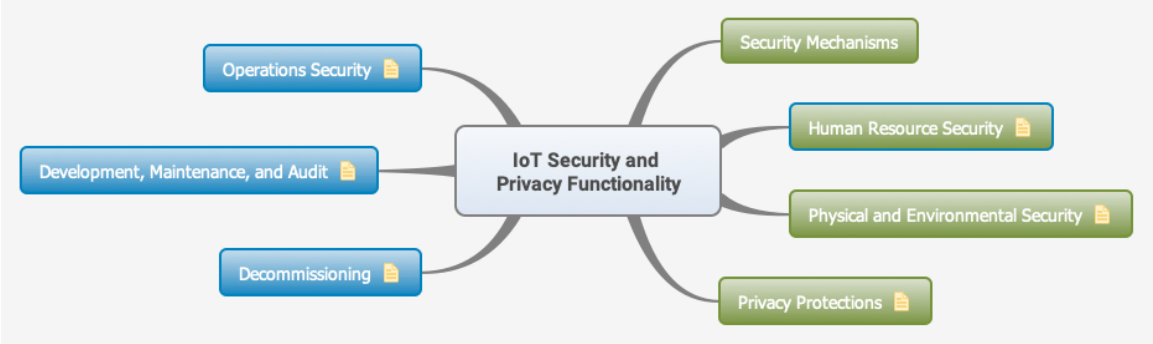
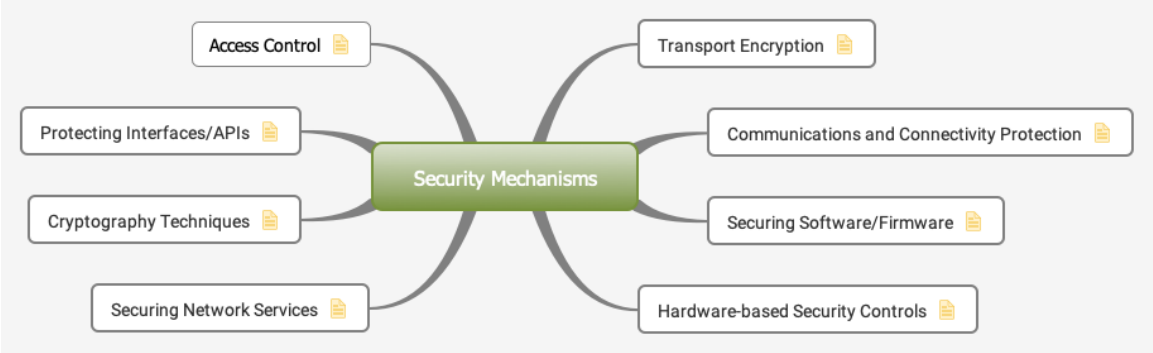
IoT Security and

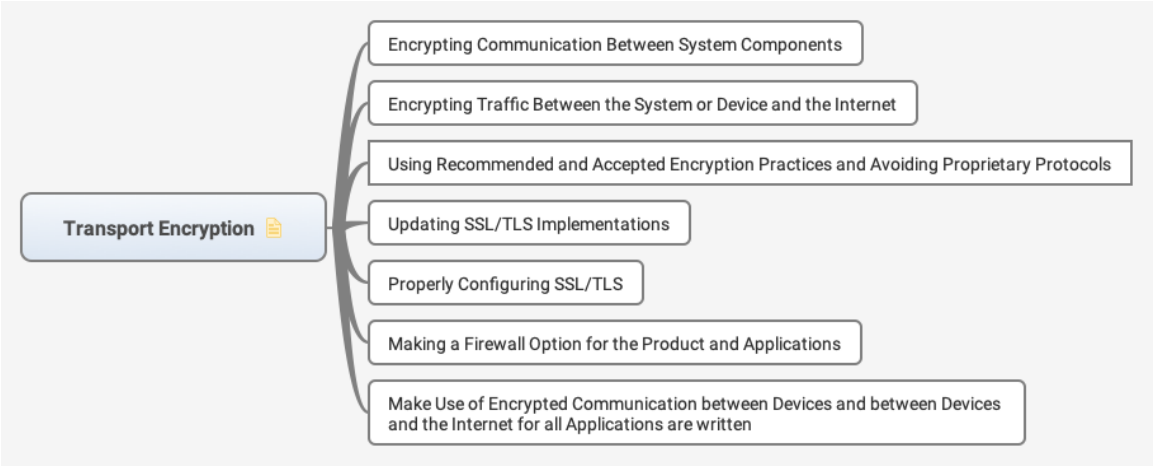
Privacy Functionality



1. Security Mechanisms



1.1. Transport Encryption



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

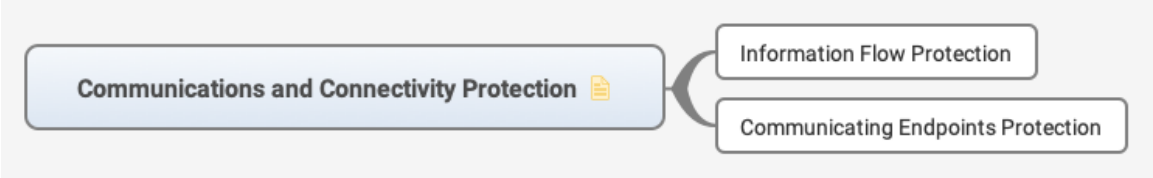
1.1.4. Updating SSL/TLS Implementations

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. Communications and Connectivity Protection



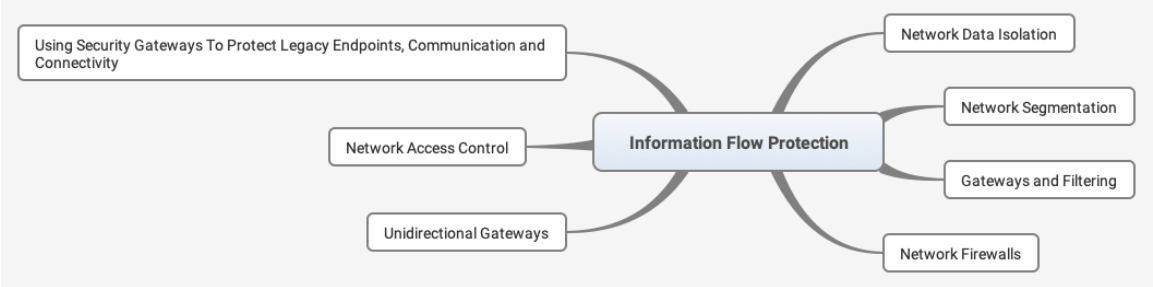
References:

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

1.2.1. 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

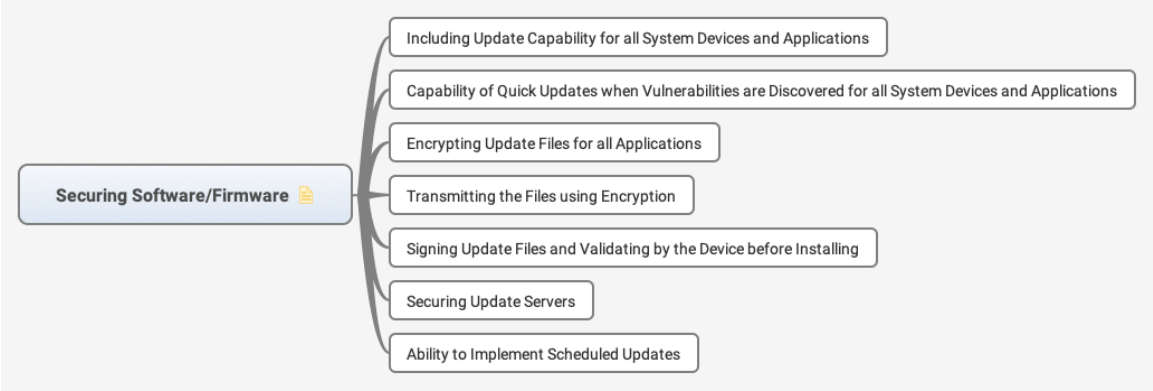
1.2.1.5. Unidirectional Gateways

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

1.3. Securing Software/Firmware



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

1.3.1. 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

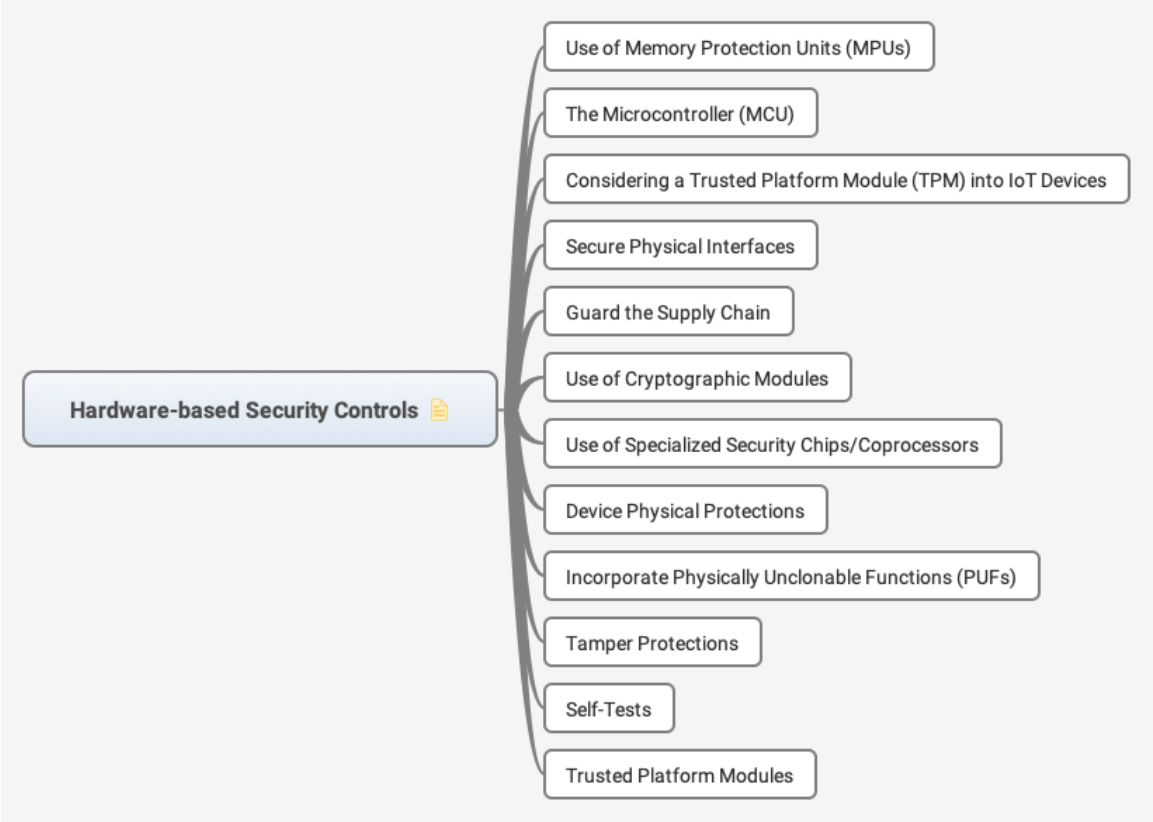
1.3.4. Transmitting the Files using Encryption

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

1.4. Hardware-based Security Controls



References:

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

Industrial Internet of Things Volume G4: Security Framework, 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

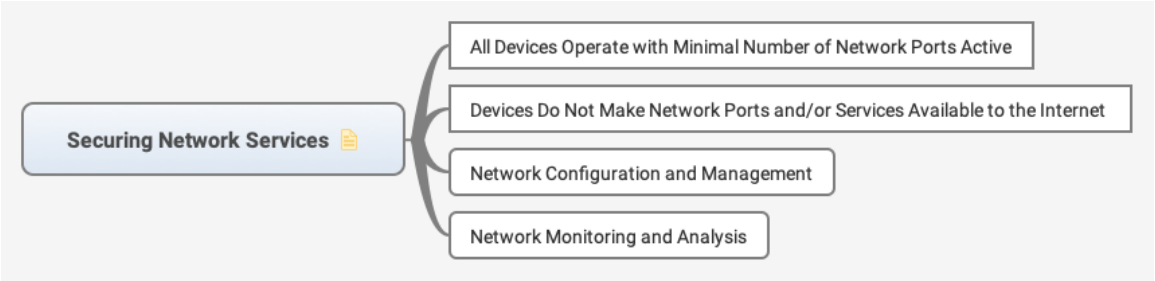
1.4.9. Incorporate Physically Unclonable Functions (PUFs)

1.4.10. Tamper Protections

1.4.11. Self-Tests

1.4.12. Trusted Platform Modules

1.5. Securing Network Services



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

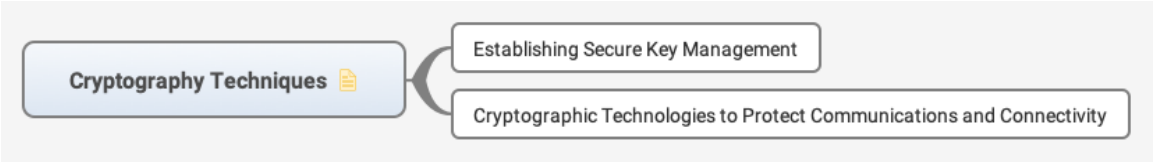
1.5.1. All Devices Operate with Minimal Number of Network Ports Active

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



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 Key Management

1.6.1.1. Design Secure Bootstrap Functions

1.6.2. Cryptographic Technologies to Protect Communications and Connectivity

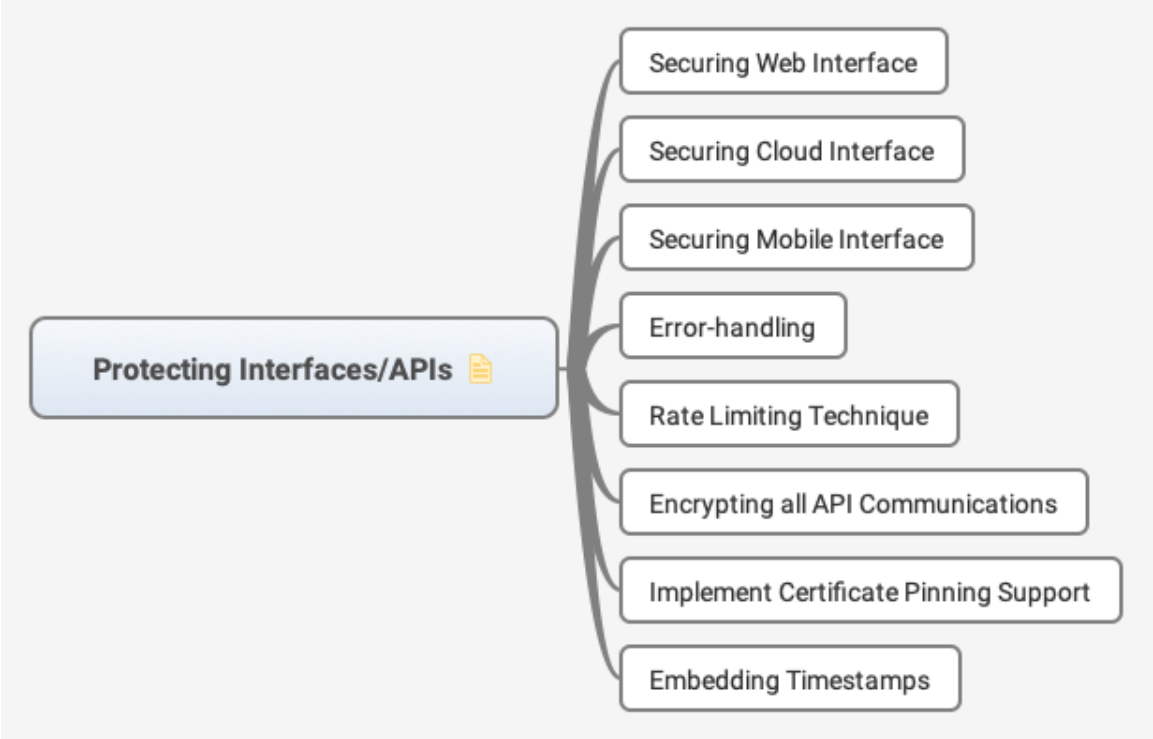
1.6.2.1. Security Controls in Communication and Connectivity Protocols

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

1.7. Protecting Interfaces/APIs



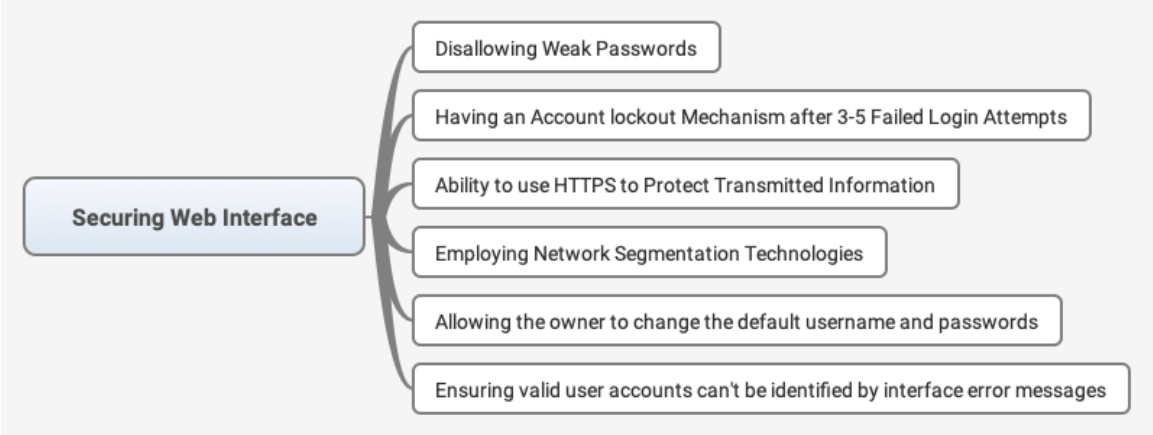
References:

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

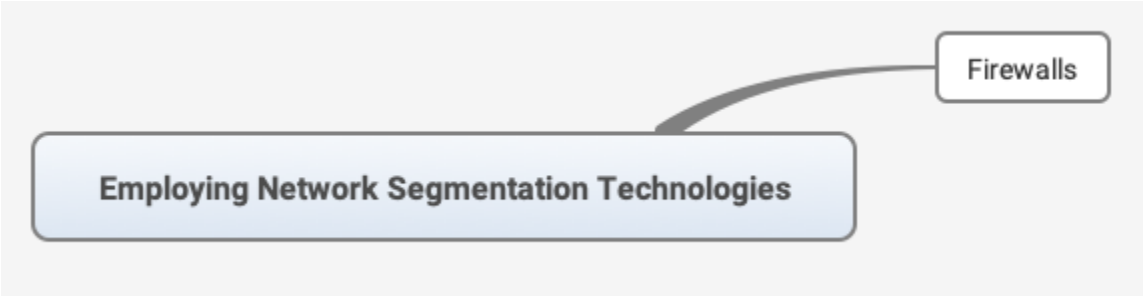


1.7.1.1. Disallowing Weak Passwords

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

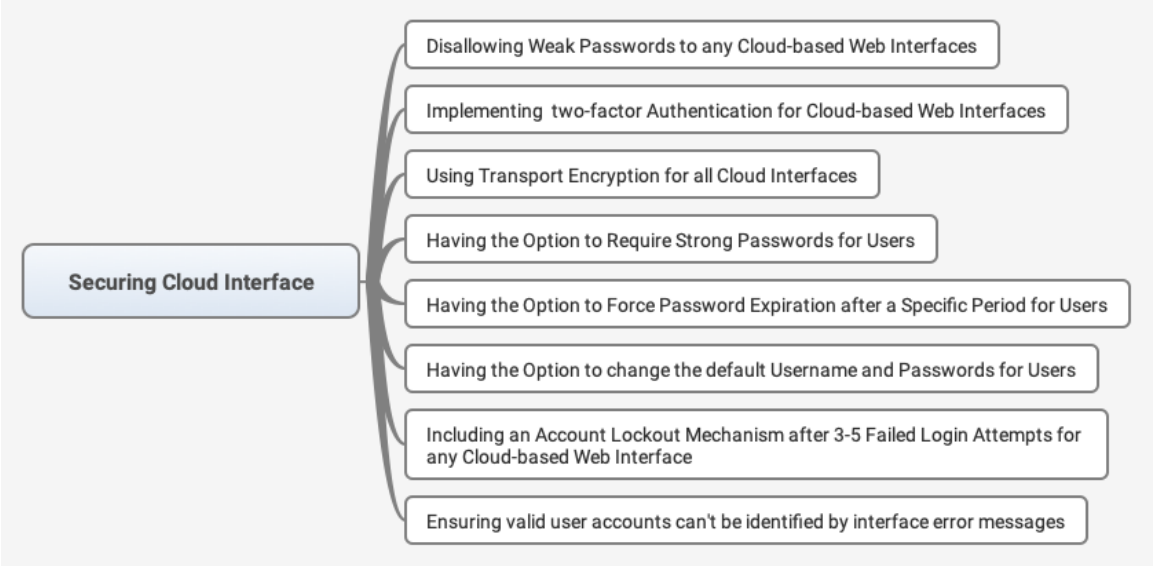


Firewalls

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



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

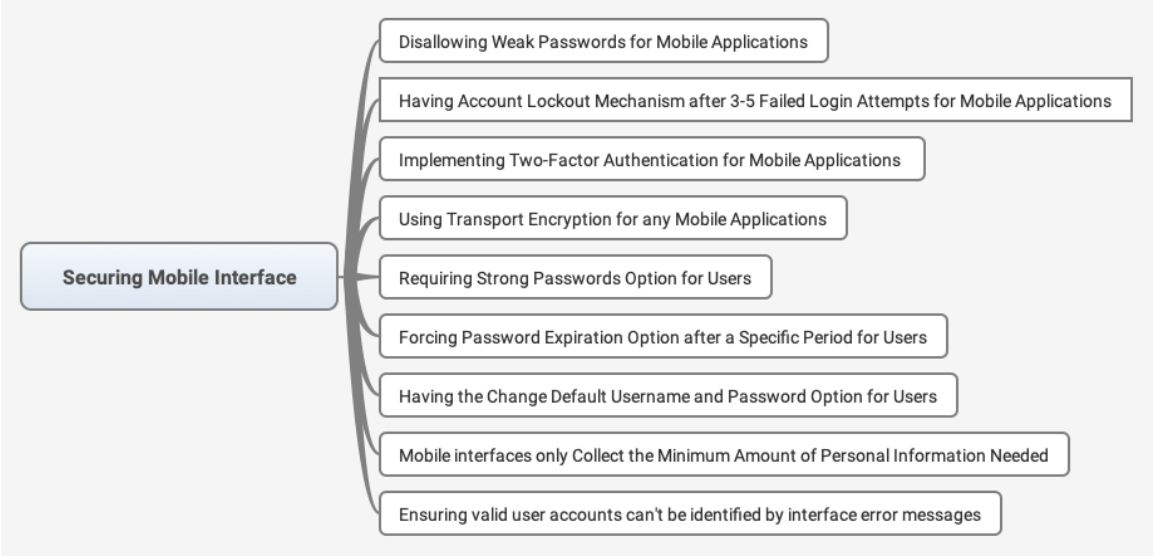
1.7.2.5. Having the Option to Force Password Expiration after a Specific Period for Users

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



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

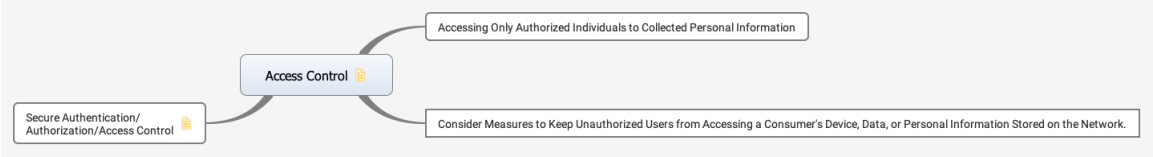
1.7.5. Rate Limiting Technique

1.7.6. Encrypting all API Communications

1.7.7. Implement Certificate Pinning Support

1.7.8. Embedding Timestamps

1.8. Access Control



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.

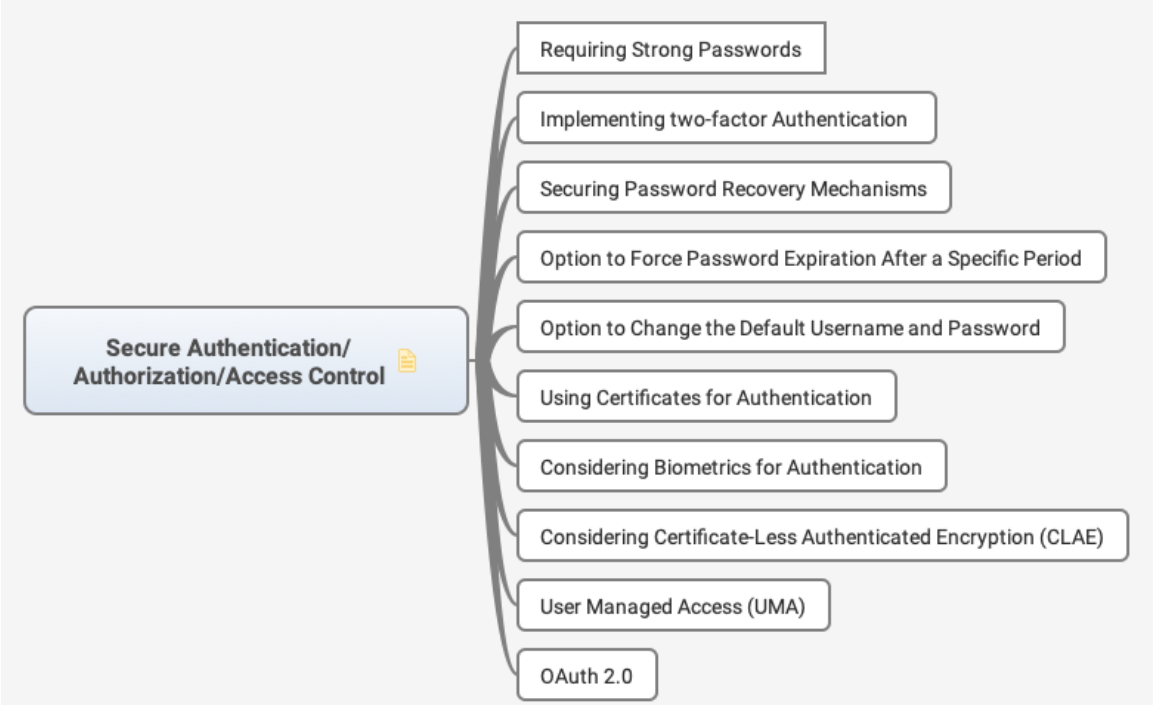
Objectives: (according to ISO27001 and ISO27002)

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



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

1.8.3.3. Securing Password Recovery Mechanisms

1.8.3.4. Option to Force Password Expiration After a Specific Period

1.8.3.5. Option to Change the Default Username and Password

1.8.3.6. Using Certificates for Authentication

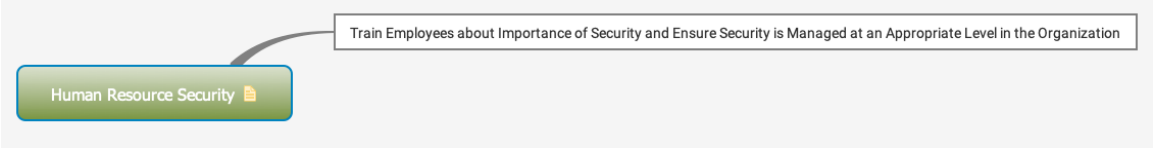
1.8.3.7. Considering Biometrics for Authentication

1.8.3.8. Considering Certificate-Less Authenticated Encryption (CLAE)

1.8.3.9. User Managed Access (UMA)

1.8.3.10. OAuth 2.0

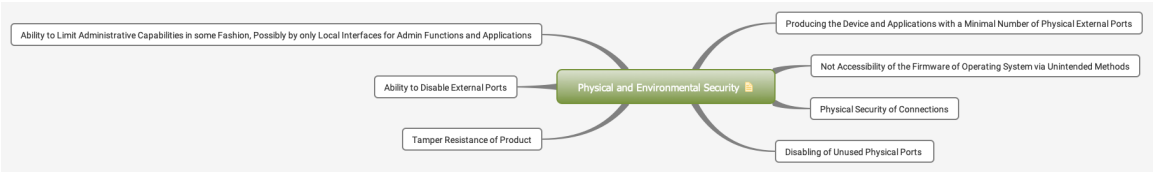
2. Human Resource Security



According to ISO27001

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

3. Physical and Environmental Security



According to ISO27001

According to ISO27002 and ISO27001

Objectives of physical and environmental security are included:

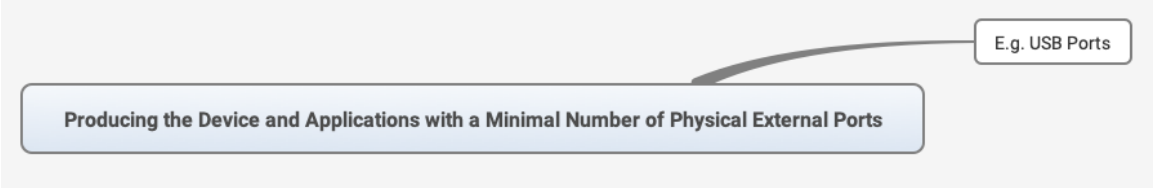
1. To prevent unauthorized physical access, damage, and interference to the organization's premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. 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



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

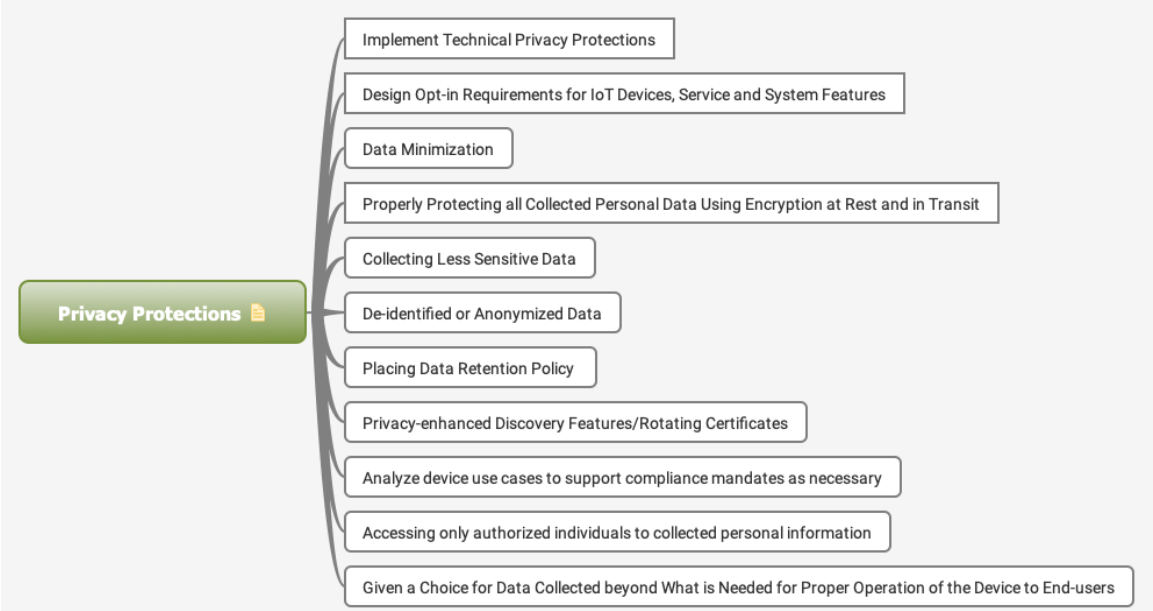
3.5. Tamper Resistance of Product

3.6. Ability to Disable External Ports

3.6.1. E.g. USB

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

4. Privacy Protections



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

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

5. Decommissioning

References:

Securing Your Embedded System Life Cycle - Microsemi

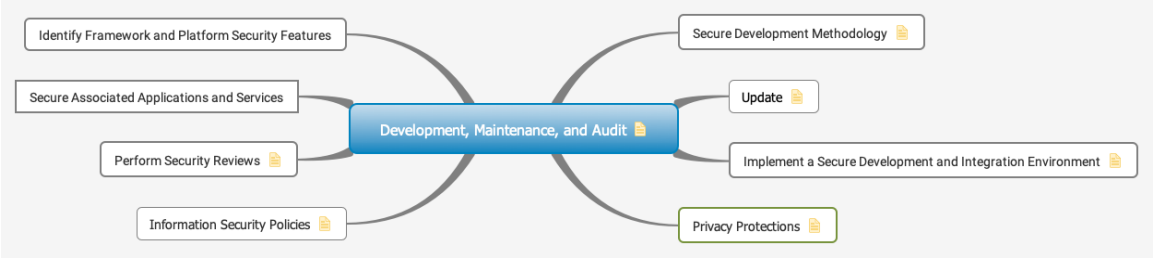
5.1. Zeroization Service

5.2. Certificate Revocation List (CRL) Support

5.3. Extensive Calculus of Construction (CoC) Capability

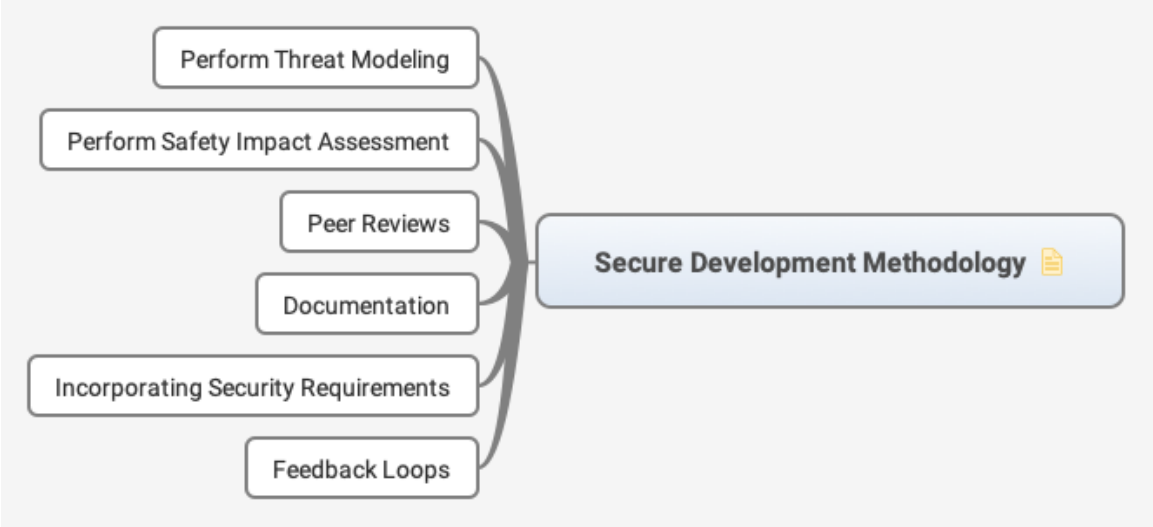
5.4. Having Anti Tampering Features

6. Development, Maintenance, and Audit



According to ISO27001

6.1. 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

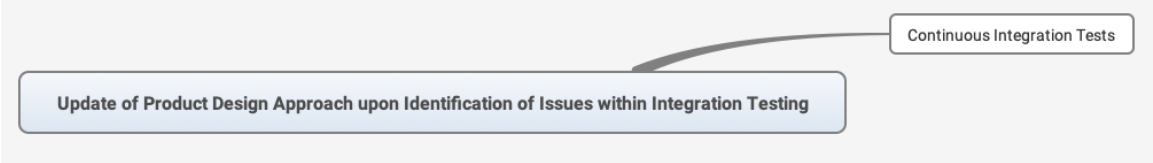
6.1.3. Peer Reviews

6.1.4. Documentation

6.1.5. Incorporating Security Requirements

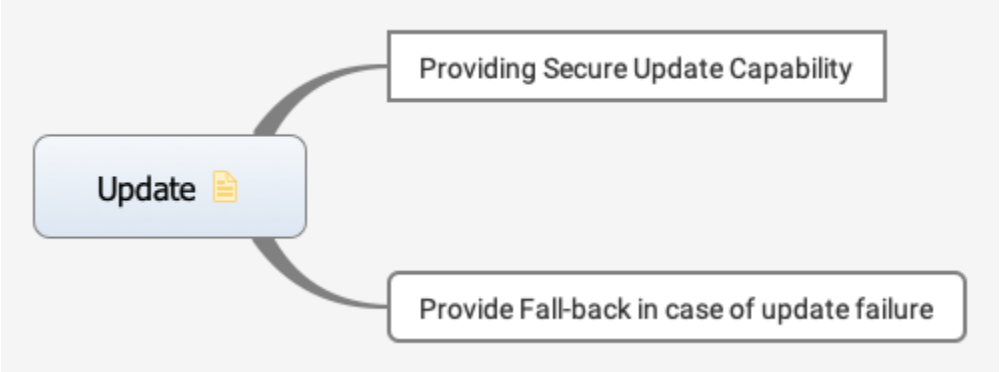
6.1.6. Feedback Loops

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



Continuous Integration Tests

6.2. Update



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

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:

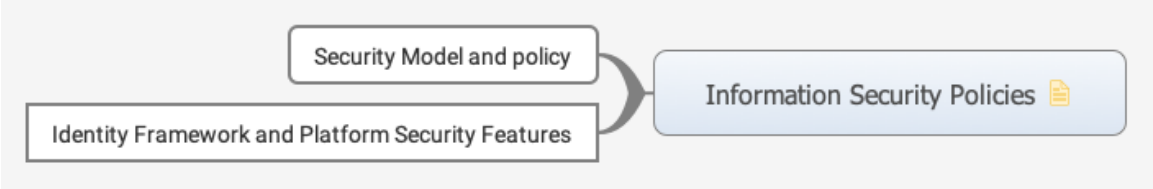
https://www.owasp.org/index.php/IoT_Security_Guidance

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



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

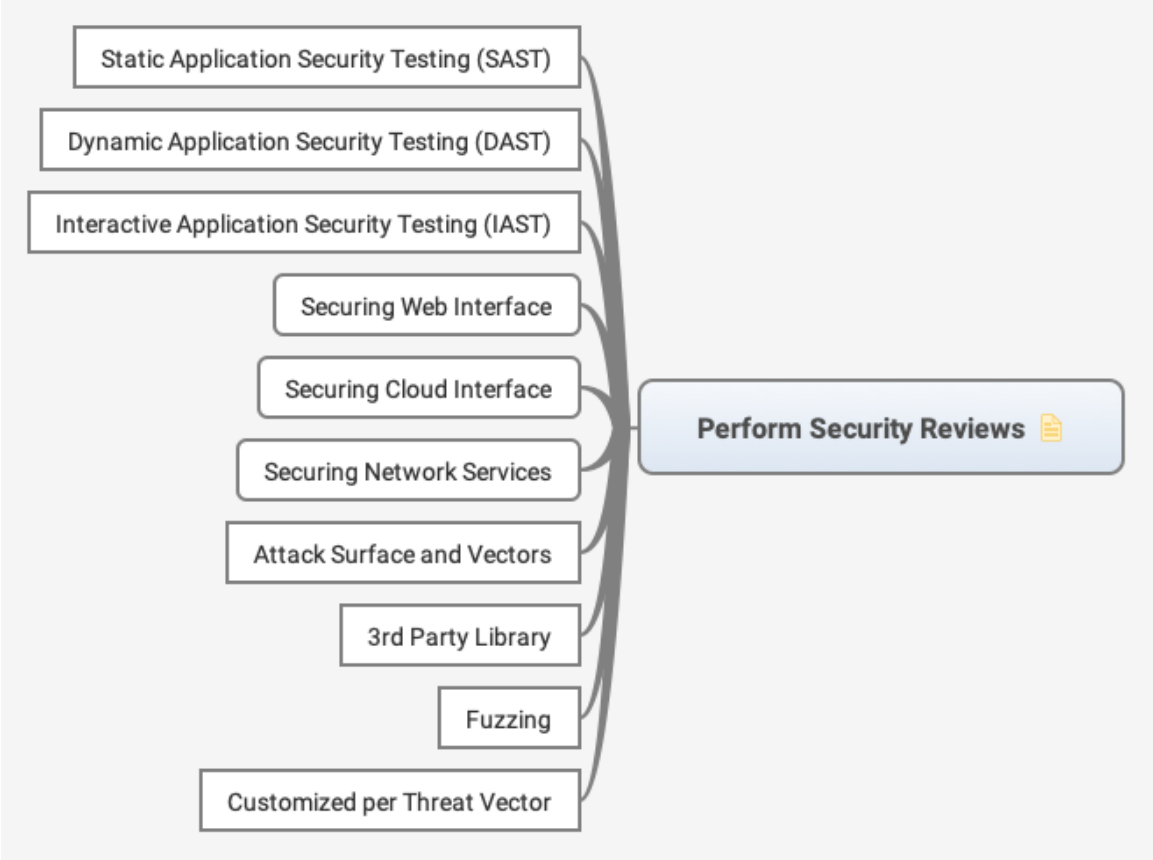
6.5.1. Security Model and policy

6.5.1.1. Data Protection

Security Considerations for Selecting IoT Communication Protocols

6.5.2. Identity Framework and Platform Security Features

6.6. 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

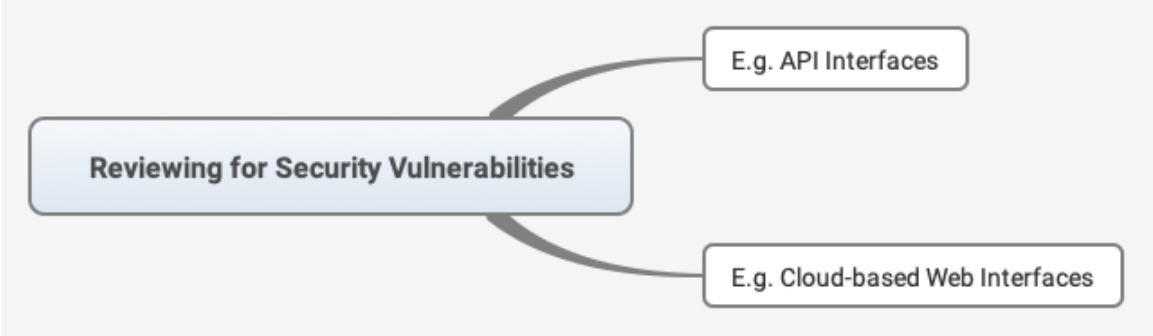
XSS

SQLi

CSRF

6.6.5. Securing Cloud Interface

6.6.5.1. Reviewing for Security Vulnerabilities



E.g. API Interfaces

E.g. Cloud-based Web Interfaces

6.6.5.2. Testing any Cloud-based Web Interface for Vulnerabilities

XSS

SQLi

CSRF

6.6.6. Securing Network Services

6.6.6.1. Review all Required Network Services for Vulnerabilities

6.6.7. Attack Surface and Vectors

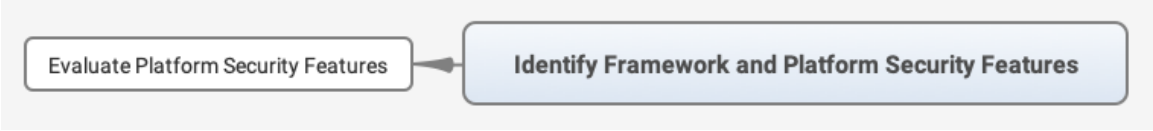
6.6.8. 3rd Party Library

6.6.9. Fuzzing

6.6.10. Customized per Threat Vector

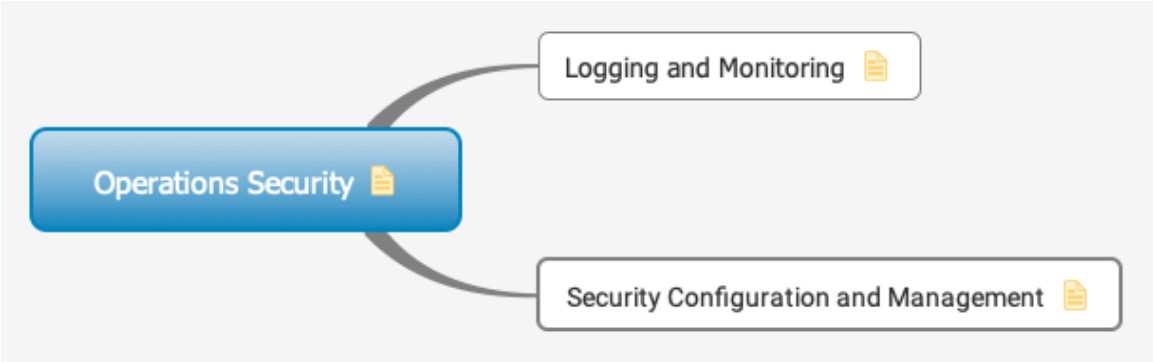
6.7. Secure Associated Applications and Services

6.8. Identify Framework and Platform Security Features



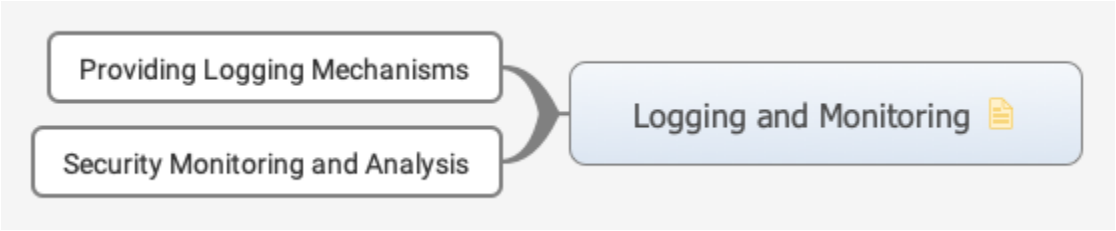
6.8.1. Evaluate Platform Security Features

7. Operations Security



According to ISO27001

7.1. Logging and Monitoring



References:

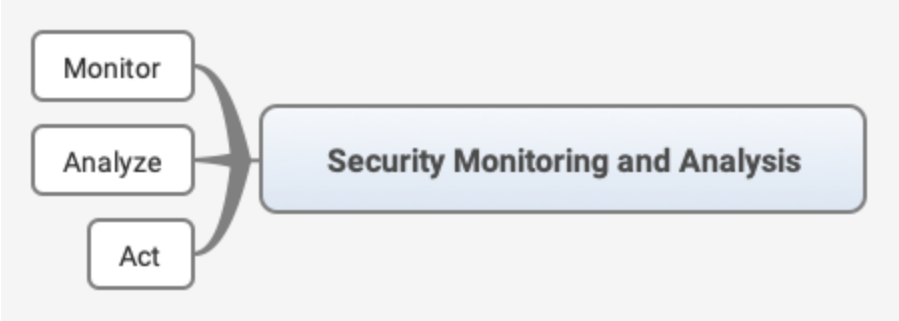
https://www.owasp.org/index.php/IoT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

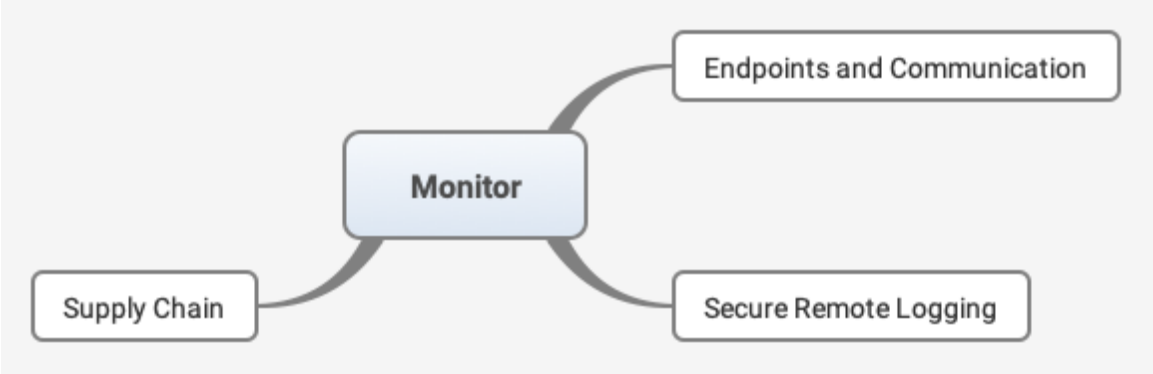
Future-proofing the Connected World - Cloud Security Alliance, 2016

7.1.1. Providing Logging Mechanisms

7.1.2. Security Monitoring and Analysis



7.1.2.1. Monitor

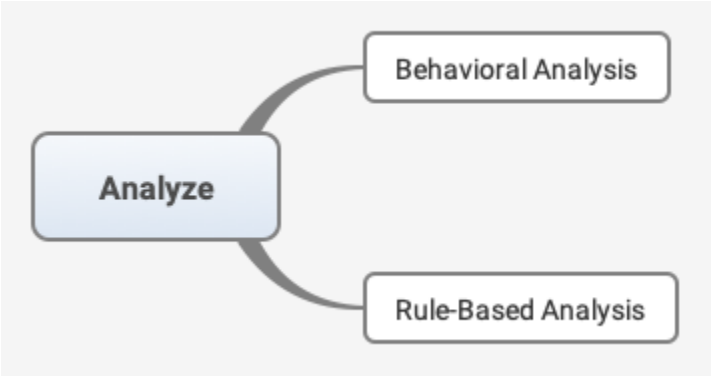


Endpoints and Communication

Secure Remote Logging

Supply Chain

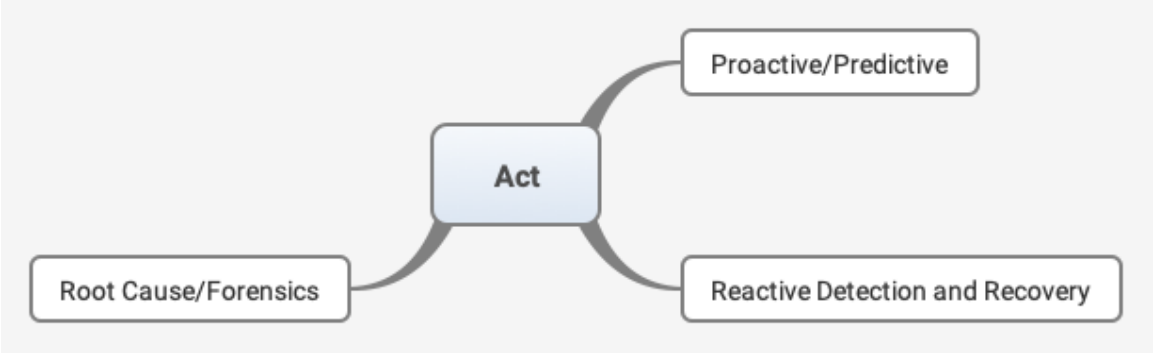
7.1.2.2. Analyze



Behavioral Analysis

Rule-Based Analysis

7.1.2.3. Act

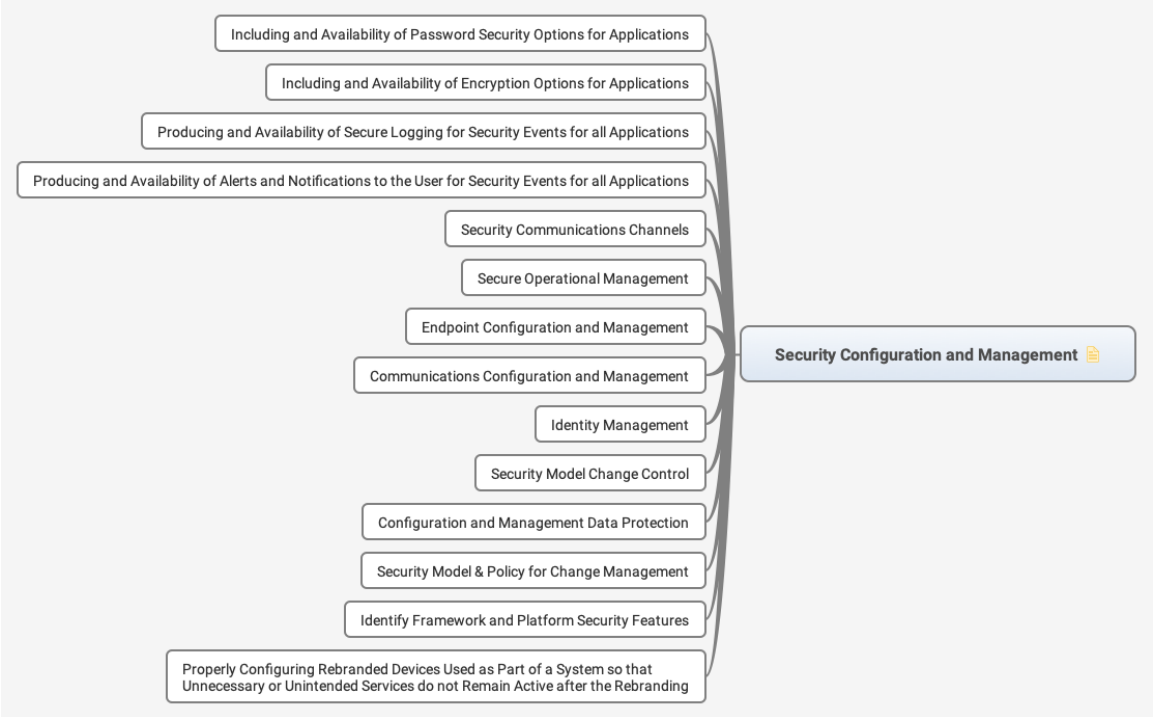


Proactive/Predictive

Reactive Detection and Recovery

Root Cause/Forensics

7.2. Security Configuration and Management



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

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

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

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