CIS
CRITICAL
SECURITY
CONTROLS

Internet of Things Security Companion

to

the CIS Critical Security Controls *(Version 6)*

Center for
Internet Security®

October 2015

Internet of Things Security Companion to the CIS Critical Security Controls (Ver. 6)

Introduction

The Internet of Things (IoT) is a natural evolution of the Internet as we know it today to include ubiquitous smart end devices providing a variety of services and functions in the commercial, consumer, and government environments. Many applications, and in particular the legacy applications known as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, modern digital factory and health care networks, as well as onboard systems in ships and cars, healthcare devices, etc. are in reality "Intranets of Things*(IoT), using standalone networks, with proprietary and custom protocols designed for use in trusted, secure environments. Business exigencies and efficiencies drive increased connectivity of these custom intranets to the corporate network and from that to the Internet, providing adversaries and hackers new access vectors to launch attacks against these important networks. Thus, it is natural that the Center for Internet Security Critical Security Controls (CIS Controls) also be directly applicable to the current and future IoT networks.

Most IT practitioners are familiar with standard office and other ubiquitous computing environments, and have limited exposure or training in the custom IoT networks, networks that may be run by plant or facility engineers. It is useful to highlight the difference in perspective demanded by legacy and future IoT networks when applying the Controls.

The table below highlights some key areas where IoT systems may differ from the standard corporate IT systems with which most CIS Controls practitioners are familiar. Engineering analysis of the IoT system needing security controls should explore these and any other systems' specific differences in deciding the correct control prioritization for optimal risk mitigation under resource constraints.

Standard Corporate IT Systems	IoT Systems
General TCP/IP stack. General-purpose messaging and file transfer.	Proprietary protocol stack elements; byte-oriented link protocols. Well-defined messages and message sequencing. Designed for reliability in the presence of noise.
Commodity hardware. Commodity cybersecurity appliances and software solutions.	Custom hardware or operating system implementations. Use of limited kernel capabilities.
Updated frequently; patches for security and feature improvement. Relatively short version life.	Long-term, reliable devices. 5 – 10 years or more; rarely changed, and if so, done with a full, complete flash or EEPROM upgrade.
End-points and some networking devices accept and run non-mission specific data and host non-mission-specific processes.	IoT devices don't download general files or respond to unknown messages. In fact, many devices are susceptible to DoS attacks (e.g., by a naïve penetration tester using a commodity tool) because they are not designed to deal with unknown message formats or protocol violations that would not be caused by "known" means (e.g., noise dropping packets).
Security built into the user interface, and includes user authentication.	Security assumes physical integrity. If you can open the IoT box and connect to the maintenance port, you are "in."
Anomalies are the norm.	Anomalies are rare, and trigger high-visibility alarms / alerts. (Strong security feature!)

Description

Several global topics apply to many, if not all, of the CIS Controls. Network segmentation and controls, in particular, including Firewalls, VLAN segmentation, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and actual air-gapping are all both primary controls as well as compensating controls where many of the other CIS Controls are unavailable or inadvisable.

Support for robust independent testing of security controls for new development is a chance to finally implement those controls that have been lacking in legacy devices. And evaluation of security controls as well as prior testing of the controls in these devices as a part of Enterprise purchase decisions will help to foster acceptance of the need for controls and development of same.

CIS Critical Security Controls (Version 6): IoT Security

CIS Critical Security Controls (Version 6): IoT Security			
CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
1	Inventory of Authorized and Unauthorized Devices	This control is especially important in the context of the IoT. Organizations must deploy technology that tracks the myriad IoT devices that will be deployed across the 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 to the IoT.	Network scans for legacy and non-PC devices may be dangerous, putting IoT endpoints into error states; limited implementation of standard solutions possible where devices run IP stacks. Passive line and/or RF monitoring may be required. Proprietary communications protocols with application-specific messaging and command and control are often used in lieu of any authentication

