ETSI TR 103 305-3 V2.1.1 (2018-09)

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 3: Service Sector Implementations

Reference
RTR/CYBER-0034-3

Keywords
cyber security, cyber-defence, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 3 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence. Full details of the entire series can be found in part 1 [i.1].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document is an evolving repository for guidelines on service sector Critical Security Control implementations. Because of their rapidly scaling importance and need for defensive measures for mobile devices and Internet of Things (IoT) sectors are treated.

Introduction

The individual service sector guideline clauses below provide subject matter introductions and derived from companion guides published by the Center for internet Security [i.2] and [i.3]. The latest revision updates this material to Version 7 of the Controls [i.1].

1 Scope

The present document is an evolving repository for guidelines on service sector Critical Security Control implementations. Because of their rapidly scaling importance and need for defensive measures, the mobile device and Internet of Things (IoT) sectors are treated. The CSC are a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.2] Center for Internet Cybersecurity: "Mobile Security Companion to the CIS Critical Security Controls" (Version 6).

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-Mobile-Security-Companion-20151015.pdf.

[i.3] Center for Internet Cybersecurity: "Internet of Things Security Companion to the CIS Critical Security Controls" (Version 6), October 2015.

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf.

[i.4] NIST SP 800-101: "Guidelines on Mobile Device Forensics".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts [i.1]

SPAM: unsolicited or undesired electronic message(s)

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
API	Application Programming Interface
ARM	Advanced RISC Machine
AV	Anti-Virus
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COOP	Continuity of Operations
CSC	Critical Security Control or Capability
DDoS	Distributed Denial of Service
DiS	Data-in-Storage
DoS	Denial of Service
EEPROM	Electrically Erasable Programmable Read-Only Memory
GSM	Global System for Mobile communications
HART	Highway Addressable Remote Transducer
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol security
IPv6	Internet Protocol version 6
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LE	Low Energy
MDM	Mobile Device Management
MSSP	Managed Security Service Provider
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OS	Operating System
OWASP	Open Web Application Security Project
PC	Personal Computer
PIN	Personal Identification Number
RF	Radio Frequency
RSU	Road Side Unit
RTOS	Real-time Operating System
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information Event Management
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TV	Television
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

4 Critical Security Controls: Mobile Device Security

4.0 Introduction

Mobile devices are starting to replace laptops for regular business use. Organizations are building or porting their applications to mobile platforms, so users are increasingly accessing the same data with mobile as with their laptops. Also, organizations have increasingly implemented Bring Your Own Device (BYOD) policies to manage this trend.

However, many organizations have been struggling with the increase of personal mobile devices, and do not fully understand the security risks they may bring. There are concerns that their compact size makes them easy to lose, that they run newer operating systems that do not have decades of use and examination to uncover their weaknesses, and that there are millions of potentially malicious mobile applications that access data, spy on users, steal credentials, act as ransomware, or even become part of a Distributed Denial of Service (DDoS) botnet.

Like with traditional PC platforms, mobile still has to worry about protecting data from unauthorized access at rest and in transit; traditional network level man-in-the-middle attacks on public Wi-Fi; and similar web application threats (since mobile apps frequently access the same server endpoints as web applications). Employees today may use their mobile devices to perform the same business functions and access the same data as their PCs or laptops; but what is different is they are not physically connected to the corporate network, and likely, not even logged into the corporate domain. There are times when organizations use mobile VPNs to access the corporate network, but more and more frequently, mobile users access cloud services. It is not uncommon for corporate mobile users to access numerous cloud-based applications that reside outside their enterprise. Each of these has its own credentials, again rarely linked to enterprise. Getting visibility on the configuration, threats and behaviour of these mobile devices is a challenge, since there are no "eyes" on the device like those attached to the network.

But this environment does not preclude tracking the threats and risks. The Critical Security Controls for Effective Cyber Defence are universal and high level enough to apply to any technology implementation. Everyone needs to start with: "what is the mobile device?", "what is the configuration?" and "what risks needs to be addressed?" These are 1 - 3 of the *Controls.* Protection requires knowledge of what is being protected.

