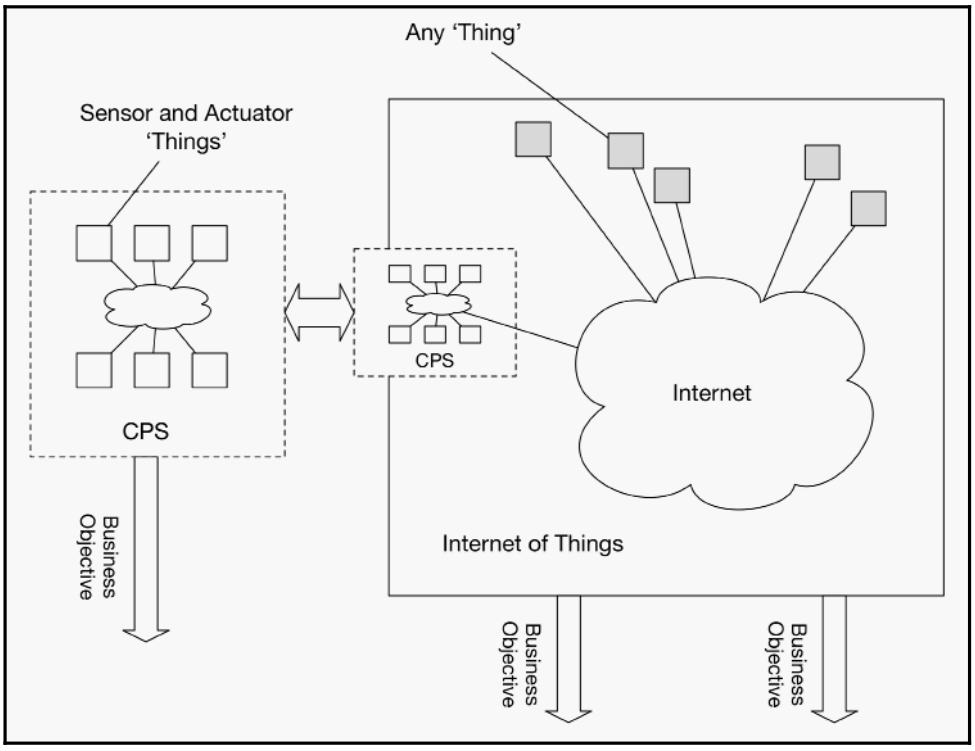
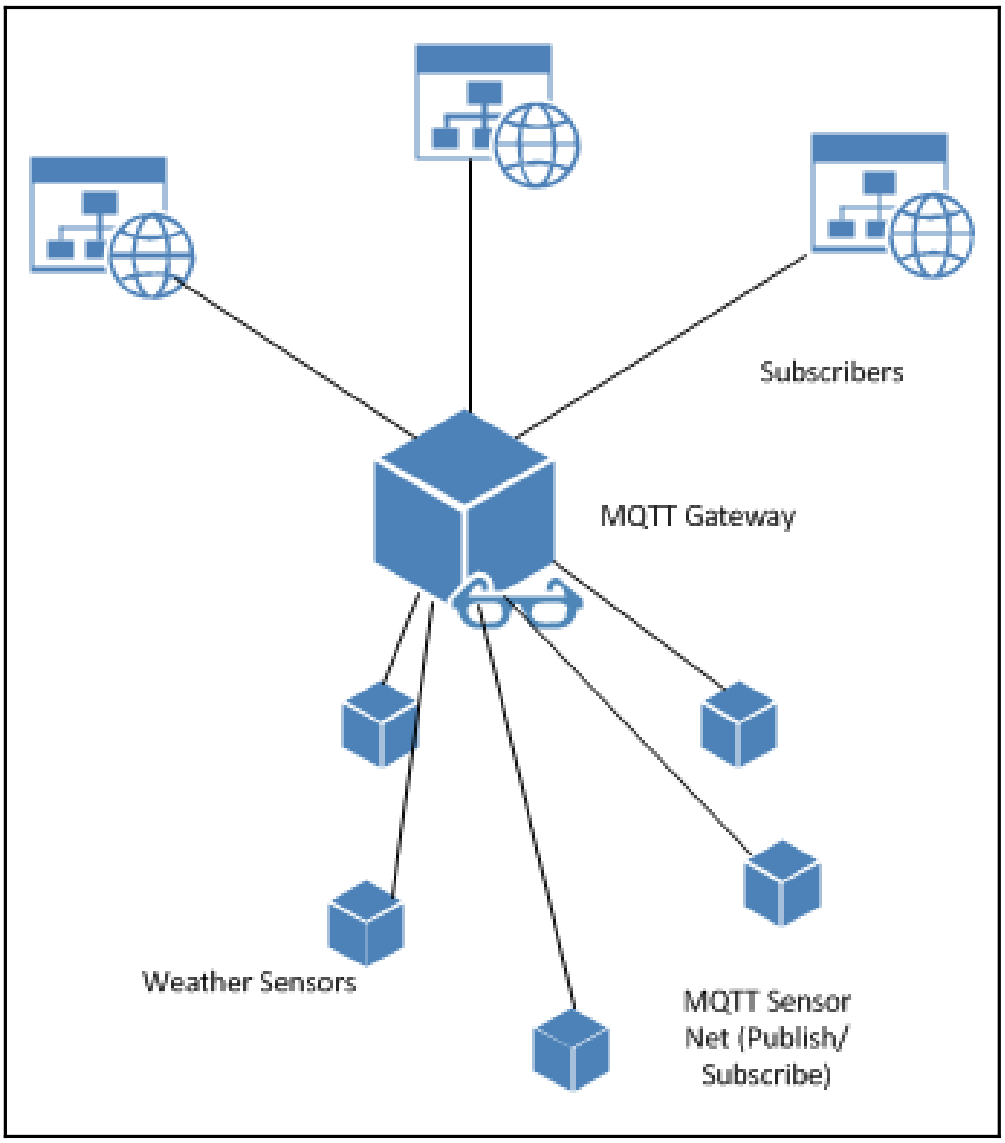
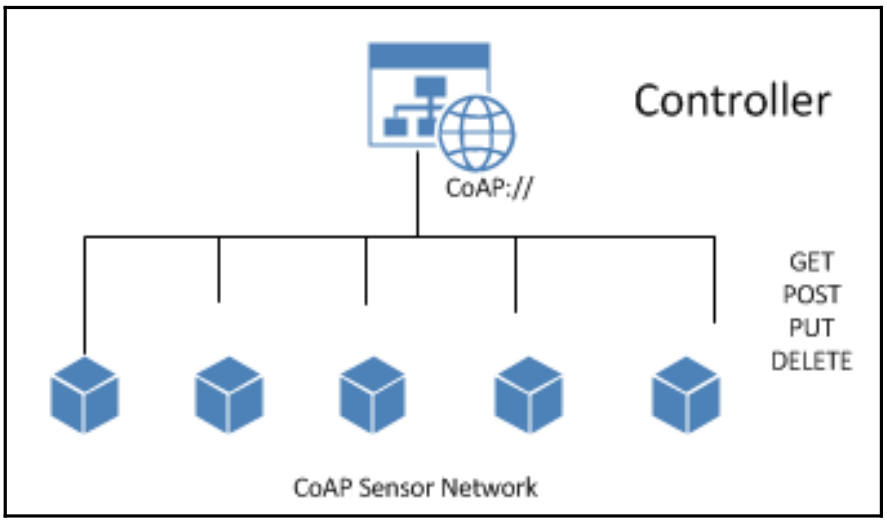
