IoT Security in Payment Environments

As IoT devices continue to become more widespread, their use and deployment is increasingly crossing over into areas of account-based payments. This may be incidental, with IoT devices deployed within a business environment where payments are also being processed, or more directly with an IoT device being used to accept, perform, or authorize payments on behalf of a user. In all cases, when considering a deployment of IoT devices, the security of the IoT devices and the payment data needs to be considered throughout the device lifecycle. For example, some questions organizations should ask include:

- Are the devices designed with security in mind?
- Are the devices deployed securely?
- Are the devices able to be maintained securely until decommissioned?
- Is there a decommission plan for the devices?

This bulletin outlines what should be considered when deploying IoT systems into an existing environment which may already contain cardholder data processing systems, from initial planning of the deployment through to the eventual decommissioning of the devices.

Stages of an IoT Deployment Lifecycle

A Baseline Approach to IoT Security Design

The first step is to seek a common understanding and definition of what an IoT device is. The Consumer Technology Association (CTA) in conjunction with the Council to Secure the Digital Economy (CSDE), have produced the *C2 Consensus on IoT Device Security Baseline Capabilities*[i] (C2 Consensus)[1], which defines 'IoT' as:

> Internet of Things. An IoT system involves a physical device that connects to a switched or wireless network, for the purposes of access and control. IoT systems may be connected to open networks, such as the Internet, or closed private networks. An IoT device may have supplementary functions provided through remote execution such as an application running on a phone, tablet, local or 'cloud' based computing system.

With this broad definition, an IoT device could be a 'smart' toaster, desk phone, HVAC (heating, ventilation, and air conditioning) system, network camera, or one of many other types of devices.

[1] The C2 Consensus also maps to important guidance from the National Institute of Standards and Technology (NIST) in their publication, NIST Interagency Report 8259A, IoT Device Cybersecurity Capability Core Baseline.

Documents such as the C2 Consensus provides a set of baseline capabilities that IoT devices should meet, as listed below:

IoT Device Security Capabilities (from the C2 Consensus)

- Device Identifiers – provision of unique values to allow for unique device identification.
- Secured Access – protection of device operational and management capabilities through user authentication.
- Data In Transit Is Protected – Protection of the confidentiality and integrity of data using cryptography.
- Data At Rest Is Protected – Protection of confidentiality and integrity of selected stored data using cryptography.
- Industry Accepted Protocols are Used for Communications – Use of secure, widely used protocols, excluding deprecated versions, for communications to and from the device.
- Data Validation – Parsing and limiting input data to prevent it from being used directly as code, commands, or other execution flow inputs.
- Event Logging – A limited persistent record in the device of relevant events, secured and available to users.
- Cryptography – Where cryptography is used, use open, published, proven, and peer-reviewed cryptographic methods with appropriate parameters, algorithms, and option selections.
- Patchability – The ability to verifiably update a device's software and firmware, post-market, with patches that are authenticated.
- Reprovisioning – The ability for authorized users to securely reconfigure and redeploy a device post market, especially to return to factory defaults and securely remove data.

These baseline controls are mapped onto specific detailed requirements in the document ANSI/CTA 2088-A (Baseline Cybersecurity Standard for Devices and Systems),[2] which has been developed through the CTA with a broad range of industry stakeholders. A similar standard for this purpose is ETSI EN 303 645 (Cybersecurity Standard for Consumer IoT Devices)[3]. For industrial control devices – a very large category that overlaps consumer technology in some areas – a popular standard is IEC 62443[4].

It is recommended that all IoT devices being purchased for deployment into corporate networks, or for use in accepting payments, consider these standards and control sets.

Mapping IoT Security Controls to PCI DSS

Although not designed specifically for payments, the C2 Consensus baseline, as with many other security standards and control sets, can be mapped to the PCI DSS requirements as shown below. Where gaps exist, they are primarily due to the difference in the target of the controls; device specific design centric (in the C2 Consensus) vs deployment environment aspects of the PCI DSS.