The real challenge to mobile security is the multitude of different mobile devices. With desktops, there are largely commodity hardware running less than half a dozen different operating systems, and through conscientious configuration management, usually a single or only a few different OS versions. Mobile devices have four different popular software platforms, with dozens of different hardware vendors, and dozens of different carriers that affect the platforms. The most prevalent platform presently has 11 OS version families, with sub-versions under them, which on most devices are non-upgradable or forward compatible, and exist on dozen of hardware platforms and carriers. So the permutations become enormous, and understanding the risks of each of these is overwhelming. This is why, for enterprises that have strict security requirements, it is best to issue standard devices.

Within the *Controls*, application security, wireless device control, and data loss prevention all are relevant to mobile. Restricted use of administrative rights is also something that could be implemented, some MDM and mobile security platforms, have the ability to restrict administrative privileges to end users, which will prevent removal of security protections or monitoring. Malware defences are very different than traditional PC platforms. Secure configurations can also be applied, insecure features and functionality can be limited, and cloud based boundary defence can be provided. All of these areas are described in more detail in table 4-1. Using the *Controls* can be the framework to develop a security method and process to manage an organization's mobile security risks.

4.1 CSC Mobile Device Security Description

Simple security steps should always be followed to reduce the likelihood from most Mobile threats: not Rooting or Jailbreaking a device; only obtain apps from the device vendor or the organization's app stores, not 3rd party stores; being wary of any app wanting to install a Profile on a mobile device, as well as if there is an "Untrusted App Developer" popup for the app; and not leaving a device unlocked for long periods of time. For each Control, table 4-1 details the control's applicability to mobile and specific challenges, and considerations for implementation of that control.

Table 4-1: Critical Security Controls (Version 7) - Mobile Device Security

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
1	Inventory and Control of Hardware Assets	One needs to have knowledge of all devices used to access data and resources in the organization. Mobile devices are not perpetually attached to the corporate network like other IT systems, so new methods need to be used to maintain the inventory.	An organization cannot get an inventory of mobile devices by running a scan to discover what mobile devices are connected; companies can use email accounts, or active synchronization software to determine what mobile devices are used to access email (which is most popular application for mobile devices). Also, Mobile Device Management (MDM) can support this by installing agents on the mobile devices to push down configuration and security profiles, monitor devices for configuration changes, and provide access controls based on policy.
2	Inventory and Control of Software Assets	There are millions of mobile apps across dozens of different platforms. Mobile apps can bring risks and threats to data and credentials. Being able to know what is installed, and control access to malicious apps, and insecure versions of apps is important to protect the organization.	MDM tools can inventory apps, and set policies and whitelisting to promote use of secure versions of apps. However there are privacy considerations in Bring Your Own Device (BYOD) scenarios, as the organization may not need to know what apps an individual has installed on their personal device for personal use.
3	Continuous Vulnerability Management	Mobile vulnerabilities are usually linked to versions of the Operating system, or malicious apps. Because mobile devices are not always attached to the network, vulnerabilities cannot be identified and managed like as done on PCs, servers, or other permanently connected networked devices. Mobile vulnerabilities also can apply to many layers; hardware, OS (version), OS (configuration), individual application (of which there are potentially millions), network connection (cellular, Bluetooth, WiFi, NFC), app stores, physical location (i.e. countries where the government monitors mobile devices) and finally, whether the device is corporate-owned or personal (privacy requirements).	One cannot just run vulnerability scans on a network to scrutinize the mobile devices. Therefore, mobile vulnerability assessments should incorporate threat modelling, and understanding the devices, data, users, and their behaviours. MDMs can play a key role in gathering the information for the "what" and "who" for mobile management. Also, there are number of mobile security point solutions that address strong authentication, data and application security, security of data at rest and in transit, and protection from network based threats when connected to Wi-Fi, such as man-in-the-middle attacks. Organizations can choose to outsource management of their MDM platform and mobile support, similar to using Managed Security Service Providers (MSSPs) to monitor and manage network security devices.

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
4	Controlled Use of Administrative Privileges	Many intrusions use valid credentials obtained either through social engineering, or captured by other means. One important risk in mobile is protecting credentials stored on the device, because a user's email account could also be a system or Domain Admin account. Also, Admin control is different in mobile devices. Malicious apps are taking advantage of unfamiliarity with the mobile admin levels, and there are malicious apps that obtain admin rights so they can hide themselves from the user.	Mobile devices are part of the network based on their credentials, not based on their connection. It might not be possible to control admin rights on mobile devices, especially in a BYOD situation; but access based on least privilege may apply. It is dangerous to allow users to Root or JailBreak mobile devices, because it opens up risks to vulnerabilities running at that lowest level.
5	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Like with PCs, secure configurations and monitoring of these configurations are critical to maintain trust with these devices.	MDMs can restrict access to cameras, white-list Wi-Fi networks, apply password policy enforcement, and inventory what apps are installed. Be aware, this last feature can be a privacy issue in a BYOD scenario. An organization may not want the liability of knowing or having access to employee's personal email, apps that track health information, financial data, personal contacts and calendars, apps used in their personal lifestyle, or their location. MDM tools can scale to hundreds of thousands of devices, and provide the necessary monitoring to be alerted when devices are out of compliance; for instance, if someone installs an unauthorized application, turns off encryption, or jailbreaks or roots their device.
6	Maintenance, Monitoring & Analysis of Audit Logs	Monitoring is irrelevant if there is not a process to identify events and respond to them. And this response should be matched with the potential impact of the event. This is the human aspect: determining what events or alerts can potentially damage the organization, and execute response in a timely fashion based on that.	MDM and mobile security tools can provide visibility by having agents on phones that send events and alerts to a central server. These can be integrated with traditional Security Operations platforms. Different types of mobile monitoring sources can provide different data. MDMs use the more traditional network operations type of approach: Is the device live? What is the make model and version? Is it up to date? What applications are installed? Has the device been rooted or jailbroken? How much traffic is it sending and receiving? The security tools have more granular logging, such as installation of known bad or suspicious applications, application-level changes to data, network routing changes, SSL certificates used, VPN launching, and in the case of cloud filtering; traditional perimeter gateway logs for web traffic, or other application traffic. There is also the practice of monitoring account connections to the network domain or a specific application.

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
			Metrics should be actionable, not just "how many" of an event happened. More effective things to track are: Am I getting data from everything I should (how many devices are sending events)? Is the right data being collected (are all data logs the correct ones)? Another item to track is the turnover rate of mobile devices, which can be higher than laptops. Multiple user accounts may exist for the mobile devices.
7	Email and Web Browser Protections	Mobile devices change the traditional enterprise architecture by not only extending it outside a traditional perimeter, but also bypassing the need to route much or all traffic through the enterprise network due to use of cloud services. However, web and email threats are still a concern with mobile devices.	Traditional email gateway security controls for SPAM and phishing reduction, and malware and malicious URL links apply to mobile. Mobile security tools use an agent-based approach that gives a view to threats on and to the mobile device, such as malicious applications and profiles, and malicious WiFi networks or Man in the Middle web proxy attacks. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.
8	Malware Defences	Mobile does not have same concept of malware as with PCs. Mobile malware is really about malicious apps. It takes more diligence to understand current threats, and the behaviour of known malicious apps, which often are re-packaged legitimate apps. Preventing the user from installing these apps, intentionally or unintentionally is key. From a BYOD perspective, personal phones are a greater risk, as users download a larger number of apps for personal use than business use. Also, mobile devices themselves are also risks to PCs. Email attachments forwarded from mobile devices might have PC malware that does not affect the mobile device, but could infect the PC. Mobile devices connected via USB to a PC could also have malicious PC files as they can act as removable media. PC AV also cannot always scan mobile devices like a traditional USB drive.	Traditional techniques of using Anti-Virus (AV) do not apply to mobile. AV is not feasible on some restricted operating systems, due to the platform not allowing access at a level where applications can have general knowledge about other applications running on the device, and many argue that it is equally not effective on other operating systems. Most restricted OS vulnerabilities only affect jailbroken devices; but that is recently becoming less true. Application whitelisting is a common approach to mitigate malicious apps. But user behaviour is also important. Users should not install Profiles for apps that should not require one. There are mobile security tools that scrutinize apps for validate if they are legitimate, and compare versions to known-bad repackaged apps. Traditional PC USB port monitoring can help with threat of mobile device connected to PC.
9	Limitations and Control of Network Ports, Protocols and Services	The concept of network ports and protocols do not apply to Mobile like they do to PCs. The only correlation is the turning on of different wireless interfaces, such as WiFi, Bluetooth, or Near Field Communications (NFC). These should be controlled, as they my broadcast presence of the mobile device to the surrounding area.	Traditional guidance on limiting interfaces to only those necessary for purpose, and restricting viewing or connecting to these interfaces apply.