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
			mechanism, making remote recognition of a device as “unauthorized” difficult. This may require some combination of manual assessment, audits using sampling, and/or segregation of devices within subnets to protect legacy devices when newer or other devices can’t handle scans. Many newer IoT devices support integration into IoT management systems via Application Programming Interfaces (APIs). Leverage systems such as these to support inventory of authorized devices on the network.
2	Inventory of Authorized and Unauthorized Software	Keeping control of the versions of software and firmware that drive IoT components within the enterprise will be a challenge. Identifying secure software/firmware baselines for various types of components ensures that the security team has reviewed the threats associated with a particular version of functionality.	May be able to leverage central command and control systems, which are aware of device firmware versions. Custom and restricted OSs may limit remote query capability. In general, IoT software is not patched, but loaded as a new complete flash, image, etc. Manual sampling via IoT direct maintenance port using proprietary tools may be required. In some cases, firmware must be delivered over the network to IoT devices. In these situations, use best practices for securing images, to include applying digital signatures that are evaluated by the device before loading. This requires a secured space within

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
			the device to store credentials used for signature validation.
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	IoT components typically lack the range of configuration customization that laptops and even mobile devices offer, however when there are configuration options available, security practitioners should review and decide if any particular configurations are unallowable or if a certain configuration is required to assure the security of the component on the network. Security practitioners should baseline these controls and keep documented as security best practices.	Hardening templates may be applicable for PC-based processor OSs and other standard (e.g. ARM) host OSs. IoT devices sold as "appliances" with integrated software generally comprise proprietary software components, limiting applicability of post-development hardening or standard methods for securing configurations. Standard control implementations apply to the use of BYOD and ruggedized commodity devices that are integrated into an IoT mission system. Some newer 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. Ensure that 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.

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
4	Continuous Vulnerability Assessment and Remediation	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 fed back into the best practices for secure IoT deployment kept by the organization.	Vulnerability assessments in an operational environment may be dangerous or impractical. 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 and Analysis Center, 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 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 must be isolated in some fashion.
5	Controlled Use of Administrative Privileges	Some IoT components include administrative accounts for management of the system. Ensure that when evaluating IoT components for use in the Enterprise that 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.	Many IoT devices are deployed in insecure areas (e.g., road side units (RSUs) in the transportation sector). These devices have sometimes been 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

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		For administrator accounts, attempt to ensure that at a minimum strong passwords are used and that 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.	additional physical security. Newly designed IoT devices and subsystems should integrate use of this control.
6	Maintenance, Monitoring & Analysis of Audit Logs	Organizations should always identify methods of extracting audit logs from components on the network and IoT components are no different. This may prove challenging in some instances however, so the default stance should always be to attempt to collect these logs. Having the logs is one success, but means little 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 Event Management (SIEM) system. The creation of custom connectors should be investigated when	Legacy IoT systems are designed for reliable operations and efficient maintenance towards rapid recovery. These designs include logs which may be sufficient. Consolidating and command/control subsystems may use alternate, out-of-band effective logging of activities that should be considered when assessing the need for a separate control.

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		IoT components do not provide standards-based log output. Just as important however, 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.	
7	Email and Web Browser Protections	IoT devices generally do not use email or external web browser applications or interfaces, although some standalone IoT management systems may leverage standard web browser technologies for visualization and a common user experience.	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, and require best practice protections. Where web browser technologies are incorporated in standalone IoT networks, a risk analysis should be performed to address the need to update the applications when patches and new versions are released.
8	Malware Defenses	Given the limited processing power of many IoT components, host-based malware protections are often challenging. Although we have not yet seen significant progress towards writing	Commercial network malware detection systems, e.g., in-line monitoring, may not apply due to latency requirements or the use of non-IP protocols. However, continuous monitoring at corporate or other

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		exploits that target specific IoT components, this will likely change with more widespread adoption of those components. Additional security research into this topic is required, however certain controls such as whitelisting may help to somewhat mitigate this issue for the time being.	gateways through which IoT information (updates or data) flows may be used to detect adversary malware, or to correlate observed activity with known legitimate planned activity. A primary access vector for malware against an IoT device is through maintenance action or supply chain interdiction of a new IoT device software load. Supply Chain Risk Management and gold-standard sampling are candidate mitigators. Additionally, periodic validation of IoT device operation via alternate 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.
9	Limitations and Control of Network Ports, Protocols and Services	IoT components communicate on specific ports and with specific protocols just as other Information Technology (IT) assets. The definition of the allowable ports, protocols and services that may be used by IoT components must be performed and then enforced. IoT components are oftentimes different in this regard, however, as they may implement other	IoT network traffic is highly predictable and repetitious, in comparison with commodity enterprise traffic. Commercial / 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

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		communication protocols that do not ride over the corporate network. As an example, IoT components that implement Bluetooth could be used as a jumping off point once exploited, to move to a nearby target that does not have that protocol locked down. It is important to fully understand the protocols employed by each IoT component allowed within an enterprise and design an overarching security strategy that mitigates the risk associated with these implementations.	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 the IoT is related to employees and others bringing consumer IoT devices into the enterprise. Research [OpenDNS 2015 IoT Security Report] has shown that employees often associate IoT software on their corporate assets (laptops/phones) with their personal IoT devices (e.g., fitness trackers), or bring their personal IoT devices directly into the network (e.g., smart TVs). This opens up command and control channels between the installed software of hardware and sites on the Internet used for data collection or management. Organizations should monitor for personal IoT-related traffic and take actions to deny that traffic when necessary.
10	Data Recovery Capability	In some instances, IoT devices do not provide data storage capabilities and in other instances they do provide for storage of data. Some devices hold data and pass it on and others	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

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		simply stream data across the network in near real-time. When taking an inventory of the types of IoT components planned 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.	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, Wi-Fi, 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. In addition, some IoT systems (e.g., health care systems) may use external subsystems to contemporaneously memorialize sensor data; data recovery requirements may apply.
11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	With the planned implementation of IoT components within an enterprise, take the opportunity to review the configurations for firewalls, routers and switches to ensure that additional vulnerabilities are not introduced through misconfigurations.	This is applicable to the limited case of IoT systems that use TCP/IP networks. More typically, raw Ethernet is used, IP is used without TCP, point-to-point, multi-drop serial, and multicast are used. Legacy ICS systems favor proprietary byte-oriented protocols. 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. Newer IoT devices oftentimes use RESTful APIs that require that the web services that support these

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
			devices be implemented securely. In addition, many IoT devices implement IPv6 communications, sometimes using protocols such as 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.
12	Boundary Defense	As discussed in other Controls, 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, Intrusion Detection and Intrusion Prevention systems provide some degree of assurance that a compromise of the less trusted IoT network will have limited effect on the more secure corporate network.	IoT devices are increasingly being connected to cloud-based systems. Full infrastructures that support capture, processing, and analysis of data from IoT endpoints exist in the cloud. In addition, the IoT can support sharing of information across many different organizations. These considerations are driving the need to evaluate whether traditional boundary defense measures are sufficient for the protection of IoT data. For cloud-based systems that support the 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.
13	Data Protection	Data protection is a critical aspect of securing an IoT implementation. Data-in-Transit security	Many legacy IoT systems do not use encryption or encoding to protect the data. Often, IoT message

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		through protocols such as IPsec or Transport Layer Security (TLS) must be implemented if possible to guard against eavesdropping on data flowing between IoT components and other components in the Enterprise. Data-in-Storage (DiS) protections must also be implemented through encrypted storage when feasible. An area of data protection that is always hard to achieve correctly and in the case of the IoT requires additional exploration, is the management of the cryptographic keys that support the data protection capabilities.	traffic is perishable, near real-time, of limited historical value, and tolerant of loss. Sophisticated attacks that seek mission effects through data manipulation require deep system knowledge and serious mission value to justify the cost of technique development; in cases where actual threats or observed threat intent indicates the need, methods such as multi-path redundancy, cross-sensor correlation, or a custom in-line device may be applied to effect this control. Note that this is not necessarily true in all newer IoT environments, where we have seen researchers able to easily demonstrate significant exploits against things such as cars, baby monitors, etc. 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.
14	Controlled Access	Authentication to IoT components is sometimes	Legacy IoT systems without automated access control

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
	Based on the Need to Know	not required which leaves a big challenge in establishing controlled access to devices. This is another topic for longer-term research that must be investigated. In the interim, organizations should look to purchase IoT components that require password protections at a minimum and should ensure when possible that passwords are of sufficient strength. In addition, organizations should work to integrate IoT component authentication with an enterprise authentication capability such as LDAP or Active Directory where practical. As a design goal for new IoT systems, IoT components should authenticate themselves to the network when joining.	should still consider policies and manual or physical security solutions, consistent with the assessed risk profile.
15	Wireless Access Control	Many IoT components will make use of wireless communications (although there are also IoT components that rely upon Ethernet connections such as in building automation controls). 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	Many IoT devices use the global and ubiquitous HART (Highway Addressable Remote Transducer) protocol. Others use proprietary solutions, with built-in access control. Geographically distributed systems may use elements of the GSM or other cellular stacks. RF environment characterization, threat assessment, and, if necessary, continual or continuous RF monitoring may be required.

CIS Critical Security Controls (Version 6): IoT Security			
CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		to do this however, an organization must first define the types of devices that are allowed to be connected to the enterprise network. A segregated network could also be used to allow for untrusted devices, such as BYOD, depending on the environment; and the enterprise environment protected by use of Firewalls, IDS, IPS, VLAN segmentation, or physical separation.	IoT devices in the Enterprise may implement a number of protocols, such as Zigbee, ZWave and Bluetooth-LE. Security engineers should ensure that only needed protocols are allowed within the organization.
16	Account Monitoring and Control	Registering devices within an enterprise directory system such as Active Directory or LDAP may be a valid method for restricting access but also for effectively monitoring who has authenticated to the device, for those devices that can be configured this way. 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.	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 effect this control.
17	Security Skills Assessment and	The deployment of IoT components brings with it new operational capabilities as well as new	Legacy systems operators that migrate to remote operations or reporting capabilities that leverage

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
	Appropriate Training to Fill Gaps	system and security management requirements. It is important that organizations do not overlook the need to understand where there are skill gaps in existing staff coverage and work towards 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 the IoT would prove valuable to those charged with protecting the enterprise.	commodity IT (e.g., TCP/IP networks and PC-based or common mobile devices) 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 the 'net. Additionally, the 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 the IoT.
18	Application Software Security	From an enterprise point of view, the manufacturers of IoT components will be required to assure the security of the firmware/software that powers these devices. There will likely be a number of proprietary applications that communicate with IoT	Many IoT device applications are designed to ensure reliable, fail-safe operations in a controlled, known network environment, often in the presence of substantive noise conditions. For legacy long-life applications, neither the hardware nor software is updated frequently, if at all; and the use of proprietary

CIS Critical Security Controls (Version 6): IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		components located throughout the enterprise. These applications may be cloud-based systems that analyze data from distributed sensors and other components, or may be mobile applications that provide limited situational awareness related to some aspect of the enterprise, or an ability to control IoT components. Software being developed by enterprises to connect to IoT components must follow the same secure development standards that the organization is already using for other internally developed applications. For procured IoT components, the Enterprise should understand what security best practices were employed by the vendor and help to push vendors towards developing IoT software and firmware securely. This should also be a part of acquisition evaluation.	protocols and underlying operating systems (often simple real-time schedulers) presents a completely different environment than that found in standard commercial commodity IT systems, with a risk level that may not require controls for mitigation at the device level. Legacy integrating applications that run on commodity platforms are also designed with a focus on operational reliability. Application of this control beyond standard industry current best practices for any software should be informed by instances of actual risk posed by specific, known threats. This threat evaluation should be iterative on some schedule to allow proper evaluation and protection against evolving threats. Industry best practices for appliances (e.g., secure use, closure of test ports, enabling only features used by the mission) should be applied. Data collected from IoT devices, as raw data or through compilation, may require additional privacy protections to ensure compliance with applicable laws and regulations. The IoT development lifecycle also introduces a significant mix of hardware and software engineering activities requiring engineers to be versed in secure development guidelines for both. Ensuring that

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
			devices do not expose active physical test ports and that devices that process sensitive information have tamper protections applied are examples of hardware-security best practices that should be applied to the IoT.
19	Incident Response and Management	Just as security practitioners establish incident response plans to react to the compromise of a traditional IT asset, these 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.	IoT systems are generally operational, and come with a complete maintenance oriented incident response and management subsystem of technology and business processes. Cyber security incident response and management controls should be integrated into these maintenance operations. As the IoT begins to be extended to support new business processes, perform a mapping of IoT systems to those business processes. This will aid in determining the continuity of operations (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 Critical Security Controls (Version 6): IoT Security			
CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
20	Penetration Tests and Red Team Exercises	The use of IoT components within an enterprise should result in a tailoring of penetration 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.	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 test-bed (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 or unexpected unwanted operational impact. A good example is a realistic offline threat-driven scenario.