[2] https://shop.cta.tech/collections/standards/products/https-cdn-cta-tech-cta-media-media-shop-standards-2020-ansi-cta-2088-a-final-pdf
[3] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf
[4] https://www.iec.ch/blog/understanding-iec-62443

This mapping is not intended to imply that a device deployed in a PCI DSS compliant environment meets the C2 Consensus Controls, or that a device meeting the C2 Consensus Controls automatically meets those mapped aspects of PCI DSS. Instead, it shows how requirements for IoT device security capabilities – like those found in the C2 Consensus – can be considered along with the requirements of standards such as PCI DSS to help inform and secure a deployment of IoT devices across the lifecycle of those products.

PCI DSS Requirement (For Deployment Environments)		C2 Consensus Control (For the device)_
1	Install and maintain network security controls	
2	Apply secure configurations to all system components	Secured Access
3	Protect stored account data	Data At Rest Is Protected
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Data In Transit Is Protected Industry Accepted Protocols are Used for Communications
5	Protect all systems and networks from malicious software	
6	Develop and maintain secure systems and software	Data Validation Patchability
7	Restrict access to system components and cardholder data by business need to know	Secured Access
8	Identify users and authenticate access to system components	Device Identifiers
9	Restrict physical access to cardholder data	
10	Log and monitor all access to system components and cardholder data	Event Logging
11	Test security of systems and networks regularly	
12	Support information security with organizational policies and programs	Reprovisioning

This mapping shows that strong network controls and monitoring remain vital for secure IoT deployments. Use of network intrusion detection, which is IoT aware, and consideration for the protocols used by IoT devices is important. For example, many IoT devices communicate using wireless communications methods not common in traditional IT deployments – such as Zigbee. Traditional anti-virus may not be easily deployed to IoT systems, but host-based intrusion detection and prevent mechanisms may help mitigate the risks posed if correctly deployed and managed.

Secure Deployment and Management of IoT Systems

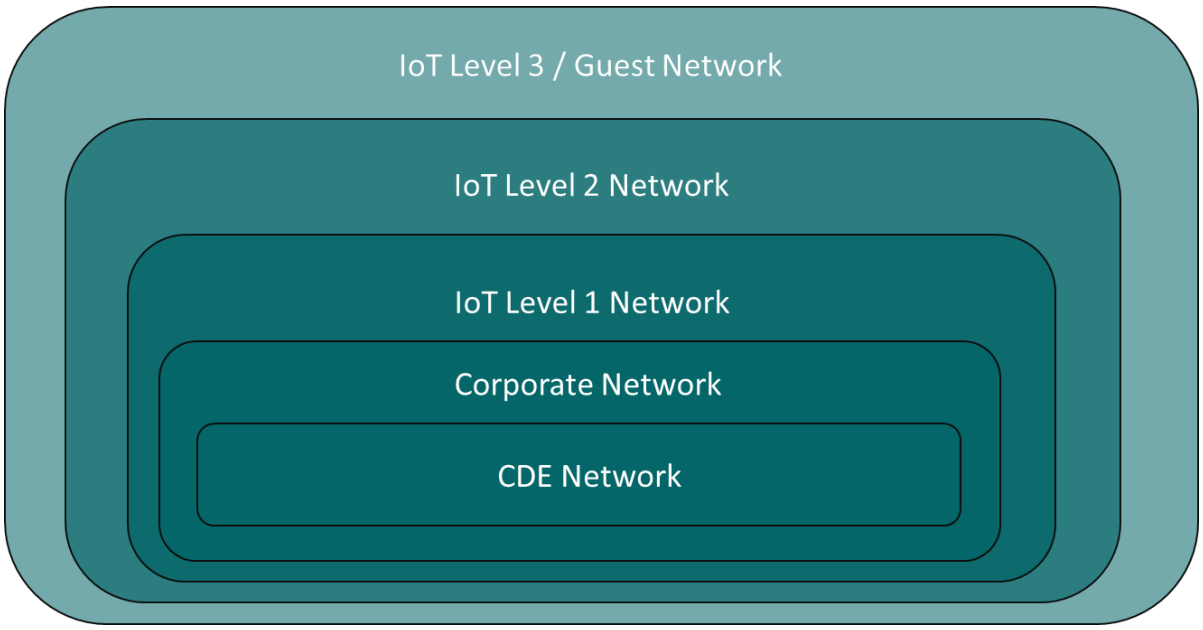
As with all security, IoT security is constantly evolving; new threats emerge, and new vulnerabilities are discovered. To protect networks from the risk of insecure IoT systems, choose secure devices and deploy and securely maintain those devices until they are decommissioned.

