highway Addressable Remote Transducer |
| HIPAA | Health Insurance Portability and Accountability Act |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| ISAC | Information Sharing & Analysis Center |
| IT | Information Technology |
| JTAG | Joint Test Action Group |
| LDAP | Lightweight Directory Access Protocol |

| | |
|-----------|--|
| LTE | Long-Term Evolution |
| M2M | Machine-to-Machine |
| MAC | Media Access Control (address) |
| MFA | Multifactor Authentication |
| MTD | Mobile Threat Defense |
| NFC | Near Field Communication |
| NIST | National Institute of Standards and Technology |
| OEM | Original Equipment Manufacturer |
| OS | Operating System |
| OWASP | Open Web Application Security Project |
| P2P | Peer-to-Peer |
| PCI | Payment Card Industry |
| REST(ful) | Representational State Transfer |
| RF | Radio Frequency |
| RFID | Radio Frequency Identifier |
| RSU | Roadside Unit |
| RTOS | Real-Time Operating System |
| SD | Secure Digital |
| SIEM | Security Information and Event Management |
| SP | Special Publication |
| SSID | Service Set Identifier |
| SYN | Synchronization |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TTP | Tactics, Techniques, and Procedures |
| UMTS | Universal Mobile Telecommunications System |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| WAF | Web Application Firewall |
| WAN | Wide Area Network |
| WiFi | Wireless Fidelity |
| WPA2-PSK | WiFi Protected Access 2 Pre-Shared Key |

Links and Resources

Attify IoT Penetration Testing Guide
<https://www.iotpentestingguide.com>

CIS Controls™
<https://www.cisecurity.org/controls/>

CIS Controls™ Cloud Companion Guide
<https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/>

CIS Controls™ Mobile Companion Guide
<https://www.cisecurity.org/white-papers/cis-controls-mobile-companion-guide-2/>

CVSS
<https://www.first.org/cvss/>

DDoS in the IoT: Mirai and Other Botnets
<https://ieeexplore.ieee.org/abstract/document/7971869>

ICS Cert
<https://ics-cert.us-cert.gov/>

ICS ISAC
<http://ics-isac.org/blog/>

Mobile version of ATT&CK
<https://attack.mitre.org/tactics/mobile/>

NIST SP 800-160 Revision 1
<https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final>

OWASP IoT Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

OWASP IoT Testing Guide
https://www.owasp.org/index.php/loT_Testing_Guides

The Internet of Things: An Overview
<https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>

Towards a Definition of the Internet of Things
https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

Closing Notes

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7 to IoT environments. The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, N.Y. 12061
518.266.3460
controlsinfo@cisecurity.org