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
10	Data Recovery Capability	Data recovery has always been inherent to the mobile process; unlike with PCs. Mobile devices are replaced on a more frequent basis. And with portability comes ease of loss, damage, or theft. So, mobile has always had the ability to backup data (mostly to the cloud) for easy transfer of contacts and phone numbers, or restoration of data to a new device, which promotes testing the restore process.	One should verify and review backup (e.g. cloud system) settings to make sure it is backing up what is needed, and not what it should not. This might include corporate email, corporate contacts or calendar, or documents to personal backup. The former would be stored on the corporate Exchange server already. There might be corporate policy against backing up this data to a public cloud. Also, ensure there is a good password or strong credentials protecting that cloud backup.
11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	This section has less little direct effect on mobile security. There is guidance on WiFi security, but it applies to all computing devices.	
12	Boundary Defence	Mobile devices remove the concept of the infrastructure boundary by often accessing cloud-based services directly, without routing through corporate infrastructure. However, Boundary Defence applies to Mobile as traditional firewall restrictions, security monitoring sensors, email, web gateway filters, IDS and IPS alerts, and proper logging of events and alerts to feed the incident response process are all important. These can be implemented in a cloud-filtering infrastructure where mobile devices are routed instead of through the enterprise. Coordination or integration with cloud vendors can implement change control to customize these rules, or performing the same with direct control of these rules will be necessary. Consider these filters an extension of the security perimeter, and apply the same rigor to applying of policy, change control, and system monitoring.	Organizations can choose to VPN Mobile traffic to their infrastructure, where traditional boundary defence guidance applies. However, there are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
13	Data Protection	Almost all mobile devices have the ability to encrypt their data at rest, and include a PIN or password (or biometric) to restrict access. Some devices can link encryption or identity to a hardware root of trust. Mobile devices can use traditional VPNs for network or application access. Though most mobile applications store data in cloud, which could require partner or vendor protection requirements built into the agreement. The entire data supply chain should also need to be examined, not just at collection points. Is this data flowing to a back end system? Is data stored in multiple places? Is this data in a cloud? In what country is this data stored (for privacy considerations)?	Traditional guidance on encrypting data one the devices, and using a VPN with good encryption for protecting sensitive data in transit still apply to Mobile. There are VPNs that allow mobile devices to connect to corporate network to access applications or data shares, as well as application specific VPNs that encrypt the data in transit for that application. Some of these technologies include a hardware component, such as a microSD chip, for encryption key management. Traditional enterprise Data Loss Prevention can be helpful for email and network stored data. But cloud applications and data may be more difficult to get visibility from mobile device and user access. There are tools that leverage cloud service APIs to gain this visibility, or filtering clouds that proxy mobile users to these external services, which can provide a source for data access controls. Organizations with Bring Your Own Device (BYOD) programs will need to consider end user privacy implications within policies and security monitoring and operations procedures.
14	Controlled Access Based on the Need to Know	This control is has no specific application to Mobile, as the concept of controlled access to data is universal for different data access. Since mobile devices are more personal devices, and do not usually store data like PCs, access controls are at closer to where the data is stored.	Traditional access and authorization control guidance applies to Mobile.
15	Wireless Access Control	WiFi controls still apply to Mobile, such as restricting connection to only authorized devices, and use of encryption and authentication, but with mobile devices wireless includes cellular, Bluetooth, and potentially NFC as well. Unlike with PCs, there is limited risk to remote connection to the device, like connecting via Telnet or SSH to the mobile device, like on a PC; but, there are network level man-in-the-middle attacks, which can sniff unencrypted traffic, or re-route traffic to insecure web sites that can steal credentials.	Traditional guidance on WiFi security with use of strong credentials for connectivity, encrypted links, and restricting unauthorized device connectivity. Mobile security tools use an agent-based approach that gives a view to threats on and to the mobile device, such as malicious applications and profiles, alerting to malicious WiFi networks or Man in the Middle SSL/TLS web proxy attacks.
16	Account Monitoring and Control	Account monitoring is performed mostly on enterprise platforms, and not on the mobile device. However, always-remote access, and use of cloud-based applications can complicate visibility and auditing.	Many organizations are using cloud applications; those additional credentials will need to be disabled during employee separation as well. Keeping track of these external credentials might take management, or federating these credentials with identify management tools.
17	Implement a Security Awareness and Training Program	This control does not specifically apply to Mobile.	Training users and administrators on risks and threats specific to mobile platforms is prudent.