IoT devices often provide a range of features and functions which require network and Internet based access. However, not all these features may be required, or even desired, in an IoT deployment. When

considering deployment for an IoT system it is important to understand what required features of any IoT systems are, and plan accordingly. For example, an IoT product feature that requires Internet access may not be desired – but if deployed without any Internet access, the product may not be able to download and install firmware updates, potentially increasing the risk posed by that device.

Some IoT deployments may not require the network features be enabled at all – for example, a TV may be deployed for use in a meeting room but have no need for the network features it provides. Even in these cases, it is important to consider the security and deployment methods; for example, if someone connects the device to the network themselves, is that now a risk (because an unpatched and potentially insecure device is now connected to the corporate network)? If so, how is this risk best mitigated or controlled?

Often it can be helpful to have separate network segments for different IoT systems and use these to isolate them from other systems on your network. Consider the use of a layered network design, where devices with less security assurance are in isolated network segments. Any access that is required can be provided, but with suitable additional controls. Products that cannot be sufficiently secured may be treated in the same way as 'guests,' and given their own network, completely isolated from other devices and systems, if the functions that require access are still needed (like the common 'guest' network implementation).



Example of a Layered Network Architecture to isolate IoT Systems

Maintaining updates for IoT products is important, as they are as vulnerable to new threats as any other IT product. However, not all IoT products are supplied with regular and on-going security patches. When considering purchase of a new IoT system, the total cost of ownership should be taken into account, and this includes the ability to maintain the product securely over time – a less expensive product may be more costly in the long term if you need to replace it sooner than others, as it is no longer being supplied with patches and may become a way for criminals to enter your network.

Planning of Decommissioning

It is common for IoT systems to require some form of personalization during their deployment; from configuration with Wi-Fi settings through to details about the users, and installation of certificates to provide secure network access. This information can often be sensitive and important to remove prior to disposal of the IoT device; if a malicious party was to obtain a device used in your network, could they extract the network certificates or details, and use that as part of an attack?

It's vital that there are plans for the decommissioning of devices once they are no longer required or need to be replaced. The C2 Consensus baseline takes note of this need in the 'Reprovisioning' capability and considering not only how you will use an IoT system, but how you will securely end its use can assist with the purchase and deployment decisions.

IoT System Security Checklist/Questions

The following questions are recommended for those planning the purchase and deployment of IoT systems, to help the secure deployment, use, and decommissioning of these systems in an environment.

Does the device accept or facilitate payments, and how is this securely disabled or configured this for use? Is it included in the cardholder data flows for the network?
Does the deployment plan consider how to integrate the IoT device(s) into your environment in compliance with the PCI DSS? Note: This may be required even for devices which do not facilitate payments, or are not involved directly in cardholder data flows, depending on how they are deployed.
Is the device designed with security in mind, and has it been tested against relevant standards such as ANSI/CTA-2088-A?
Does the vendor of the product guarantee updates for a set period of time, and have a history of on-going product security support? How does this align with the expected deployment period of the product in your environment?
What connectivity does the product require to provide the features required for its use and maintenance, including security updates? Is it possible to isolate the product onto its own network segment?
If network isolation is required and/or provided, how is this protected from change by operators of the device (e.g., by the user connecting to a different Wi-Fi network, or network segment)?
How can the product be securely decommissioned to ensure sensitive information is cleared before the device leaves your control?

[i] Council to Secure the Digital Economy (CSDE), The C2 Consensus on IoT Device Security Baseline Capabilities, https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf