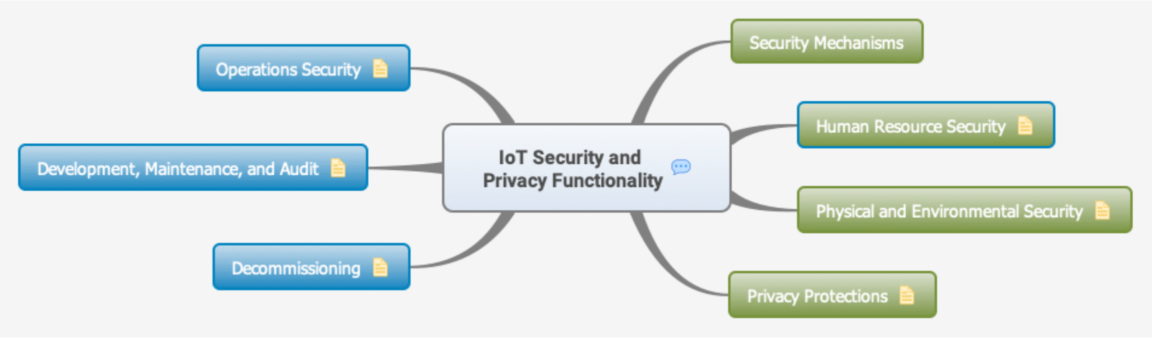
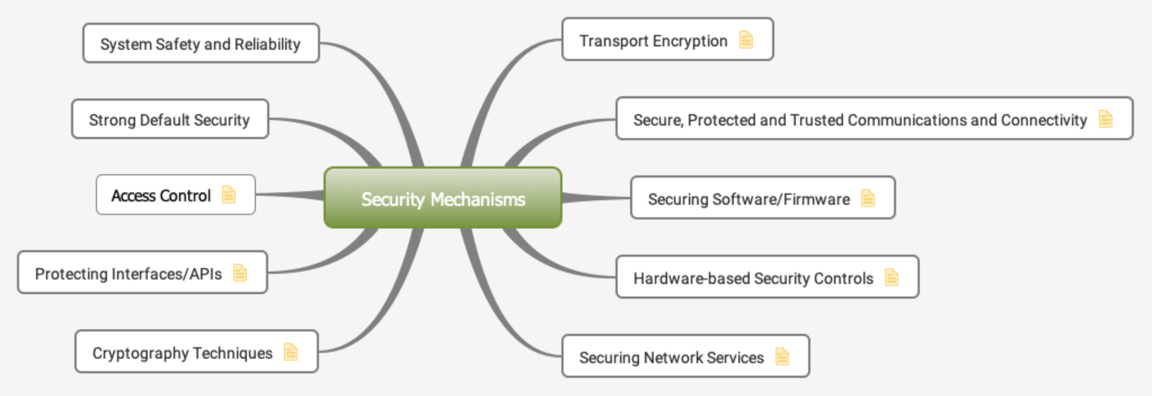
IoT Security and

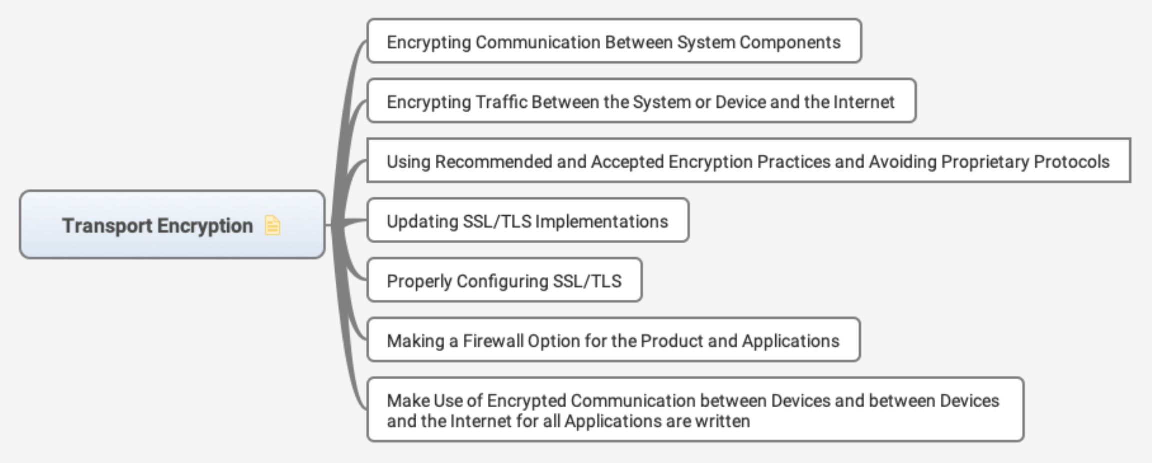
Privacy Functionality


IoT Security and Privacy Functionality
Operations Security
Development, Maintenance, and Audit
Decommissioning
Security Mechanisms
Human Resource Security
Physical and Environmental Security
Privacy Protections

1. Security Mechanisms


Security Mechanisms
System Safety and Reliability
Strong Default Security
Access Control
Protecting Interfaces/APIs
Cryptography Techniques
Transport Encryption
Secure, Protected and Trusted Communications and Connectivity
Securing Software/Firmware
Hardware-based Security Controls
Securing Network Services

1.1. Transport Encryption


Transport Encryption
Encrypting Communication Between System Components
Encrypting Traffic Between the System or Device and the Internet
Using Recommended and Accepted Encryption Practices and Avoiding Proprietary Protocols
Updating SSL/TLS Implementations
Properly Configuring SSL/TLS
Making a Firewall Option for the Product and Applications
Make Use of Encrypted Communication between Devices and between Devices and the Internet for all Applications are written

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

1.1.1. Encrypting Communication Between System Components

1.1.2. Encrypting Traffic Between the System or Device and the Internet

1.1.3. Using Recommended and Accepted Encryption Practices and Avoiding Proprietary Protocols

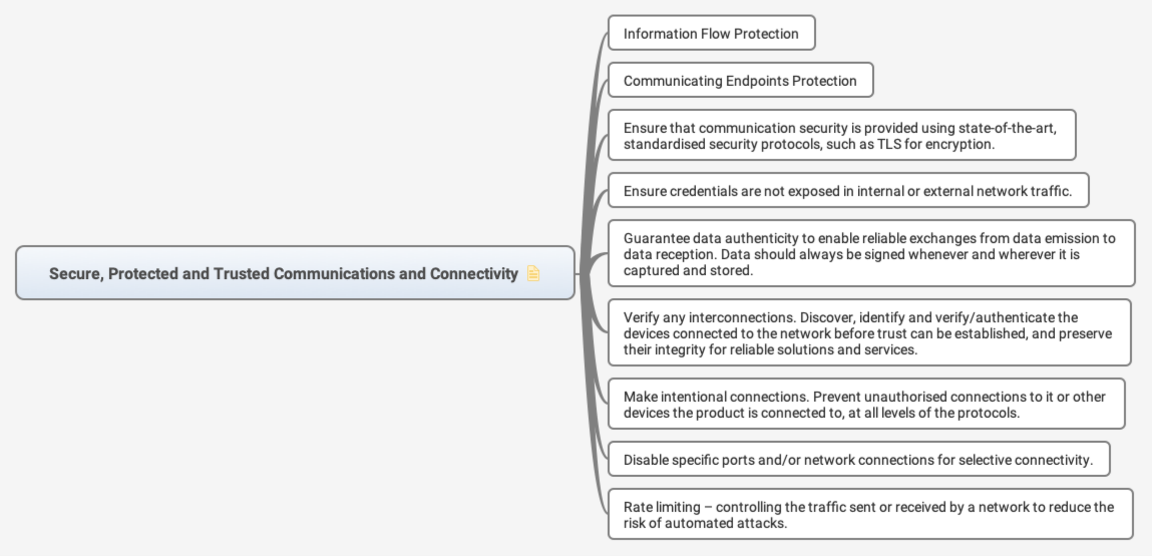
1.1.4. Updating SSL/TLS Implementations

1.1.5. Properly Configuring SSL/TLS

1.1.6. Making a Firewall Option for the Product and Applications

1.1.7. Make Use of Encrypted Communication between Devices and between Devices and the Internet for all Applications are written

1.2. Secure, Protected and Trusted Communications and Connectivity



Secure, Protected and Trusted Communications and Connectivity

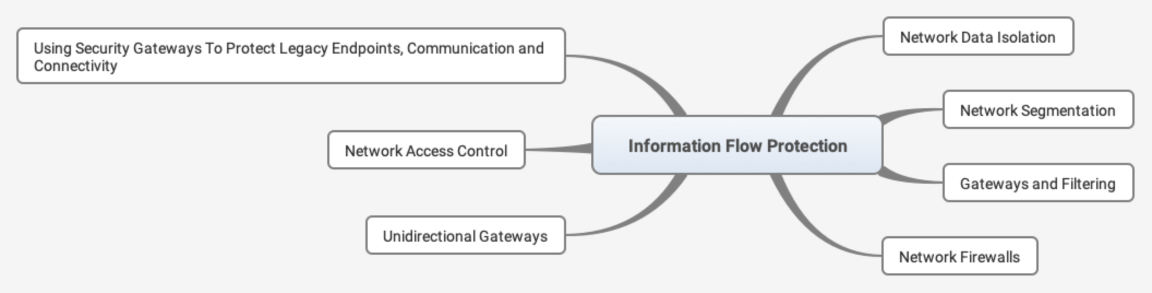
- Information Flow Protection
- Communicating Endpoints Protection
- Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.
- Ensure credentials are not exposed in internal or external network traffic.
- Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored.
- Verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.
- Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.
- Disable specific ports and/or network connections for selective connectivity.
- Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

1.2.1. Information Flow Protection



1.2.1.1. Network Data Isolation

1.2.1.2. Network Segmentation

1.2.1.3. Gateways and Filtering

1.2.1.4. Network Firewalls

1.2.1.5. Unidirectional Gateways

1.2.1.6. Network Access Control

1.2.1.7. Using Security Gateways To Protect Legacy Endpoints, Communication and Connectivity

1.2.2. Communicating Endpoints Protection

1.2.3. Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.

1.2.4. Ensure credentials are not exposed in internal or external network traffic.

1.2.5. Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored.

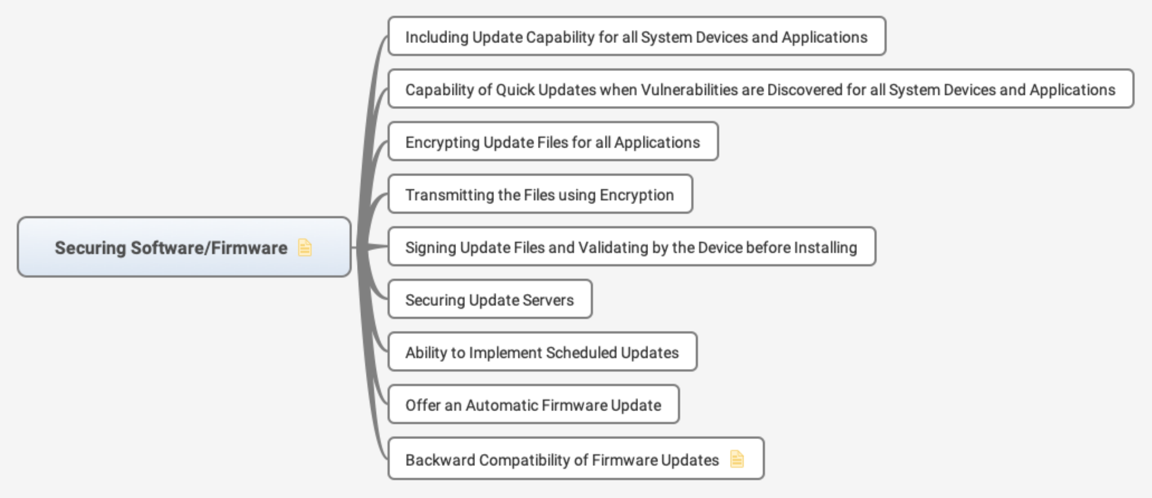
1.2.6. Verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.

1.2.7. Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.

1.2.8. Disable specific ports and/or network connections for selective connectivity.

1.2.9. Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.

1.3. Securing Software/Firmware


Securing Software/Firmware
Including Update Capability for all System Devices and Applications
Capability of Quick Updates when Vulnerabilities are Discovered for all System Devices and Applications
Encrypting Update Files for all Applications
Transmitting the Files using Encryption
Signing Update Files and Validating by the Device before Installing
Securing Update Servers
Ability to Implement Scheduled Updates
Offer an Automatic Firmware Update
Backward Compatibility of Firmware Updates

References:
https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

ENISA:Baseline Security Recommendations for IoT

1.3.1. Including Update Capability for all System Devices and Applications

1.3.2. Capability of Quick Updates when Vulnerabilities are Discovered for all System Devices and Applications

1.3.3. Encrypting Update Files for all Applications

1.3.4. Transmitting the Files using Encryption

1.3.5. Signing Update Files and Validating by the Device before Installing

1.3.6. Securing Update Servers

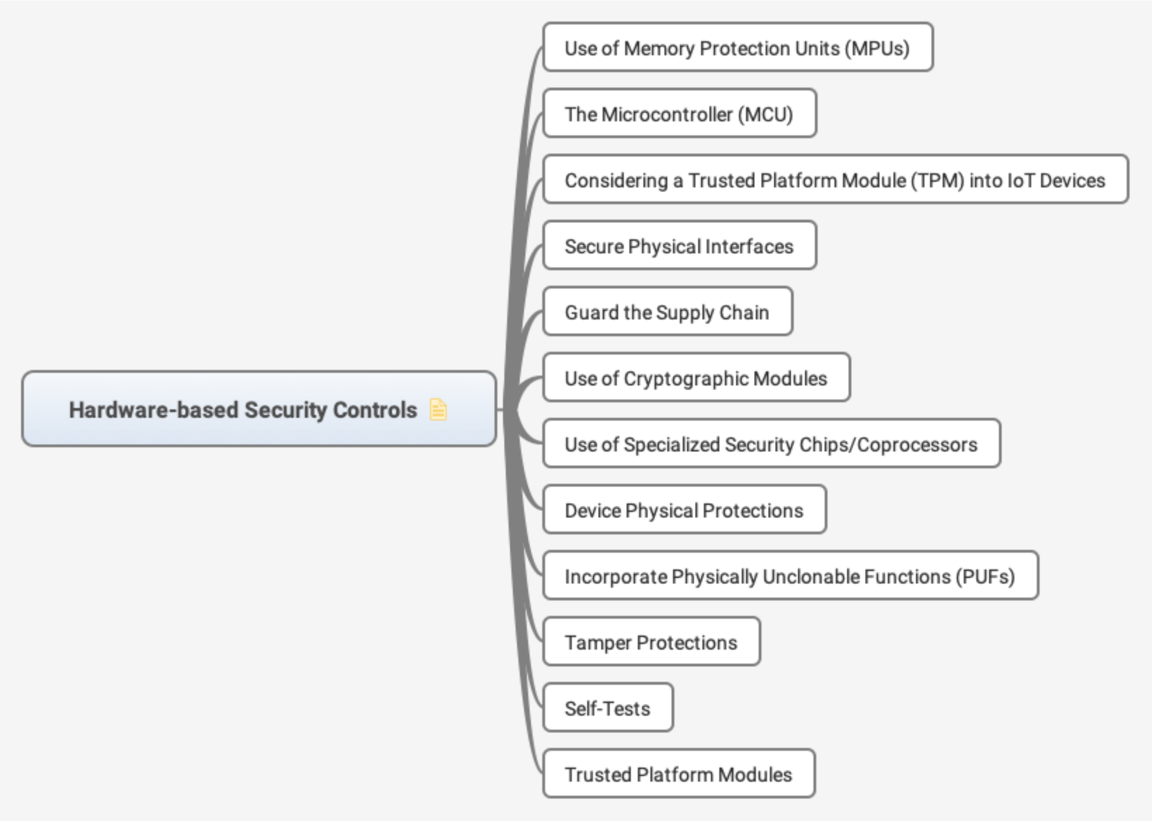
1.3.7. Ability to Implement Scheduled Updates

1.3.8. Offer an Automatic Firmware Update

1.3.9. Backward Compatibility of Firmware Updates

Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.

1.4. Hardware-based Security Controls


Hardware-based Security Controls
Use of Memory Protection Units (MPUs)
The Microcontroller (MCU)
Considering a Trusted Platform Module (TPM) into IoT Devices
Secure Physical Interfaces
Guard the Supply Chain
Use of Cryptographic Modules
Use of Specialized Security Chips/Coprocessors
Device Physical Protections
Incorporate Physically Unclonable Functions (PUFs)
Tamper Protections
Self-Tests
Trusted Platform Modules

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

1.4.1. Use of Memory Protection Units (MPUs)

1.4.2. The Microcontroller (MCU)

1.4.3. Considering a Trusted Platform Module (TPM) into IoT Devices

1.4.4. Secure Physical Interfaces

1.4.5. Guard the Supply Chain

1.4.6. Use of Cryptographic Modules

1.4.7. Use of Specialized Security Chips/Coprocessors

1.4.8. Device Physical Protections

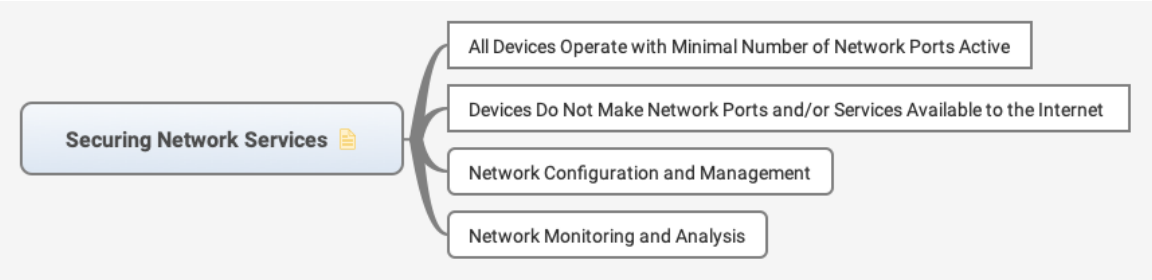
1.4.9. Incorporate Physically Unclonable Functions (PUFs)

1.4.10. Tamper Protections

1.4.11. Self-Tests

1.4.12. Trusted Platform Modules

1.5. Securing Network Services


Securing Network Services
All Devices Operate with Minimal Number of Network Ports Active
Devices Do Not Make Network Ports and/or Services Available to the Internet
Network Configuration and Management
Network Monitoring and Analysis

References:
https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

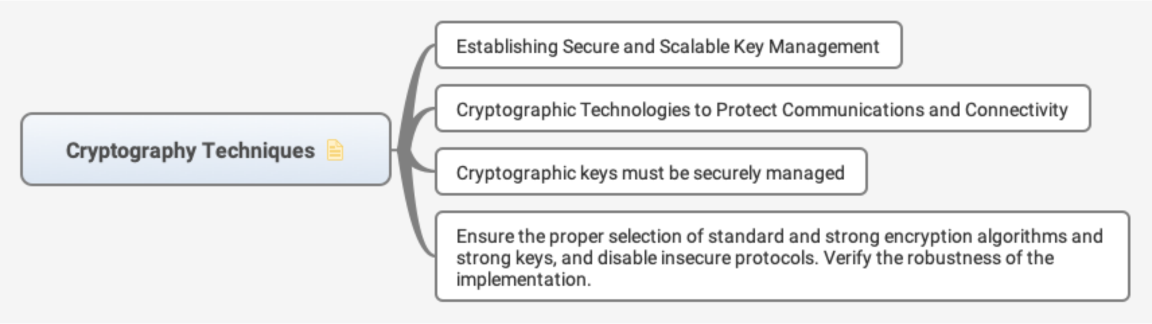
1.5.1. All Devices Operate with Minimal Number of Network Ports Active

1.5.2. Devices Do Not Make Network Ports and/or Services Available to the Internet

1.5.3. Network Configuration and Management

1.5.4. Network Monitoring and Analysis

1.6. Cryptography Techniques


Cryptography Techniques
Establishing Secure and Scalable Key Management
Cryptographic Technologies to Protect Communications and Connectivity
Cryptographic keys must be securely managed
Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

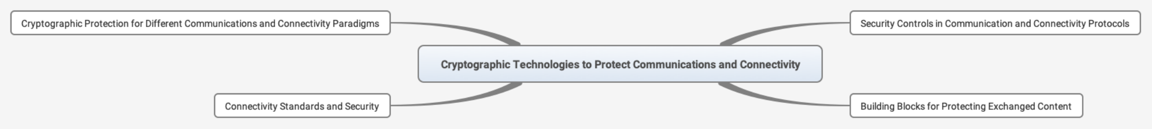
Future-proofing the Connected World - Cloud Security Alliance, 2016

1.6.1. Establishing Secure and Scalable Key Management

Establishing Secure and Scalable Key Management
Design Secure Bootstrap Functions

1.6.1.1. Design Secure Bootstrap Functions

1.6.2. Cryptographic Technologies to Protect Communications and Connectivity


Cryptographic Protection for Different Communications and Connectivity Paradigms
Connectivity Standards and Security
Cryptographic Technologies to Protect Communications and Connectivity
Security Controls in Communication and Connectivity Protocols
Building Blocks for Protecting Exchanged Content

1.6.2.1. Security Controls in Communication and Connectivity Protocols

1.6.2.2. Building Blocks for Protecting Exchanged Content

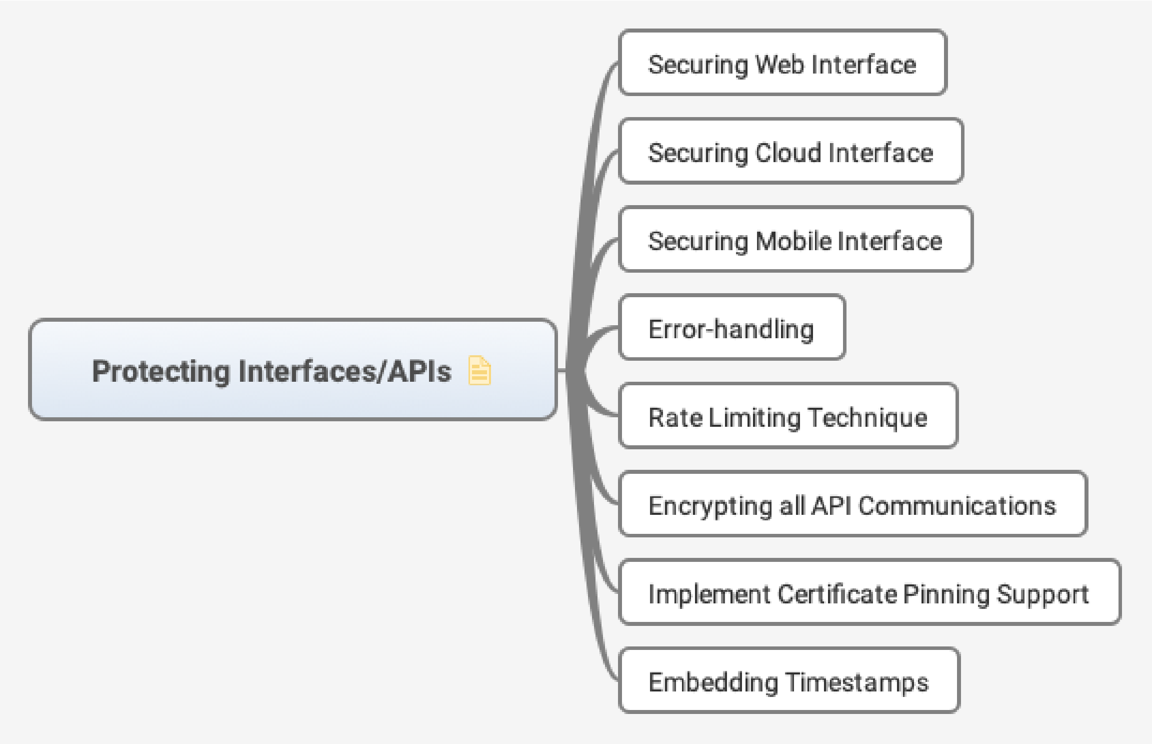
1.6.2.3. Connectivity Standards and Security

1.6.2.4. Cryptographic Protection for Different Communications and Connectivity Paradigms

1.6.3. Cryptographic keys must be securely managed

1.6.4. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.

1.7. Protecting Interfaces/APIs


Protecting Interfaces/APIs
Securing Web Interface
Securing Cloud Interface
Securing Mobile Interface
Error-handling
Rate Limiting Technique
Encrypting all API Communications
Implement Certificate Pinning Support
Embedding Timestamps

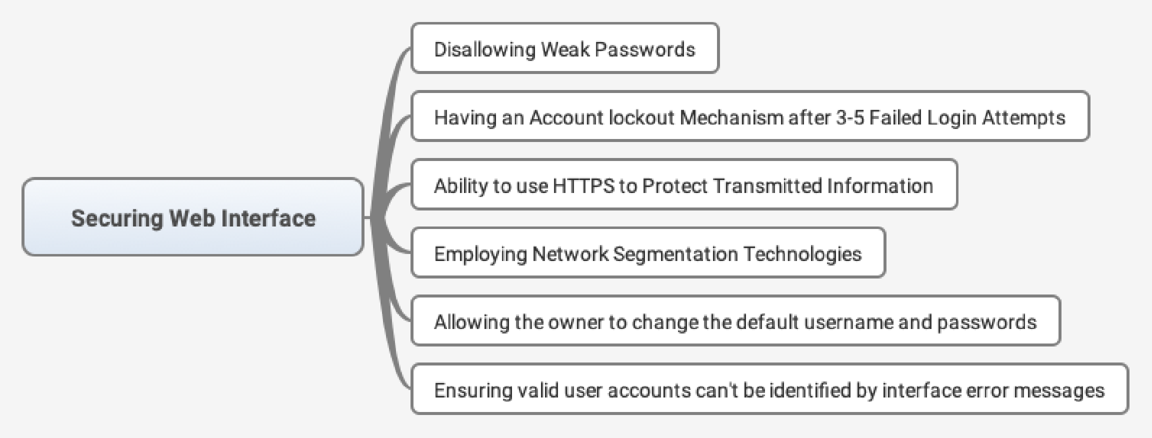
References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

1.7.1. Securing Web Interface

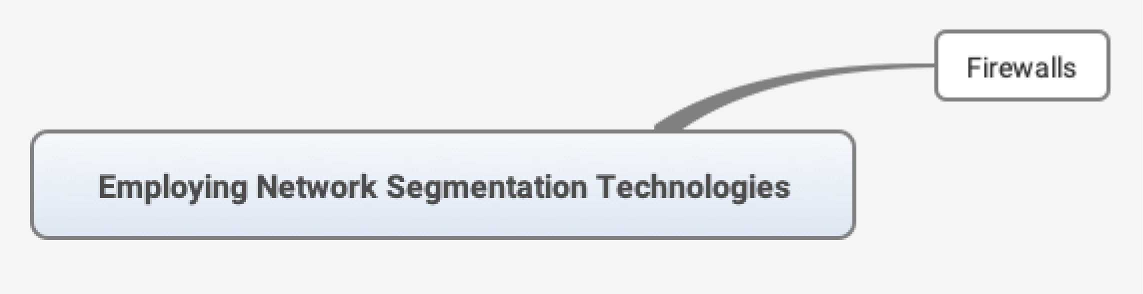

Securing Web Interface
Disallowing Weak Passwords
Having an Account lockout Mechanism after 3-5 Failed Login Attempts
Ability to use HTTPS to Protect Transmitted Information
Employing Network Segmentation Technologies
Allowing the owner to change the default username and passwords
Ensuring valid user accounts can't be identified by interface error messages

1.7.1.1. Disallowing Weak Passwords

1.7.1.2. Having an Account lockout Mechanism after 3-5 Failed Login Attempts

1.7.1.3. Ability to use HTTPS to Protect Transmitted Information

1.7.1.4. Employing Network Segmentation Technologies

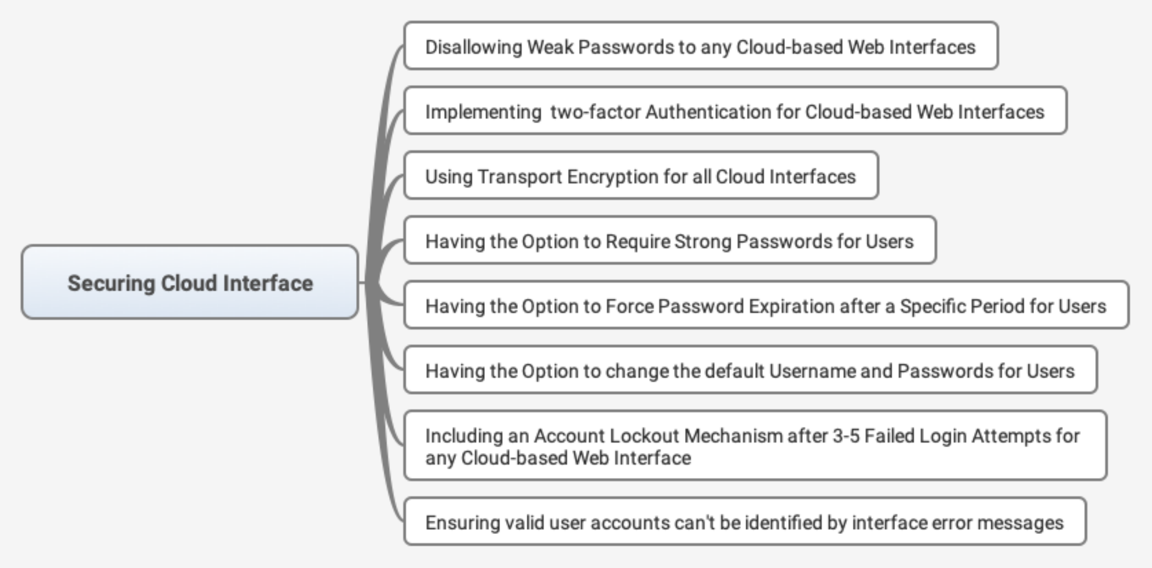


Firewalls

1.7.1.5. Allowing the owner to change the default username and passwords

1.7.1.6. Ensuring valid user accounts can't be identified by interface error messages

1.7.2. Securing Cloud Interface


Securing Cloud Interface
Disallowing Weak Passwords to any Cloud-based Web Interfaces
Implementing two-factor Authentication for Cloud-based Web Interfaces
Using Transport Encryption for all Cloud Interfaces
Having the Option to Require Strong Passwords for Users
Having the Option to Force Password Expiration after a Specific Period for Users
Having the Option to change the default Username and Passwords for Users
Including an Account Lockout Mechanism after 3-5 Failed Login Attempts for any Cloud-based Web Interface
Ensuring valid user accounts can't be identified by interface error messages

1.7.2.1. Disallowing Weak Passwords to any Cloud-based Web Interfaces

1.7.2.2. Implementing two-factor Authentication for Cloud-based Web Interfaces

1.7.2.3. Using Transport Encryption for all Cloud Interfaces

1.7.2.4. Having the Option to Require Strong Passwords for Users

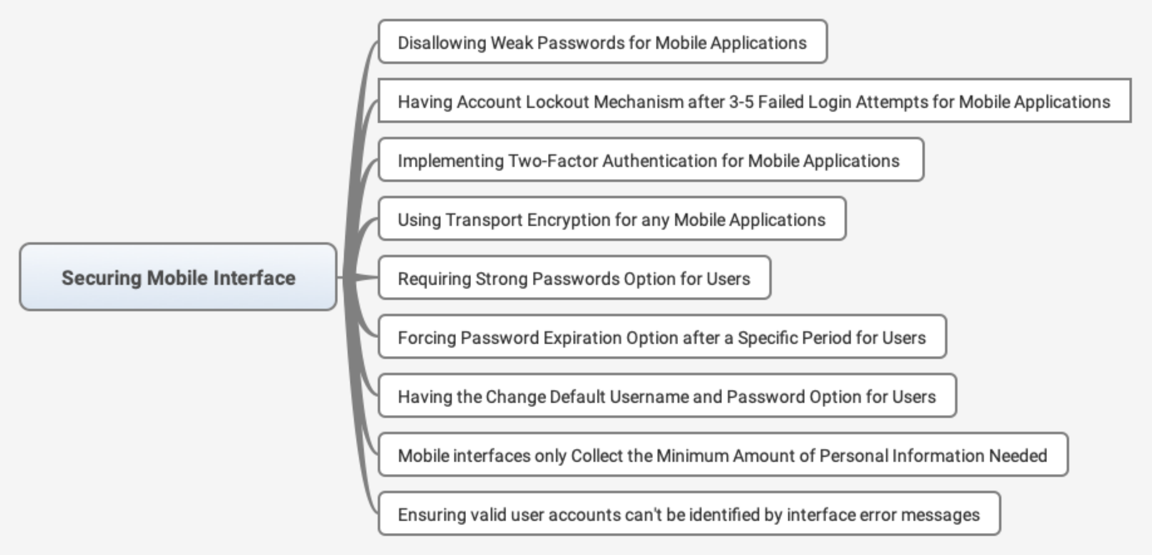
1.7.2.5. Having the Option to Force Password Expiration after a Specific Period for Users

1.7.2.6. Having the Option to change the default Username and Passwords for Users

1.7.2.7. Including an Account Lockout Mechanism after 3-5 Failed Login Attempts for any Cloud-based Web Interface

1.7.2.8. Ensuring valid user accounts can't be identified by interface error messages

1.7.3. Securing Mobile Interface


Securing Mobile Interface
Disallowing Weak Passwords for Mobile Applications
Having Account Lockout Mechanism after 3-5 Failed Login Attempts for Mobile Applications
Implementing Two-Factor Authentication for Mobile Applications
Using Transport Encryption for any Mobile Applications
Requiring Strong Passwords Option for Users
Forcing Password Expiration Option after a Specific Period for Users
Having the Change Default Username and Password Option for Users
Mobile interfaces only Collect the Minimum Amount of Personal Information Needed
Ensuring valid user accounts can't be identified by interface error messages

1.7.3.1. Disallowing Weak Passwords for Mobile Applications

1.7.3.2. Having Account Lockout Mechanism after 3-5 Failed Login Attempts for Mobile Applications

1.7.3.3. Implementing Two-Factor Authentication for Mobile Applications

1.7.3.4. Using Transport Encryption for any Mobile Applications

1.7.3.5. Requiring Strong Passwords Option for Users

1.7.3.6. Forcing Password Expiration Option after a Specific Period for Users

1.7.3.7. Having the Change Default Username and Password Option for Users

1.7.3.8. Mobile interfaces only Collect the Minimum Amount of Personal Information Needed

1.7.3.9. Ensuring valid user accounts can't be identified by interface error messages

1.7.4. Error-handling

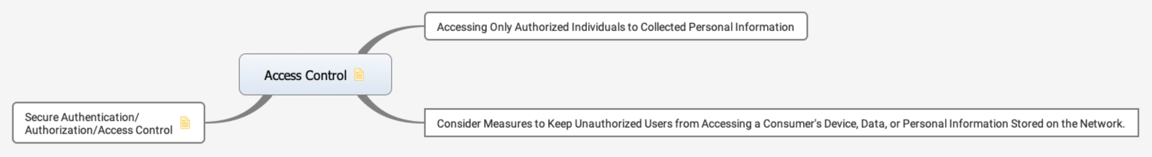
1.7.5. Rate Limiting Technique

1.7.6. Encrypting all API Communications

1.7.7. Implement Certificate Pinning Support

1.7.8. Embedding Timestamps

1.8. Access Control


Access Control
Accessing Only Authorized Individuals to Collected Personal Information
Consider Measures to Keep Unauthorized Users from Accessing a Consumer's Device, Data, or Personal Information Stored on the Network.
Secure Authentication/
Authorization/Access Control

According to ISO27001

According to definitions of ISO27000 access control means to ensure that access to assets is authorized and restricted based on business and security requirements.

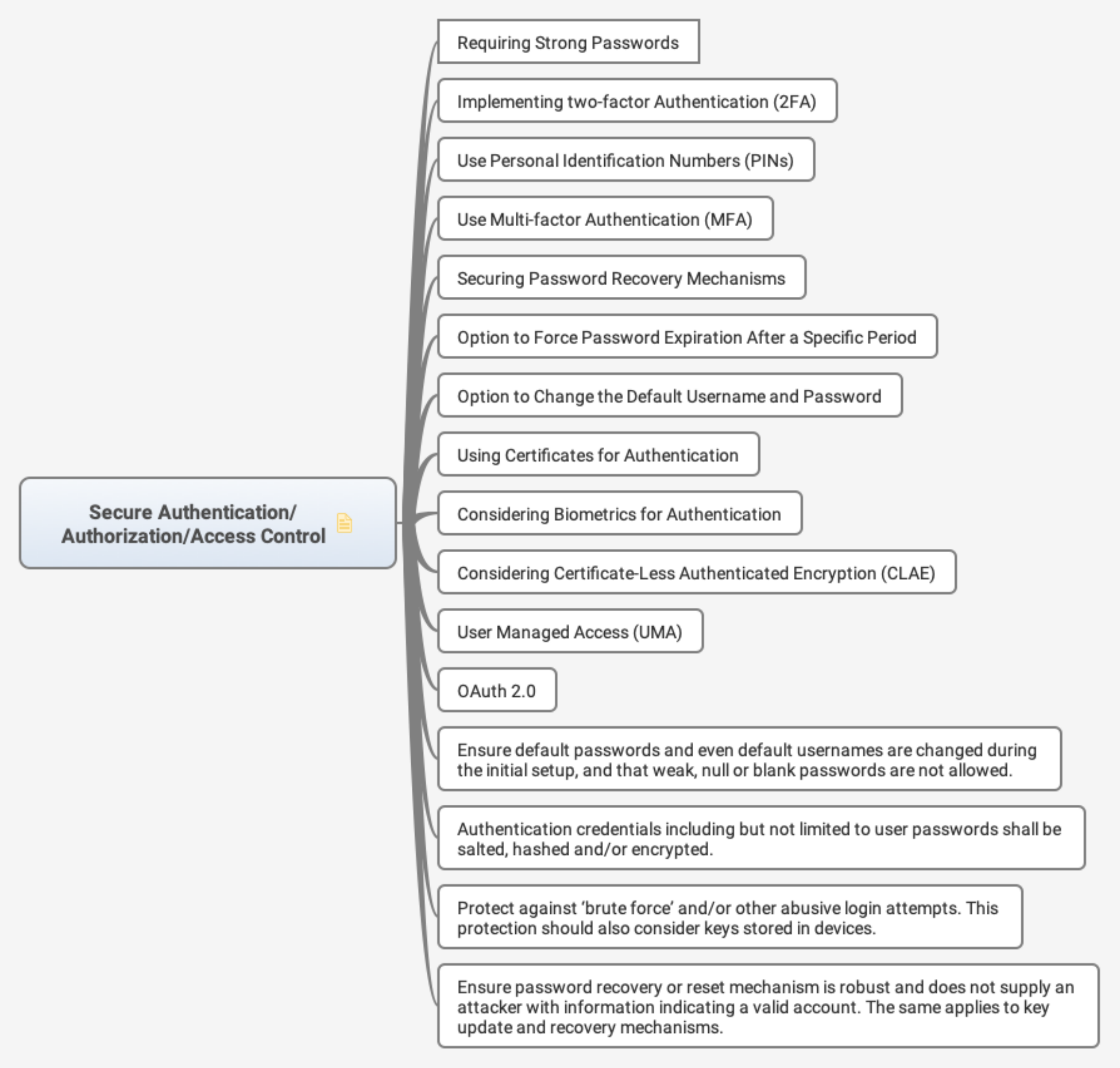
Objectives: (according to ISO27001 and ISO27002)

1. To limit access to information and information processing facilities.
2. To ensure authorized user access and to prevent unauthorized access to systems and services.
3. To make users accountable for safeguarding their authentication information.
4. To prevent unauthorized access to systems and applications.

1.8.1. Accessing Only Authorized Individuals to Collected Personal Information

1.8.2. Consider Measures to Keep Unauthorized Users from Accessing a Consumer's Device, Data, or Personal Information Stored on the Network.

1.8.3. Secure Authentication/ Authorization/Access Control



Secure Authentication/ Authorization/Access Control

Requiring Strong Passwords

Implementing two-factor Authentication (2FA)

Use Personal Identification Numbers (PINs)

Use Multi-factor Authentication (MFA)

Securing Password Recovery Mechanisms

Option to Force Password Expiration After a Specific Period

Option to Change the Default Username and Password

Using Certificates for Authentication

Considering Biometrics for Authentication

Considering Certificate-Less Authenticated Encryption (CLAE)

User Managed Access (UMA)

OAuth 2.0

Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.

Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.

Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.

Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

1.8.3.1. Requiring Strong Passwords

1.8.3.2. Implementing two-factor Authentication (2FA)

1.8.3.3. Use Personal Identification Numbers (PINs)

1.8.3.4. Use Multi-factor Authentication (MFA)

1.8.3.5. Securing Password Recovery Mechanisms

1.8.3.6. Option to Force Password Expiration After a Specific Period

1.8.3.7. Option to Change the Default Username and Password

1.8.3.8. Using Certificates for Authentication

1.8.3.9. Considering Biometrics for Authentication

1.8.3.10. Considering Certificate-Less Authenticated Encryption (CLAE)

1.8.3.11. User Managed Access (UMA)

1.8.3.12. OAuth 2.0

1.8.3.13. Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.

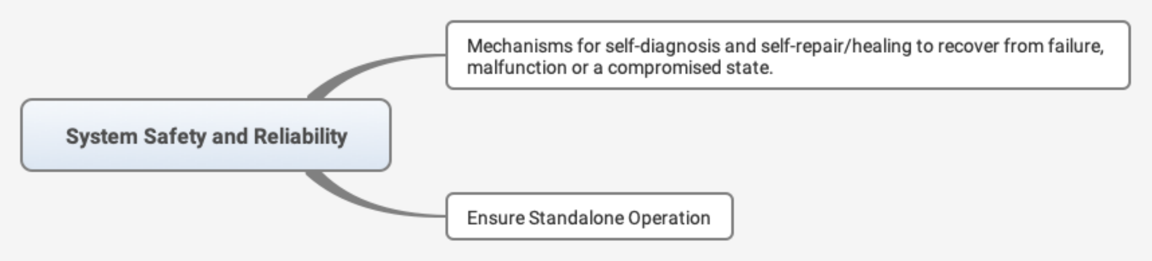
1.8.3.14. Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.

1.8.3.15. Protect against ‘brute force’ and/or other abusive login attempts. This protection should also consider keys stored in devices.

1.8.3.16. Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

1.9. Strong Default Security

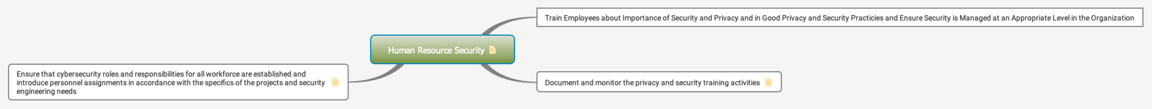
1.10. System Safety and Reliability


System Safety and Reliability
Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.
Ensure Standalone Operation

1.10.1. Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.

1.10.2. Ensure Standalone Operation

2. Human Resource Security


Human Resource Security
Train Employees about Importance of Security and Privacy and in Good Privacy and Security Practicies and Ensure Security is Managed at an Appropriate Level in the Organization
Document and monitor the privacy and security training activities
Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs

According to ISO27001

2.1. Train Employees about Importance of Security and Privacy and in Good Privacy and Security Practicies and Ensure Security is Managed at an Appropriate Level in the Organization

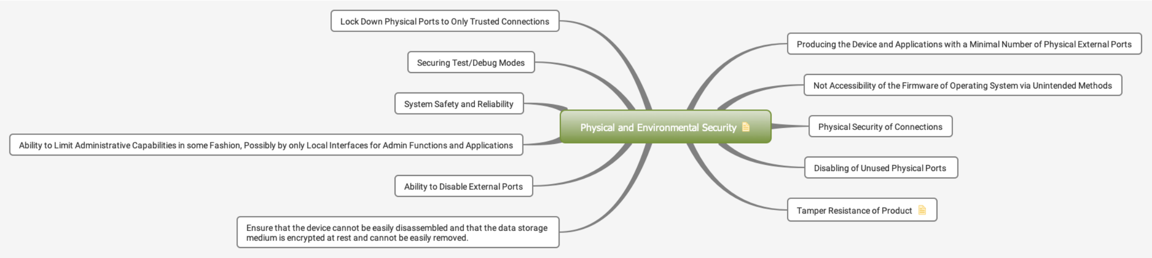
2.2. Document and monitor the privacy and security training activities

Reference: ENISA Baseline Security Recommendations for IoT

2.3. Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs

Reference: ENISA Baseline Security Recommendations for IoT

3. Physical and Environmental Security


Physical and Environmental Security
Lock Down Physical Ports to Only Trusted Connections
Securing Test/Debug Modes
System Safety and Reliability
Ability to Limit Administrative Capabilities in some Fashion, Possibly by only Local Interfaces for Admin Functions and Applications
Ability to Disable External Ports
Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.
Producing the Device and Applications with a Minimal Number of Physical External Ports
Not Accessibility of the Firmware of Operating System via Unintended Methods
Physical Security of Connections
Disabling of Unused Physical Ports
Tamper Resistance of Product

According to ISO27001

According to ISO27002 and ISO27001

Objectives of physical and environmental security are included:

1. To prevent unauthorized physical access, damage, and interference to the organization’s premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.

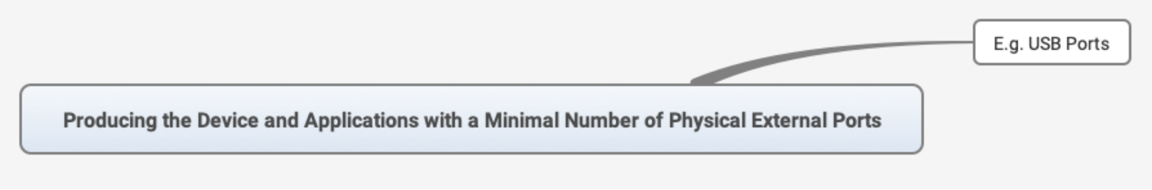
2. To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.

3. To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities. Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

Other references:

https://www.owasp.org/index.php/IoT_Security_Guidance

3.1. Producing the Device and Applications with a Minimal Number of Physical External Ports

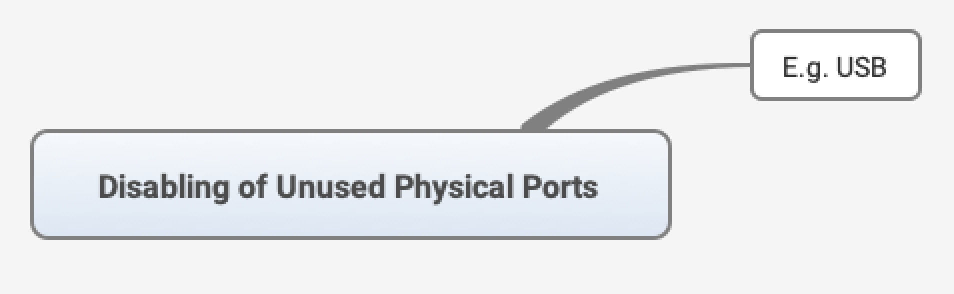

Producing the Device and Applications with a Minimal Number of Physical External Ports
E.g. USB Ports

3.1.1. E.g. USB Ports

3.2. Not Accessibility of the Firmware of Operating System via Unintended Methods

3.3. Physical Security of Connections

3.4. Disabling of Unused Physical Ports



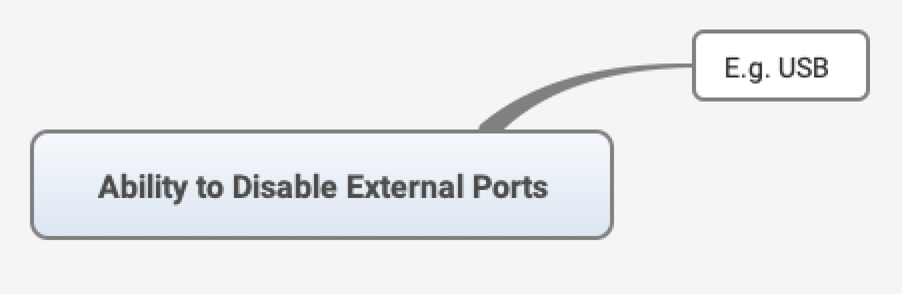
3.4.1. E.g. USB

3.5. Tamper Resistance of Product

Detection and reaction to hardware tampering should not rely on network connectivity.

3.6. Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.

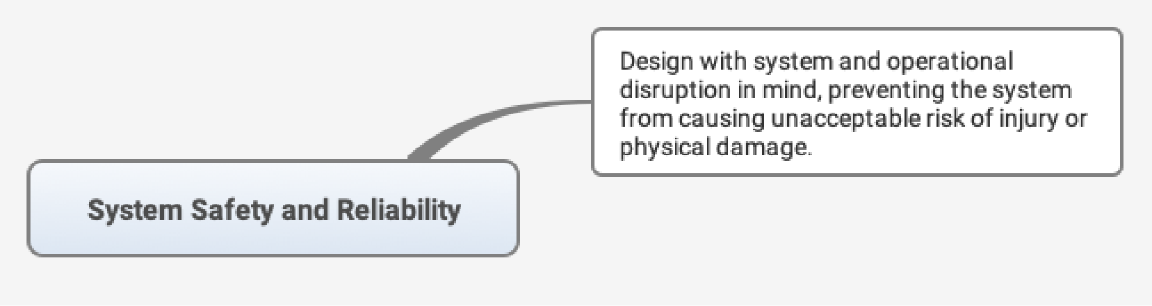
3.7. Ability to Disable External Ports



3.7.1. E.g. USB

3.8. Ability to Limit Administrative Capabilities in some Fashion, Possibly by only Local Interfaces for Admin Functions and Applications

3.9. System Safety and Reliability

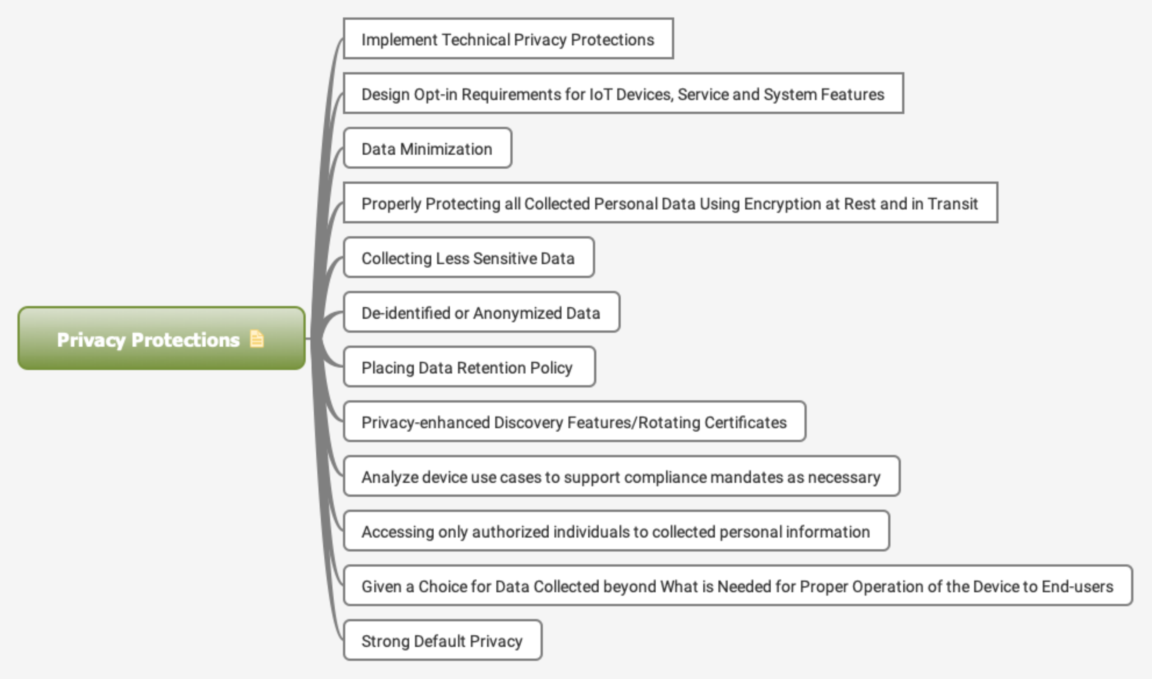

Design with system and operational disruption in mind, preventing the system from causing unacceptable risk of injury or physical damage.
System Safety and Reliability

3.9.1. Design with system and operational disruption in mind, preventing the system from causing unacceptable risk of injury or physical damage.

3.10. Securing Test/Debug Modes

3.11. Lock Down Physical Ports to Only Trusted Connections

4. Privacy Protections


Privacy Protections
Implement Technical Privacy Protections
Design Opt-in Requirements for IoT Devices, Service and System Features
Data Minimization
Properly Protecting all Collected Personal Data Using Encryption at Rest and in Transit
Collecting Less Sensitive Data
De-identified or Anonymized Data
Placing Data Retention Policy
Privacy-enhanced Discovery Features/Rotating Certificates
Analyze device use cases to support compliance mandates as necessary
Accessing only authorized individuals to collected personal information
Given a Choice for Data Collected beyond What is Needed for Proper Operation of the Device to End-users
Strong Default Privacy

Refrences:

ISO/IEC 27001

https://www.owasp.org/index.php/IoT_Security_Guidance

Future-proofing the Connected World - Cloud Security Alliance

4.1. Implement Technical Privacy Protections

4.2. Design Opt-in Requirements for IoT Devices, Service and System Features

4.3. Data Minimization

Data Minimization
Collecting Minimal Amount of Personal Information from Consumers

4.3.1. Collecting Minimal Amount of Personal Information from Consumers

4.4. Properly Protecting all Collected Personal Data Using Encryption at Rest and in Transit

4.5. Collecting Less Sensitive Data

4.6. De-identified or Anonymized Data

4.7. Placing Data Retention Policy

4.8. Privacy-enhanced Discovery Features/Rotating Certificates

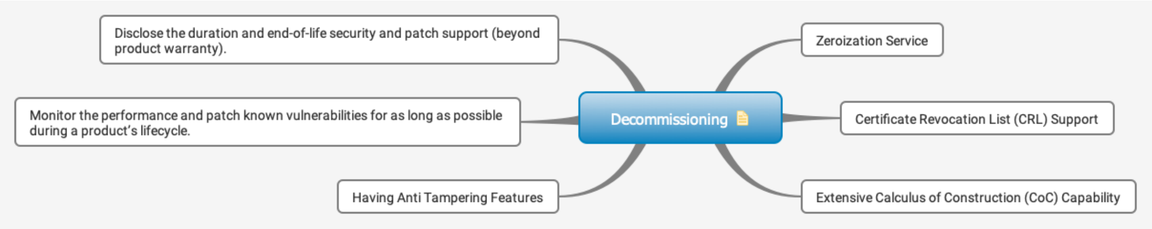
4.9. Analyze device use cases to support compliance mandates as necessary

4.10. Accessing only authorized individuals to collected personal information

4.11. Given a Choice for Data Collected beyond What is Needed for Proper Operation of the Device to End-users

4.12. Strong Default Privacy

5. Decommissioning


Disclose the duration and end-of-life security and patch support (beyond product warranty).
Zeroization Service
Monitor the performance and patch known vulnerabilities for as long as possible during a product's lifecycle.
Decommissioning
Certificate Revocation List (CRL) Support
Having Anti Tampering Features
Extensive Calculus of Construction (CoC) Capability

References:

5.1. Zeroization Service

5.2. Certificate Revocation List (CRL) Support

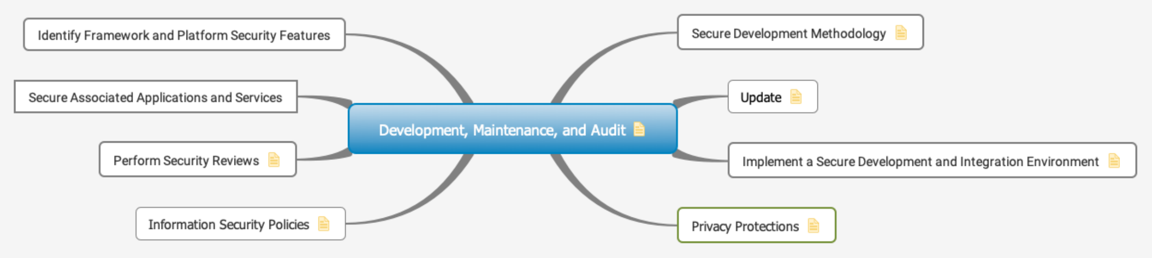
5.3. Extensive Calculus of Construction (CoC) Capability

5.4. Having Anti Tampering Features

5.5. Monitor the performance and patch known vulnerabilities for as long as possible during a product's lifecycle.

5.6. Disclose the duration and end-of-life security and patch support (beyond product warranty).

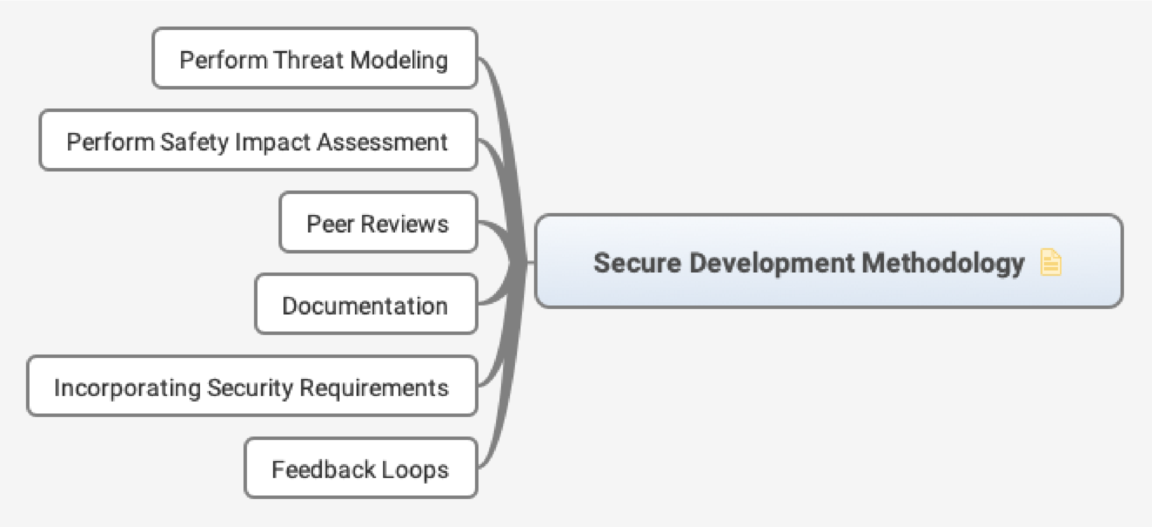
6. Development, Maintenance, and Audit


Identify Framework and Platform Security Features
Secure Associated Applications and Services
Perform Security Reviews
Information Security Policies
Development, Maintenance, and Audit
Secure Development Methodology
Update
Implement a Secure Development and Integration Environment
Privacy Protections

According to ISO27001

"Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually. Reference: ENISA Baseline Security Recommendations for IoT"

6.1. Secure Development Methodology


Perform Threat Modeling
Perform Safety Impact Assessment
Peer Reviews
Documentation
Incorporating Security Requirements
Feedback Loops
Secure Development Methodology

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

6.1.1. Perform Threat Modeling

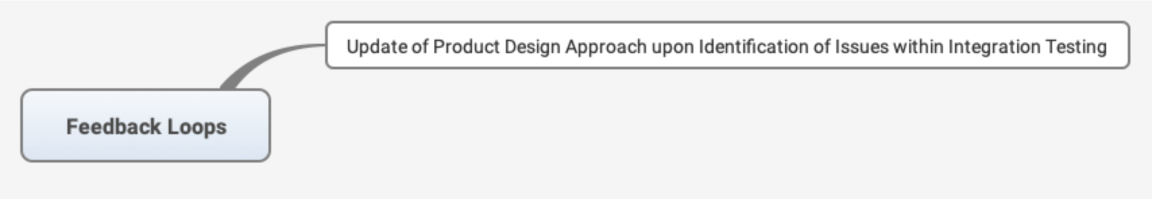
6.1.2. Perform Safety Impact Assessment

6.1.3. Peer Reviews

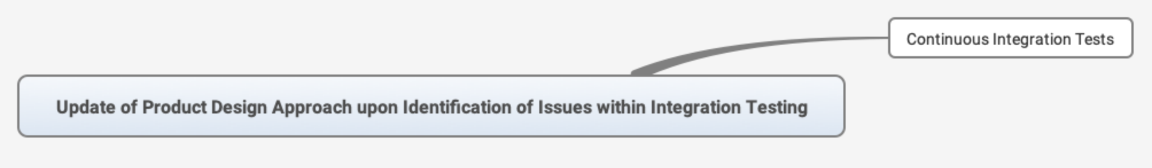
6.1.4. Documentation

6.1.5. Incorporating Security Requirements

6.1.6. Feedback Loops

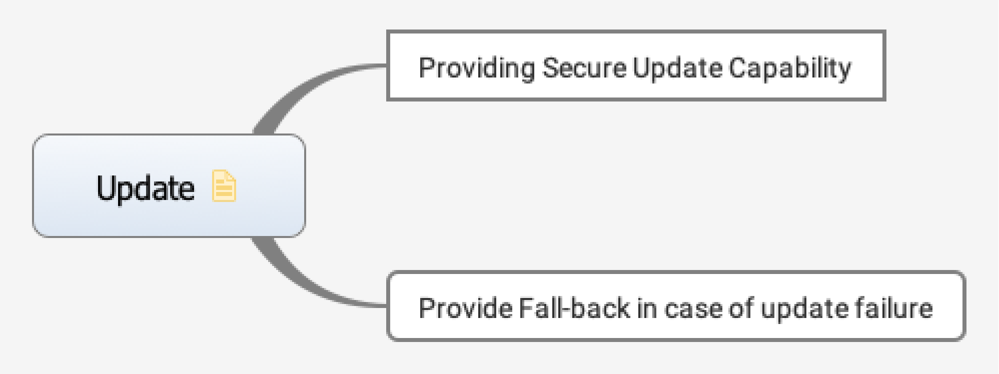

Update of Product Design Approach upon Identification of Issues within Integration Testing
Feedback Loops

6.1.6.1. Update of Product Design Approach upon Identification of Issues within Integration Testing


Update of Product Design Approach upon Identification of Issues within Integration Testing
Continuous Integration Tests

Continuous Integration Tests

6.2. Update


Update
Providing Secure Update Capability
Provide Fall-back in case of update failure

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

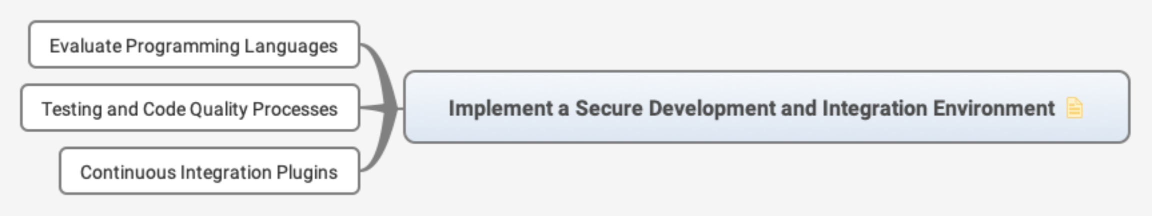
Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

6.2.1. Providing Secure Update Capability

6.2.2. Provide Fall-back in case of update failure

6.3. Implement a Secure Development and Integration Environment


Evaluate Programming Languages
Testing and Code Quality Processes
Continuous Integration Plugins
Implement a Secure Development and Integration Environment

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

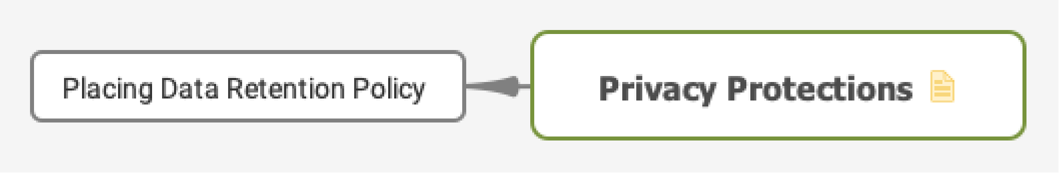
Future-proofing the Connected World - Cloud Security Alliance, 2016

6.3.1. Evaluate Programming Languages

6.3.2. Testing and Code Quality Processes

6.3.3. Continuous Integration Plugins

6.4. Privacy Protections



References:

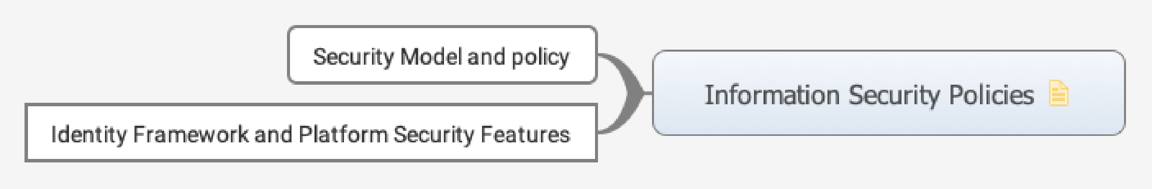
https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

6.4.1. Placing Data Retention Policy

6.5. Information Security Policies


Security Model and policy
Identity Framework and Platform Security Features
Information Security Policies

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

6.5.1. Security Model and policy

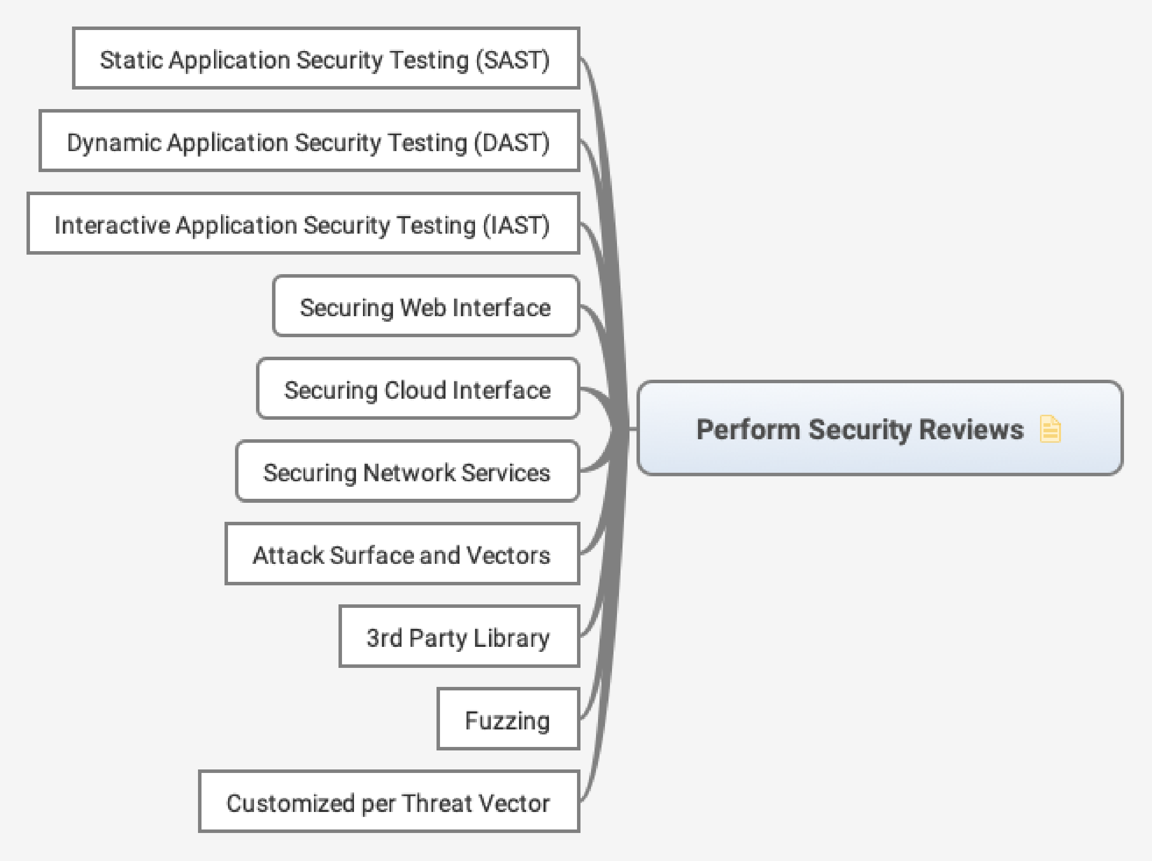
6.5.1.1. Data Protection

Security Considerations for Selecting IoT Communication Protocols
Data Protection

Security Considerations for Selecting IoT Communication Protocols

6.5.2. Identity Framework and Platform Security Features

6.6. Perform Security Reviews


Static Application Security Testing (SAST)
Dynamic Application Security Testing (DAST)
Interactive Application Security Testing (IAST)
Securing Web Interface
Securing Cloud Interface
Securing Network Services
Attack Surface and Vectors
3rd Party Library
Fuzzing
Customized per Threat Vector
Perform Security Reviews

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

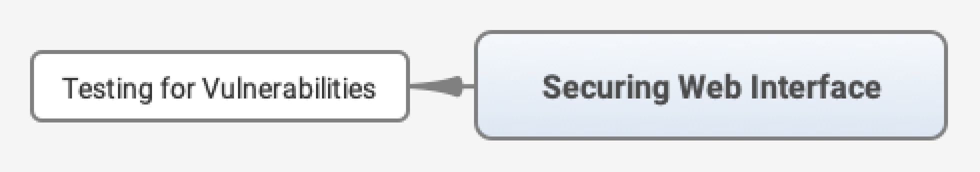
Future-proofing the Connected World - Cloud Security Alliance, 2016

6.6.1. Static Application Security Testing (SAST)

6.6.2. Dynamic Application Security Testing (DAST)

6.6.3. Interactive Application Security Testing (IAST)

6.6.4. Securing Web Interface



6.6.4.1. Testing for Vulnerabilities

XSS
Testing for Vulnerabilities
CSRF
SQLi

XSS

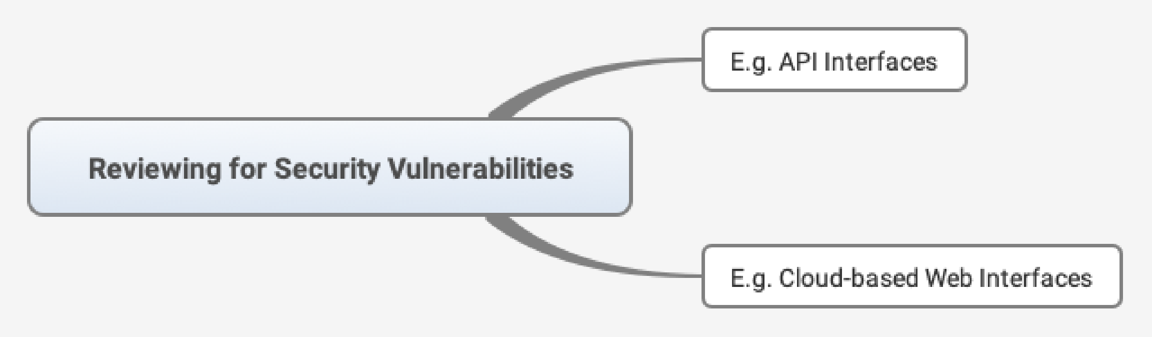
SQLi

CSRF

6.6.5. Securing Cloud Interface

Reviewing for Security Vulnerabilities
Securing Cloud Interface
Testing any Cloud-based Web Interface for Vulnerabilities

6.6.5.1. Reviewing for Security Vulnerabilities


E.g. API Interfaces
Reviewing for Security Vulnerabilities
E.g. Cloud-based Web Interfaces

E.g. API Interfaces

E.g. Cloud-based Web Interfaces

6.6.5.2. Testing any Cloud-based Web Interface for Vulnerabilities

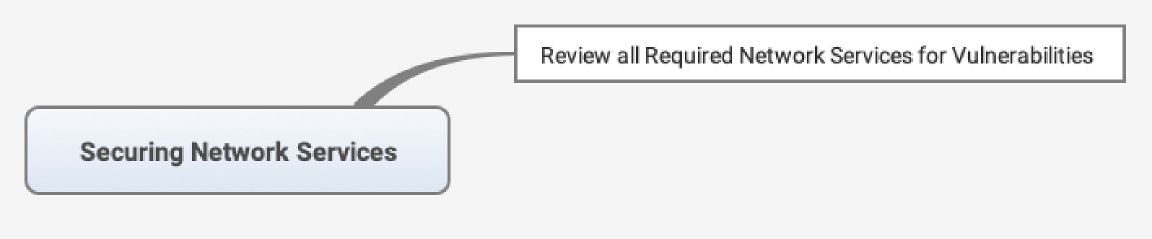
Testing any Cloud-based Web Interface for Vulnerabilities
XSS
CSRF
SQLi

XSS

SQLi

CSRF

6.6.6. Securing Network Services


Review all Required Network Services for Vulnerabilities
Securing Network Services

6.6.6.1. Review all Required Network Services for Vulnerabilities

6.6.7. Attack Surface and Vectors

6.6.8. 3rd Party Library

6.6.9. Fuzzing

6.6.10. Customized per Threat Vector

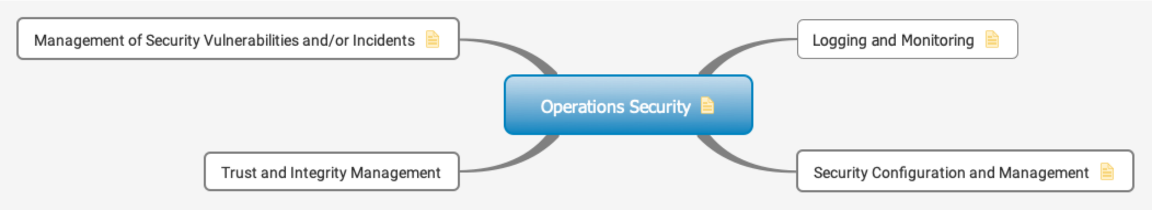
6.7. Secure Associated Applications and Services

6.8. Identify Framework and Platform Security Features

Evaluate Platform Security Features
Identify Framework and Platform Security Features

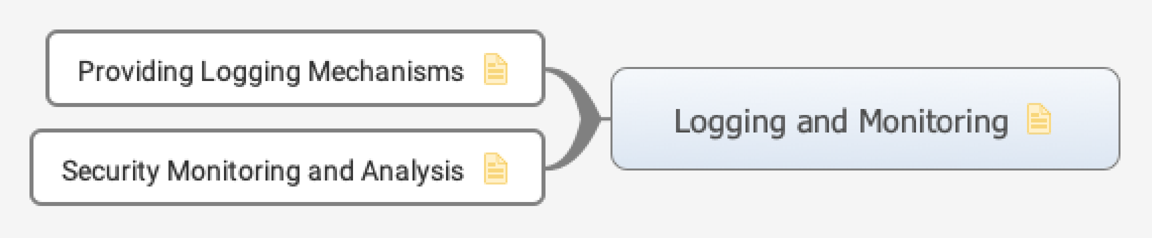
6.8.1. Evaluate Platform Security Features

7. Operations Security


Management of Security Vulnerabilities and/or Incidents
Logging and Monitoring
Operations Security
Trust and Integrity Management
Security Configuration and Management

According to ISO27001

7.1. Logging and Monitoring


Providing Logging Mechanisms
Security Monitoring and Analysis
Logging and Monitoring

References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

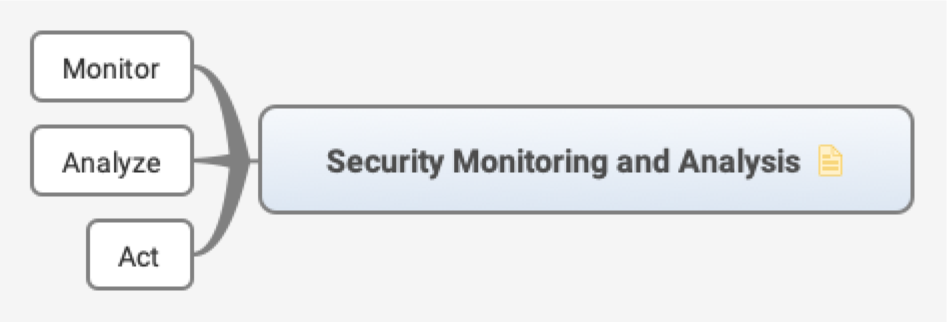
Future-proofing the Connected World - Cloud Security Alliance, 2016

7.1.1. Providing Logging Mechanisms

Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system.

Reference: ENISA Baseline Security Recommendations for IoT

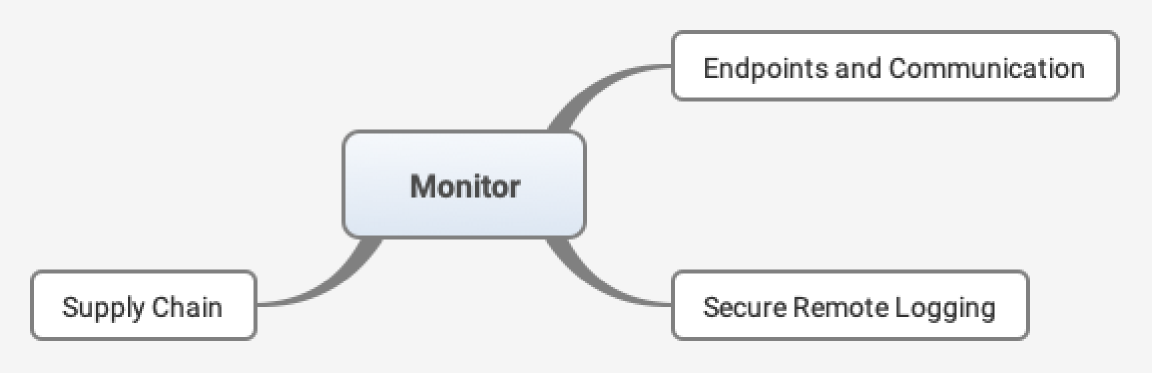
7.1.2. Security Monitoring and Analysis



Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.

Reference: ENISA Baseline Security Recommendations for IoT

7.1.2.1. Monitor

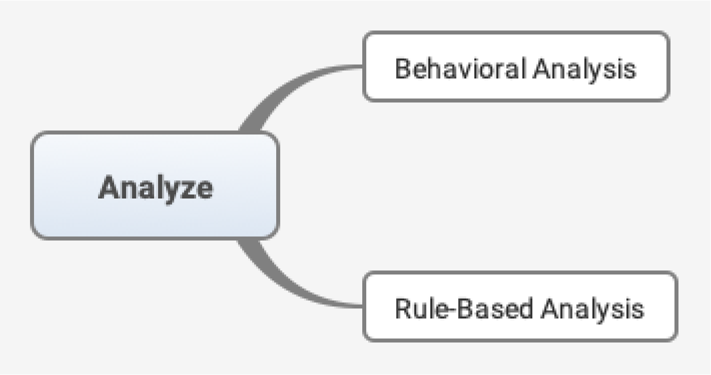


Endpoints and Communication

Secure Remote Logging

Supply Chain

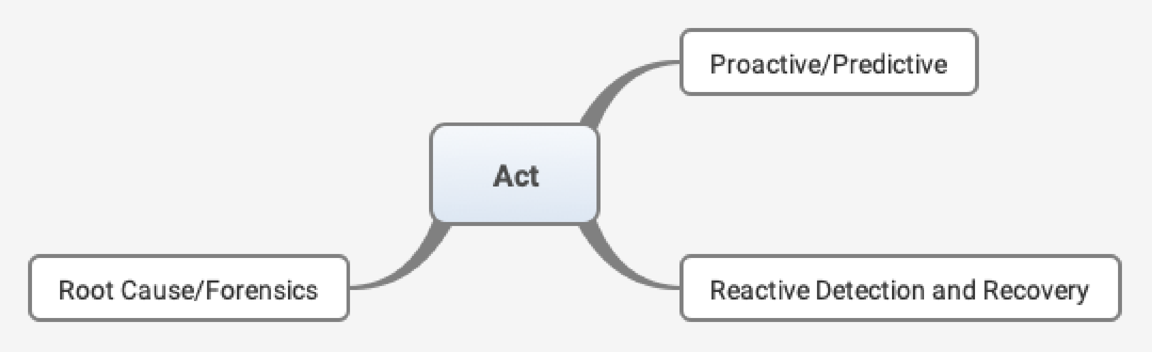
7.1.2.2. Analyze



Behavioral Analysis

Rule-Based Analysis

7.1.2.3. Act

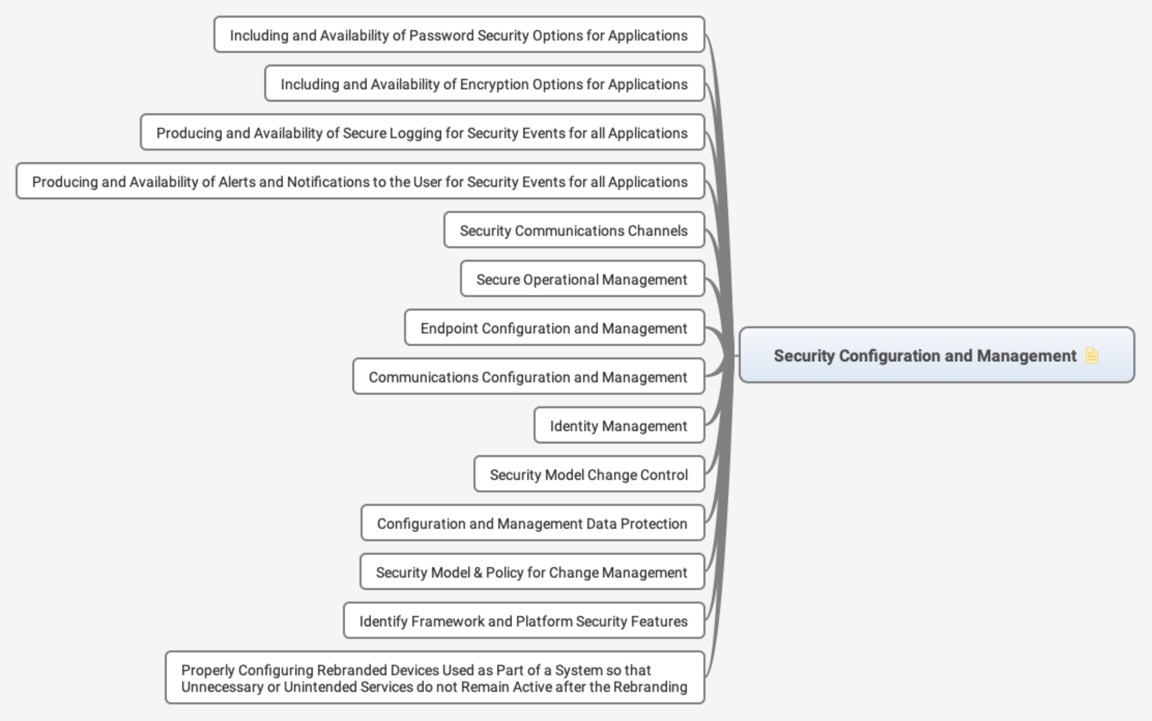


Proactive/Predictive

Reactive Detection and Recovery

Root Cause/Forensics

7.2. Security Configuration and Management


Including and Availability of Password Security Options for Applications
Including and Availability of Encryption Options for Applications
Producing and Availability of Secure Logging for Security Events for all Applications
Producing and Availability of Alerts and Notifications to the User for Security Events for all Applications
Security Communications Channels
Secure Operational Management
Endpoint Configuration and Management
Communications Configuration and Management
Identity Management
Security Model Change Control
Configuration and Management Data Protection
Security Model & Policy for Change Management
Identify Framework and Platform Security Features
Properly Configuring Rebranded Devices Used as Part of a System so that Unnecessary or Unintended Services do not Remain Active after the Rebranding
Security Configuration and Management

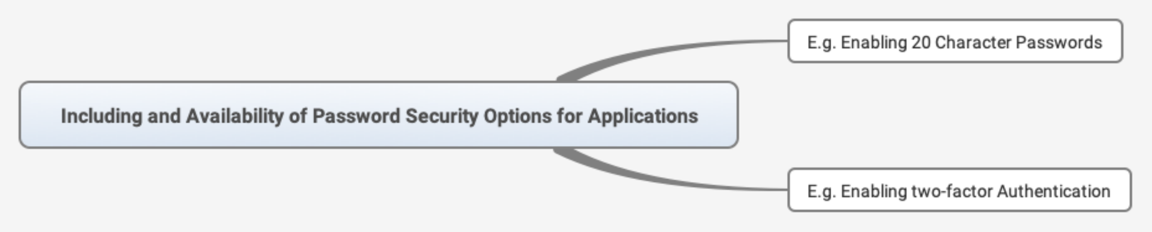
References:

https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

7.2.1. Including and Availability of Password Security Options for Applications


Including and Availability of Password Security Options for Applications
E.g. Enabling 20 Character Passwords
E.g. Enabling two-factor Authentication

7.2.1.1. E.g. Enabling 20 Character Passwords

7.2.1.2. E.g. Enabling two-factor Authentication

7.2.2. Including and Availability of Encryption Options for Applications

E.g. Enabling AES-256 where AES-128 is the default setting
Including and Availability of Encryption Options for Applications

7.2.2.1. E.g. Enabling AES-256 where AES-128 is the default setting

7.2.3. Producing and Availability of Secure Logging for Security Events for all Applications

7.2.4. Producing and Availability of Alerts and Notifications to the User for Security Events for all Applications

7.2.5. Security Communications Channels

7.2.6. Secure Operational Management

7.2.7. Endpoint Configuration and Management

7.2.8. Communications Configuration and Management

7.2.9. Identity Management

7.2.10. Security Model Change Control

7.2.11. Configuration and Management Data Protection

7.2.12. Security Model & Policy for Change Management

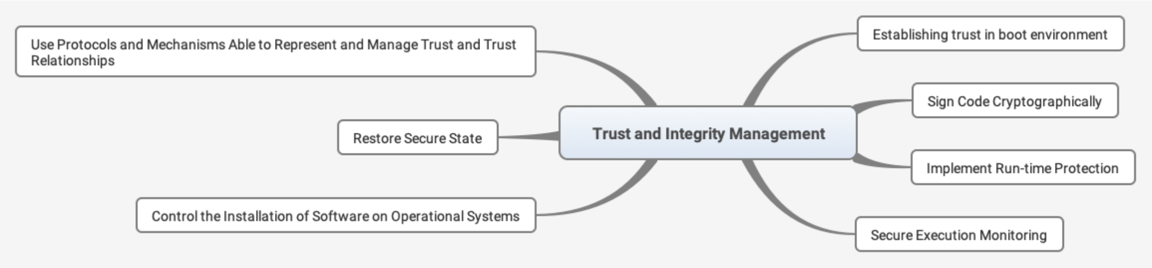
7.2.13. Identify Framework and Platform Security Features

Selecting an Integration Framework
Identify Framework and Platform Security Features

7.2.13.1. Selecting an Integration Framework

7.2.14. Properly Configuring Rebranded Devices Used as Part of a System so that Unnecessary or Unintended Services do not Remain Active after the Rebranding

7.3. Trust and Integrity Management


Trust and Integrity Management
Use Protocols and Mechanisms Able to Represent and Manage Trust and Trust Relationships
Establishing trust in boot environment
Sign Code Cryptographically
Restore Secure State
Implement Run-time Protection
Control the Installation of Software on Operational Systems
Secure Execution Monitoring

7.3.1. Establishing trust in boot environment

7.3.2. Sign Code Cryptographically

7.3.3. Implement Run-time Protection

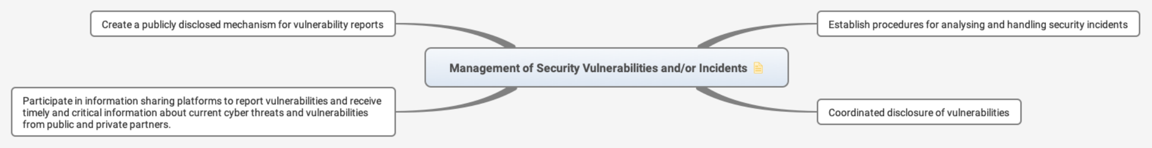
7.3.4. Secure Execution Monitoring

7.3.5. Control the Installation of Software on Operational Systems

7.3.6. Restore Secure State

7.3.7. Use Protocols and Mechanisms Able to Represent and Manage Trust and Trust Relationships

7.4. Management of Security Vulnerabilities and/or Incidents


Create a publicly disclosed mechanism for vulnerability reports
Establish procedures for analysing and handling security incidents
Management of Security Vulnerabilities and/or Incidents
Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.
Coordinated disclosure of vulnerabilities

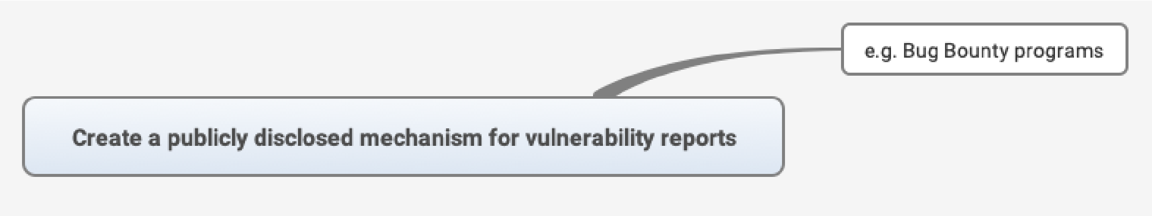
Reference: ENISA Baseline Security Recommendations for IoT

7.4.1. Establish procedures for analysing and handling security incidents

7.4.2. Coordinated disclosure of vulnerabilities

7.4.3. Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

7.4.4. Create a publicly disclosed mechanism for vulnerability reports


Create a publicly disclosed mechanism for vulnerability reports
e.g. Bug Bounty programs

7.4.4.1. e.g. Bug Bounty programs