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
18	Application Software Security	Many organizations are concerned about mobile application security, especially with the millions of apps available for personal and business use. Luckily, secure web application development and security testing has a long history, and directly applies to mobile apps. Many mobile apps are simply web based, while those using a native app running on the mobile device are just a client for a web-based application. Mobile primary application risks are the mobile apps themselves, attempting to access data on the phone, or in some case, a few nasty applications can corrupt the underlying operation system in something called a rootkit, which then renders all OS behaviour untrusted. Some additional threats for malicious native apps include affecting device itself by turning on the camera or microphone, accessing contacts or emails, logging geolocation, capturing credentials, initiating toll calls or texts, or nuisance issues like resource saturation that drains the battery.	Web application security techniques are recommended when building secure mobile apps, including following the Open Web Application Security Project (OWASP) Top 10. The quick win is to make sure the legitimate version of an app is being used; and that it is up to date. If the app is not downloaded from the vendor's app store, there is a much greater risk of installing a malicious app, or "evil twin" or "repackaged" version of the legitimate app. Some of the other guidance, like error checking on user input, testing in-house and 3rd party apps, and hardening the back end all directly apply when developing secure mobile applications. Agent-based mobile security tools can also reduce the risk of malicious behaviour of mobile apps, be preventing installing Profiles, or preventing Man in the Middle website request hijacking or redirect attacks.
19	Incident Response and Management	Like with PCs, now that many users access organization data and services with mobile devices, the need to identify, investigate, respond and recover from incidents involving mobile devices is important.	Traditional Incident response guidance applies to Mobile. This includes the need for planning, defining roles and responsibilities, and escalation path. Operations personnel and incident responders will also require training on what to look for with unusual behaviour on the mobile devices. Having visibility into mobile operations, such as described previously in CSC 6, will help in identifying these events. One challenge is the vast quantity of different types mobile device hardware, even among generations of products. When talking about data forensics on mobile devices, there is a wealth of different types of data available to support the objective of the acquisition; be it eDiscovery, miss-use, or evidence collection to support a criminal case. People have their whole life on their phones, from calendar, phonebook, and to do list, to photos, video and voice recordings (including messages). There is the geolocation data from pictures, social networking check-ins and a few applications store ones "last active location". The history of whom a person communicated with can be obtained from phone logs, text messages, email, and social networking. Information on mobile forensics procedures should be referenced [i.4].

CSC #	Control Name	Applicability to Mobile	Mobile Device Security Challenges and Considerations
20	Penetration Tests and Red Team Exercises	With traditional Pen testing, the cycle of running scans to see what ports are open, and what services are running to see if there are vulnerable versions of those services to exploit does not apply. However, phishing and other social engineering are relevant to mobile.	There is the ability to sniff traffic over the air, perform man-in-the-middle on a mobile session, and even do application re-direction attacks; but the primary threat vectors are the mobile apps themselves, as discussed in CSC 18. The traditional approach for mobile app testing has been code review tools, but standard web proxy tools and web application penetration testing techniques apply. Use of test lab and devices for more thorough hardware examination is relevant to mobile.

5 Critical Security Controls: Internet of Things Security

5.0 Introduction

Internet of Things (IoT) is an expansion of the Internet 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 Critical Security 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.

Table 5-1 highlights some key areas where IoT systems may differ from the standard corporate IT systems with which most 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.

Table 5-1: Security related differences of IoT systems from standard corporate IT systems

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 do not 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 attackers can open the IoT box and connect to the maintenance port, they are "in.".
Anomalies are the norm.	Anomalies are rare, and trigger high-visibility alarms/alerts. (Strong security feature).

5.1 CSC IoT Security Description

Several global topics apply to many, if not all, of the Critical Security 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 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.

Table 5-2: Critical Security Controls - IoT Security

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
1	Inventory and Control of Hardware Assets	This control is especially important in the context of the IoT. Organizations should 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 necessary. Proprietary communications protocols with application-specific messaging and command and control are often used in lieu of any authentication 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 cannot 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.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
2	Inventory and Control of Software Assets	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 necessary. In some cases, firmware should 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 the device to store credentials used for signature validation.
3	Continuous Vulnerability Management	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 should be isolated in some fashion.
4	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 the controls associated with administrative accounts are investigated, 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 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.	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 additional physical security. Newly designed IoT devices and subsystems should integrate use of this control.
5	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 necessary to assure the security of the component on the network.	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.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
		Security practitioners should baseline these controls and keep documented as security best practices.	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.
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 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.	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.
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.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
8	Malware Defences	Given the limited processing power of many IoT components, host-based malware protections are often challenging. Although exploits that target specific IoT components have not been seen, this will likely change with more widespread adoption of those components. Additional security research into this topic is necessary, however certain controls such as whitelisting may help to somewhat mitigate this issue for the time being.	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 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 should be performed and then enforced. IoT components are oftentimes different in this regard, however, as they may implement other 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.	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 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 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.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
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 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.	When IoT message traffic is perishable and temporary, the value of data recovery is limited to maintenance actions. Data recovery capabilities may be necessary 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, 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 favour 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 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 Defence	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 should be a connection point between an IoT segment and the corporate network, boundary defence mechanisms should 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 defence 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.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
13	Data Protection	Data protection is a critical aspect of securing an IoT implementation. Data-in-Transit security through protocols such as IPsec or Transport Layer Security (TLS) should 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 should 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.	Many legacy IoT systems do not use encryption or encoding to protect the data. Often, IoT message 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 researchers have easily demonstrated significant exploits against things such as cars, baby monitors, etc. It is important to perform methodical threat modelling 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 Based on the Need to Know	Authentication to IoT components is sometimes not necessary which leaves a big challenge in establishing controlled access to devices. This is another topic for longer-term research that should 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.	Legacy IoT systems without automated access control should still consider policies and manual or physical security solutions, consistent with the assessed risk profile.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
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 to do this however, an organization should 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.	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 necessary. IoT devices in the Enterprise may implement a number of protocols, such as Zigbee®, Z-Wave® 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 necessary, to effect this control.
17	Implement a Security Awareness and Training Program	The deployment of IoT components brings with it new operational capabilities as well as new 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.	Legacy systems operators that migrate to remote operations or reporting capabilities that leverage 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 should understand the intricate details of these protocols to be able to configure devices in a secure manner. In many cases, IoT subsystems should 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.

CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
18	Application Software Security	From an enterprise point of view, the manufacturers of IoT components will be necessary 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 components located throughout the enterprise. These applications may be cloud-based systems that analyse 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 should 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.	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 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 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.

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 should be applied that preclude any possibility of unintended or unexpected unwanted operational impact. A good example is a realistic offline threat-driven scenario.

History

Document history		
V1.1.1	August 2016	Publication
V2.1.1	September 2018	Publication