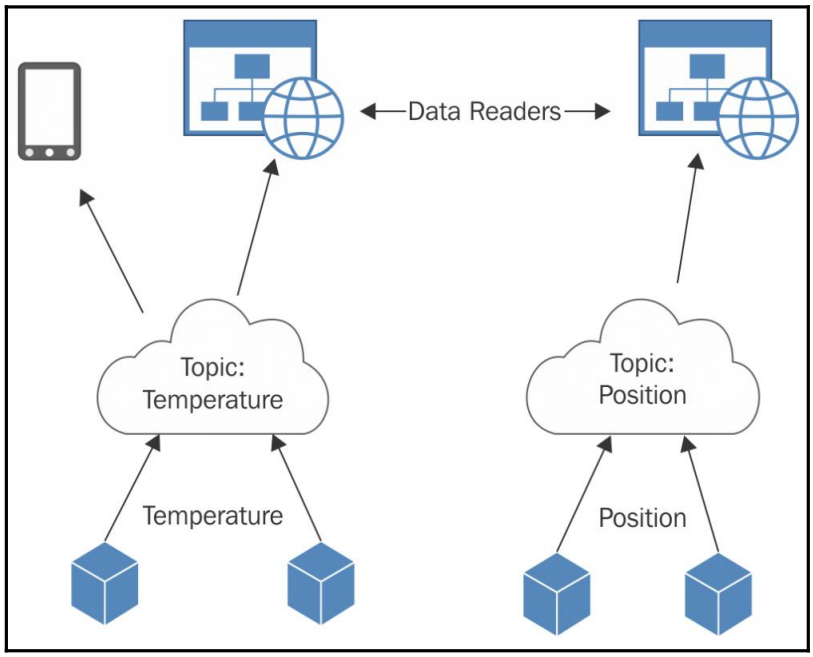
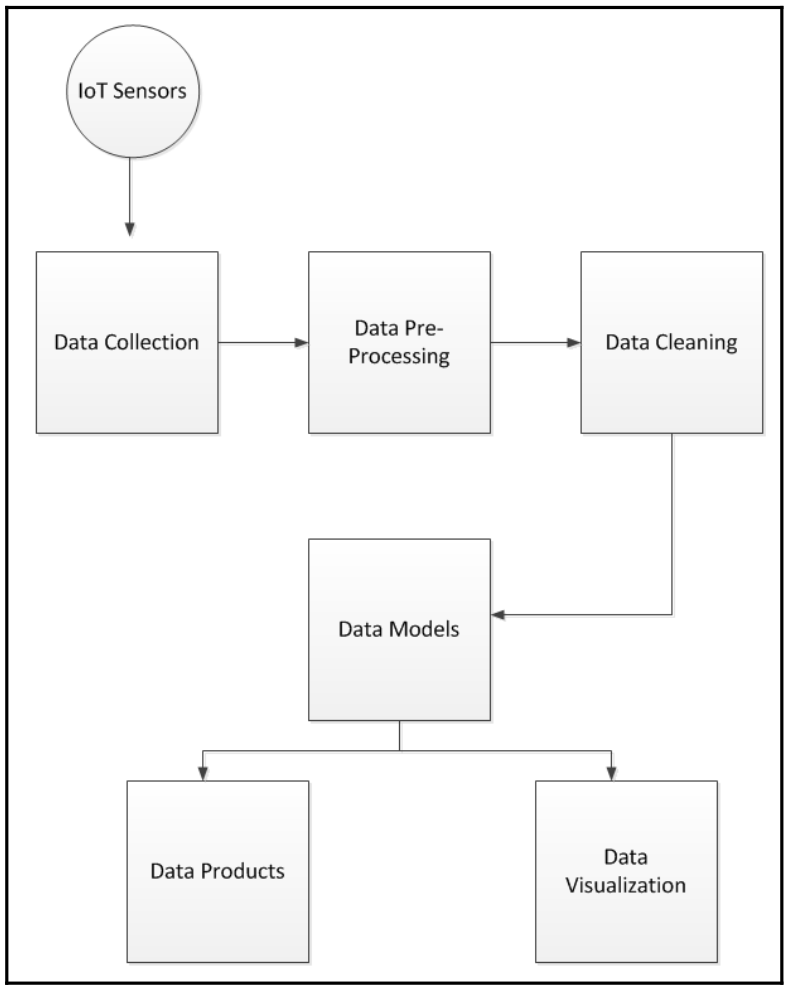
Chapter 1: A Brave New World

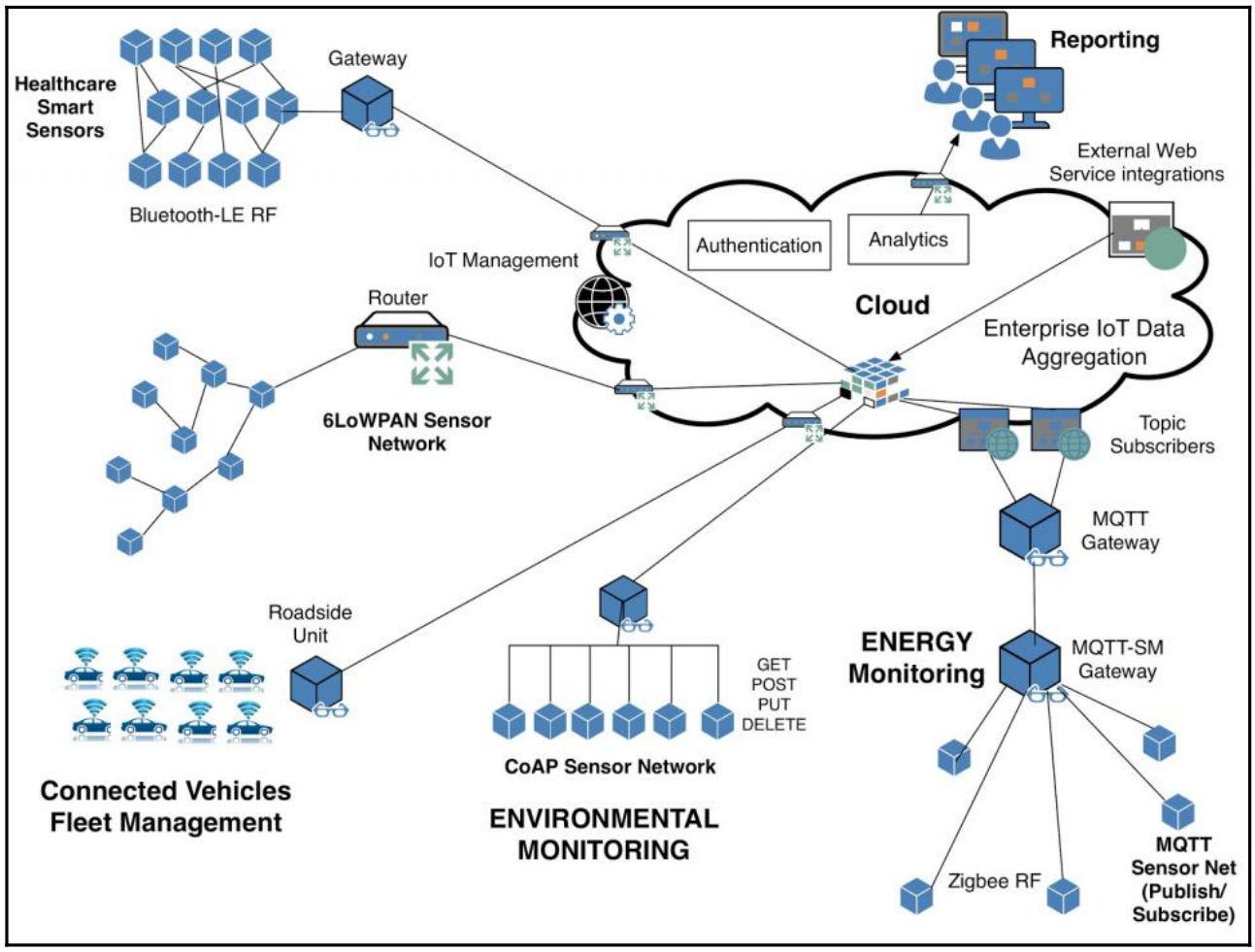



Subscribers
MQTT Gateway
Weather Sensors
MQTT Sensor Net (Publish/ Subscribe)

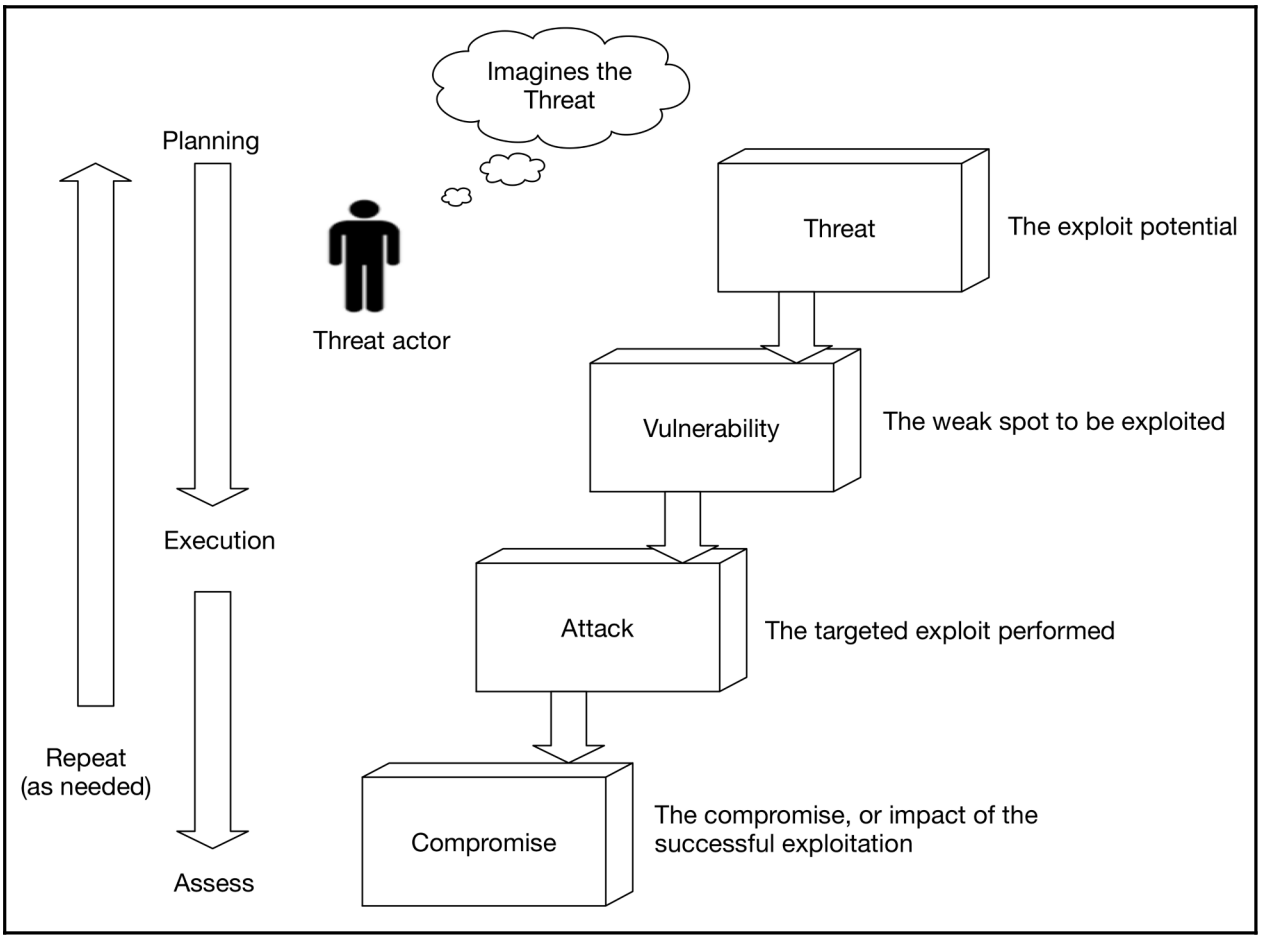

Controller
CoAP://
GET
POST
PUT
DELETE
CoAP Sensor Network

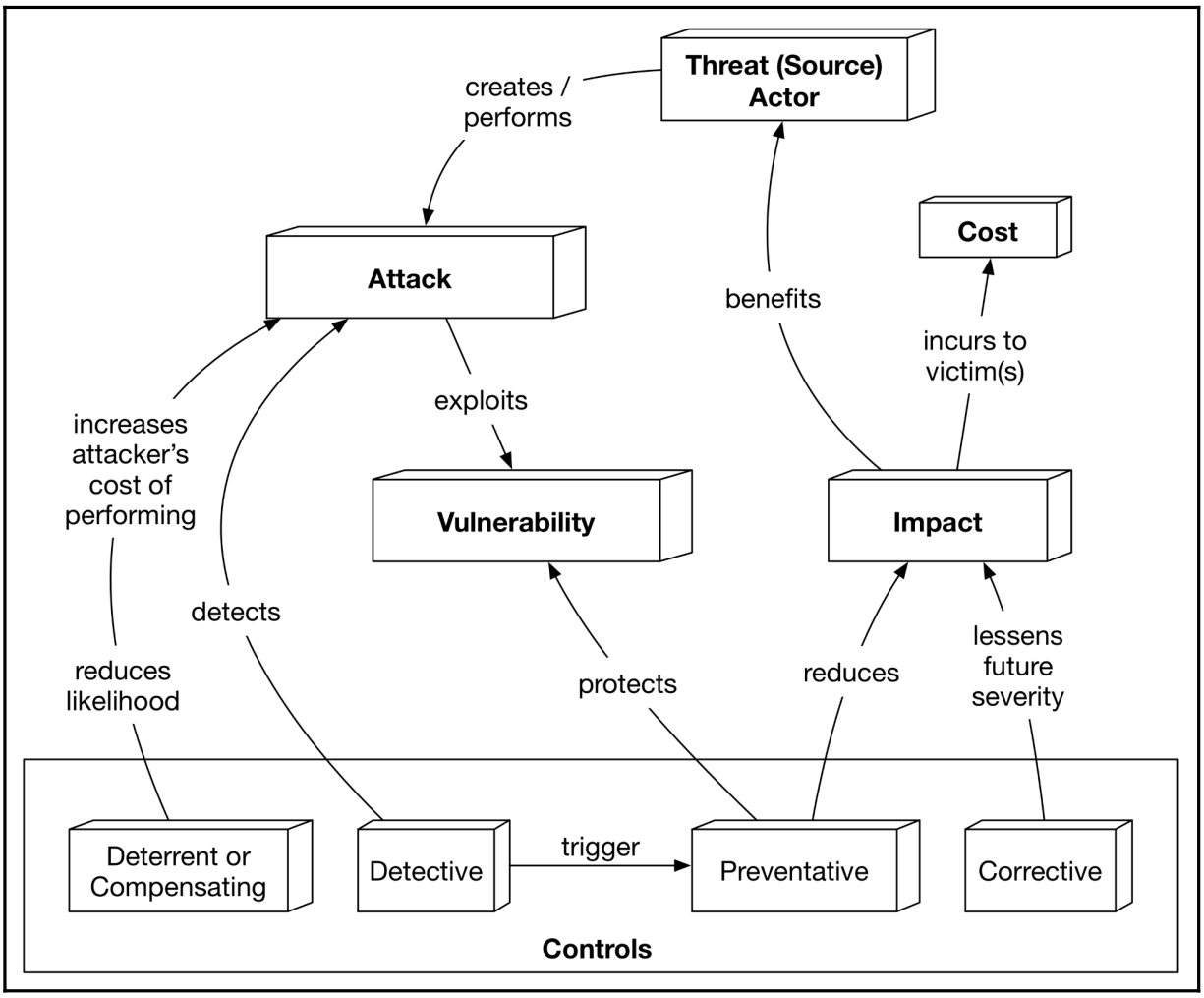

Data Readers
Topic:
Temperature
Topic:
Position
Temperature
Position

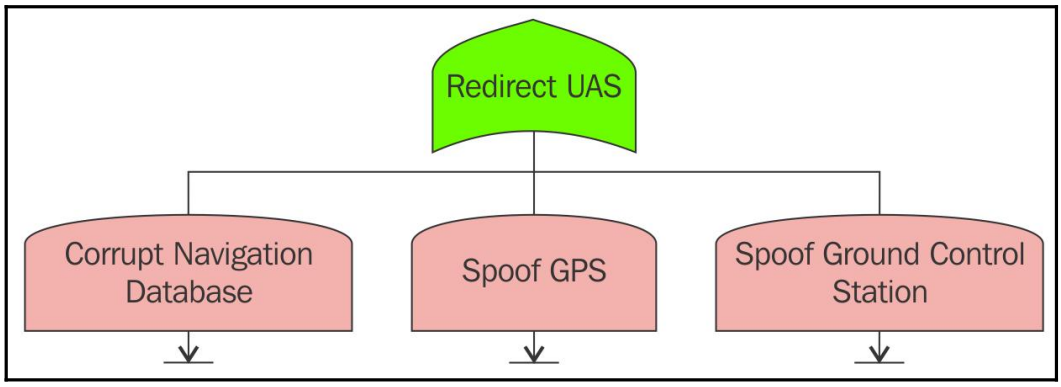

IoT Sensors
Data Collection
Data Pre-Processing
Data Cleaning
Data Models
Data Products
Data Visualization

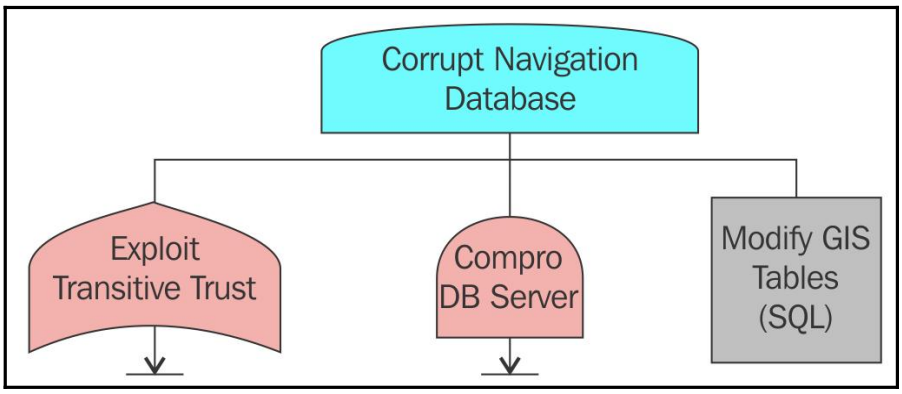

Healthcare Smart Sensors
Bluetooth-LE RF
Gateway
Reporting
External Web Service integrations
Authentication
Analytics
IoT Management
Cloud
Enterprise IoT Data Aggregation
Router
6LoWPAN Sensor Network
Topic Subscribers
MQTT Gateway
Roadside Unit
GET
POST
PUT
DELETE
CoAP Sensor Network
ENERGY Monitoring
MQTT-SM Gateway
Connected Vehicles Fleet Management
ENVIRONMENTAL MONITORING
Zigbee RF
MQTT Sensor Net (Publish/ Subscribe)

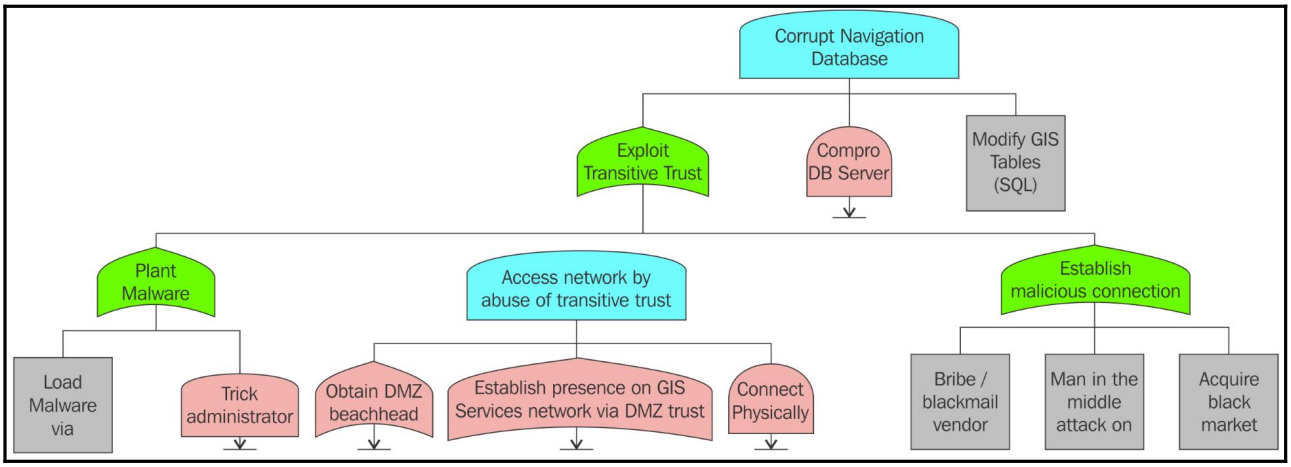
Chapter 2: Vulnerabilities, Attacks, and Countermeasures

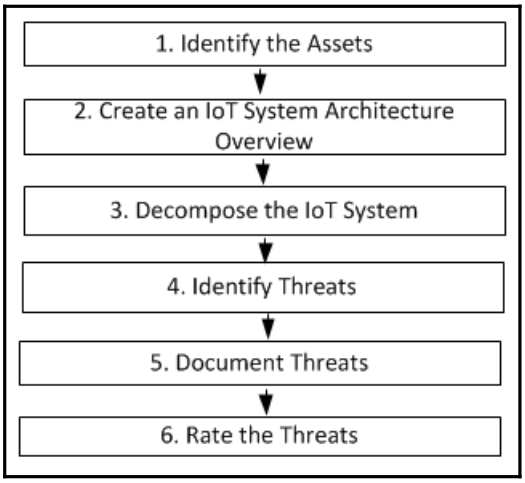


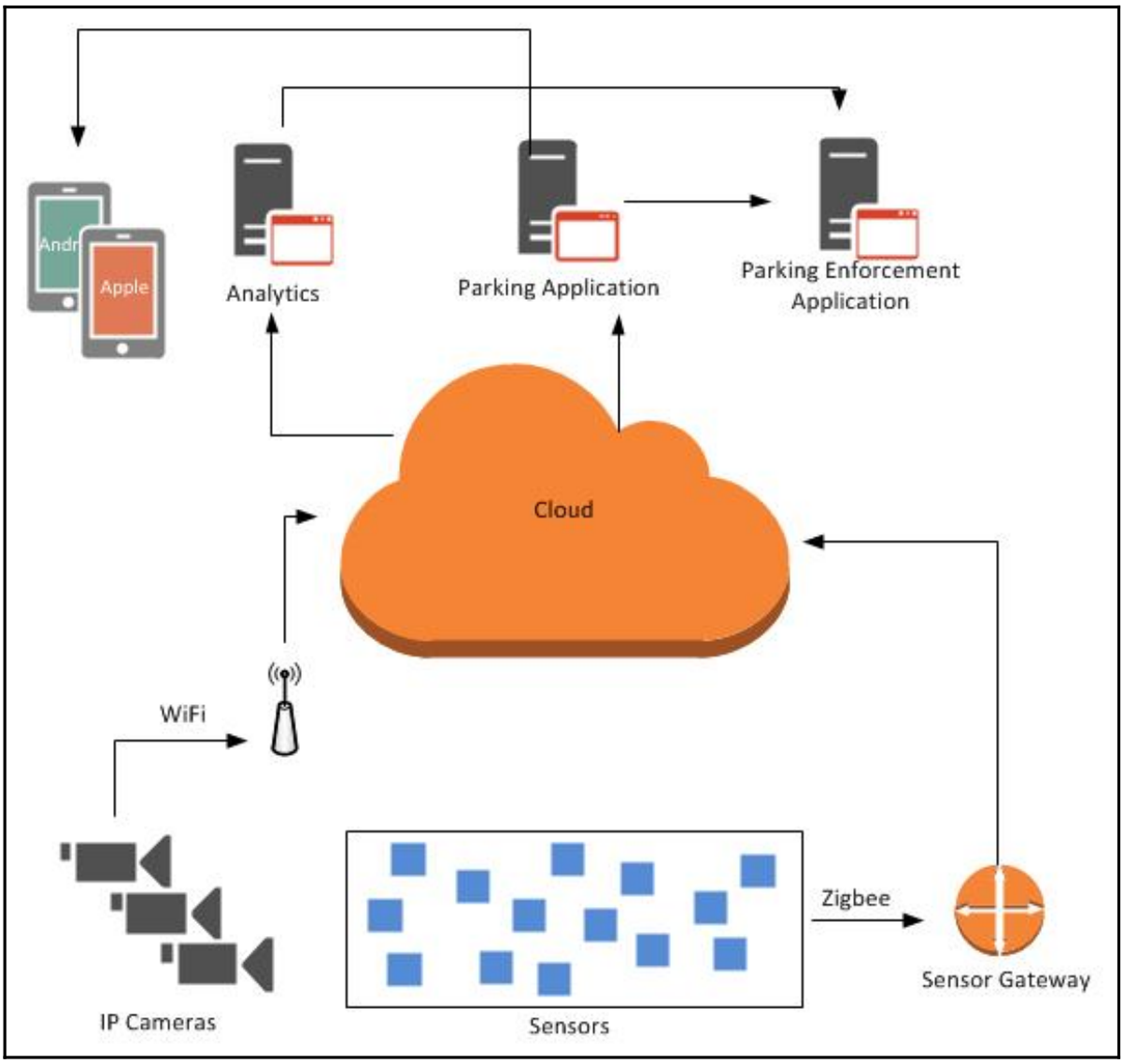

Threat (Source) Actor
creates / performs
Attack
Cost
benefits
incurs to victim(s)
exploits
increases attacker's cost of performing
Vulnerability
Impact
detects
reduces likelihood
protects
reduces
lessens future severity
Deterrent or Compensating
Detective
trigger
Preventative
Corrective
Controls

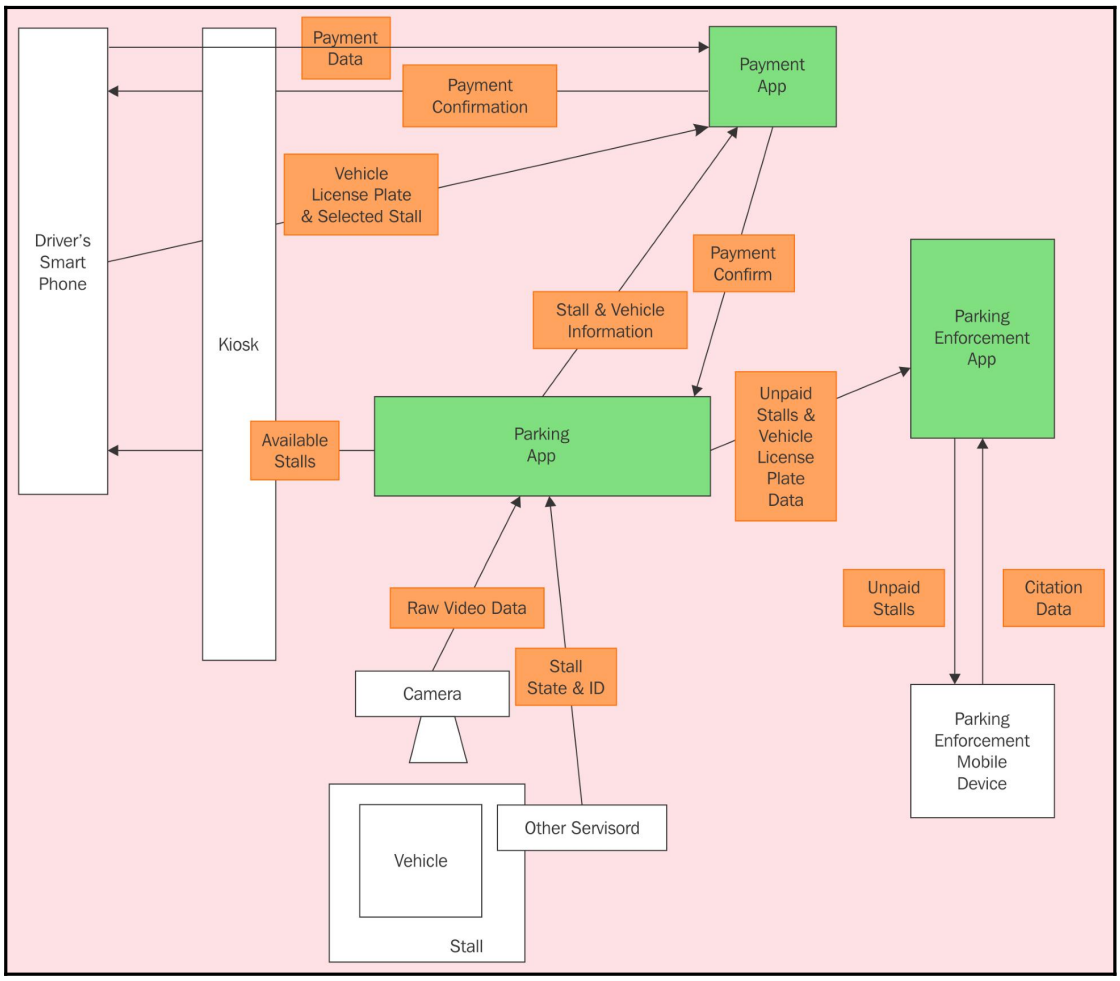

Redirect UAS
Corrupt Navigation Database
Spoof GPS
Spoof Ground Control Station


Corrupt Navigation Database
Exploit Transitive Trust
Compro DB Server
Modify GIS Tables (SQL)

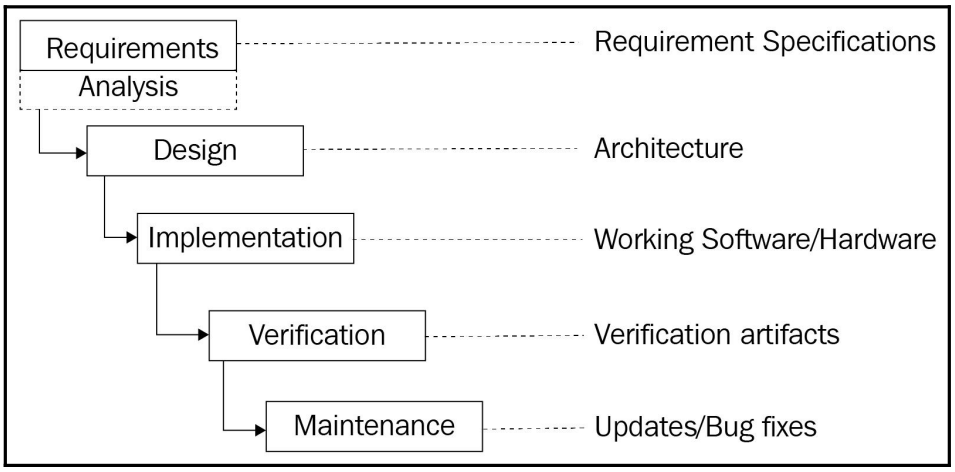

Corrupt Navigation Database
Exploit Transitive Trust
Compro DB Server
Modify GIS Tables (SQL)
Plant Malware
Access network by abuse of transitive trust
Establish malicious connection
Load Malware via
Trick administrator
Obtain DMZ beachhead
Establish presence on GIS Services network via DMZ trust
Connect Physically
Bribe / blackmail vendor
Man in the middle attack on
Acquire black market

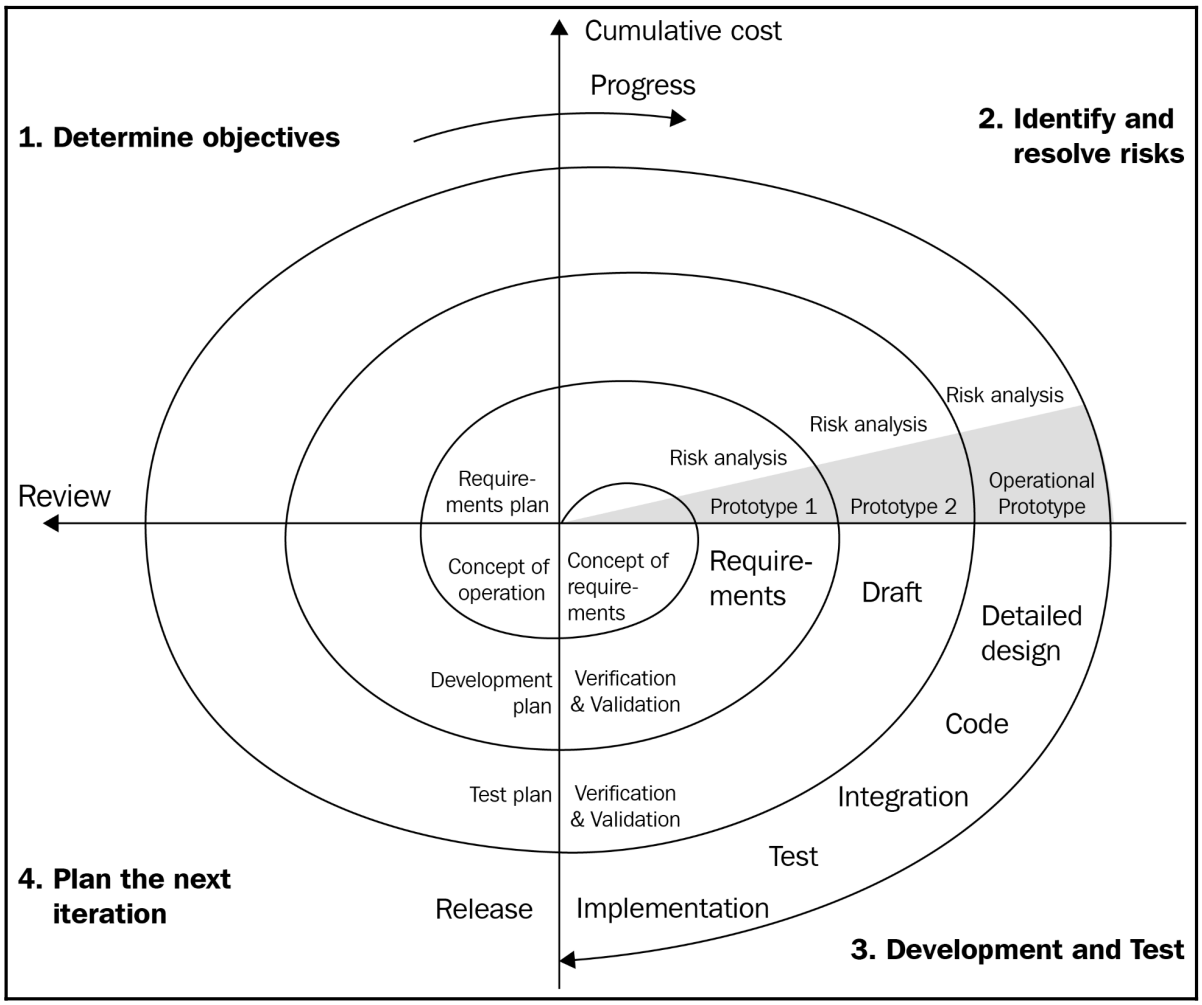

1. Identify the Assets
2. Create an IoT System Architecture Overview
3. Decompose the IoT System
4. Identify Threats
5. Document Threats
6. Rate the Threats

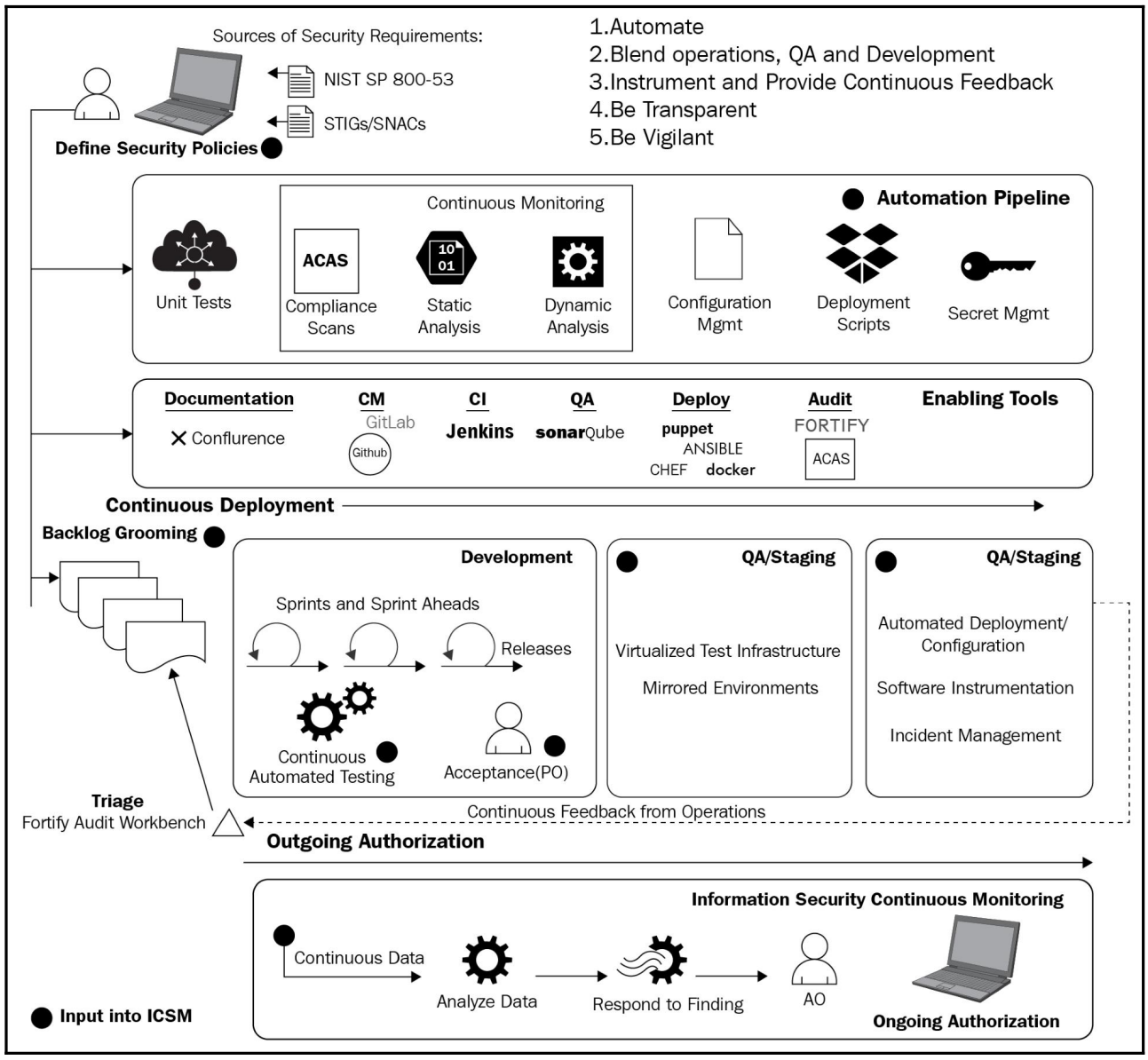

Andr
Apple
Analytics
Parking Application
Parking Enforcement Application
Cloud
WiFi
IP Cameras
Sensors
Zigbee
Sensor Gateway

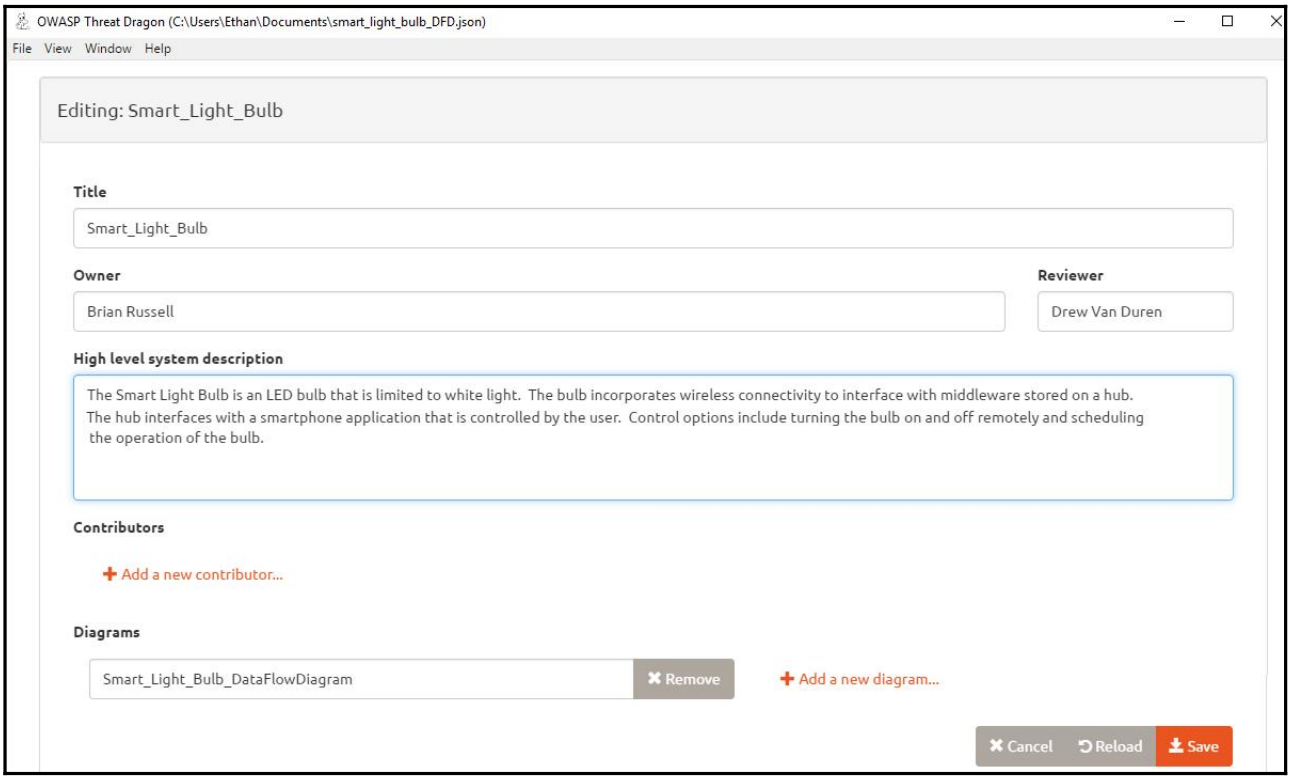

Payment Data
Payment App
Payment Confirmation
Vehicle License Plate & Selected Stall
Driver's Smart Phone
Kiosk
Payment Confirm
Stall & Vehicle Information
Parking Enforcement App
Unpaid Stalls & Vehicle License Plate Data
Available Stalls
Parking App
Unpaid Stalls
Citation Data
Raw Video Data
Stall State & ID
Camera
Parking Enforcement Mobile Device
Other Servisord
Vehicle
Stall

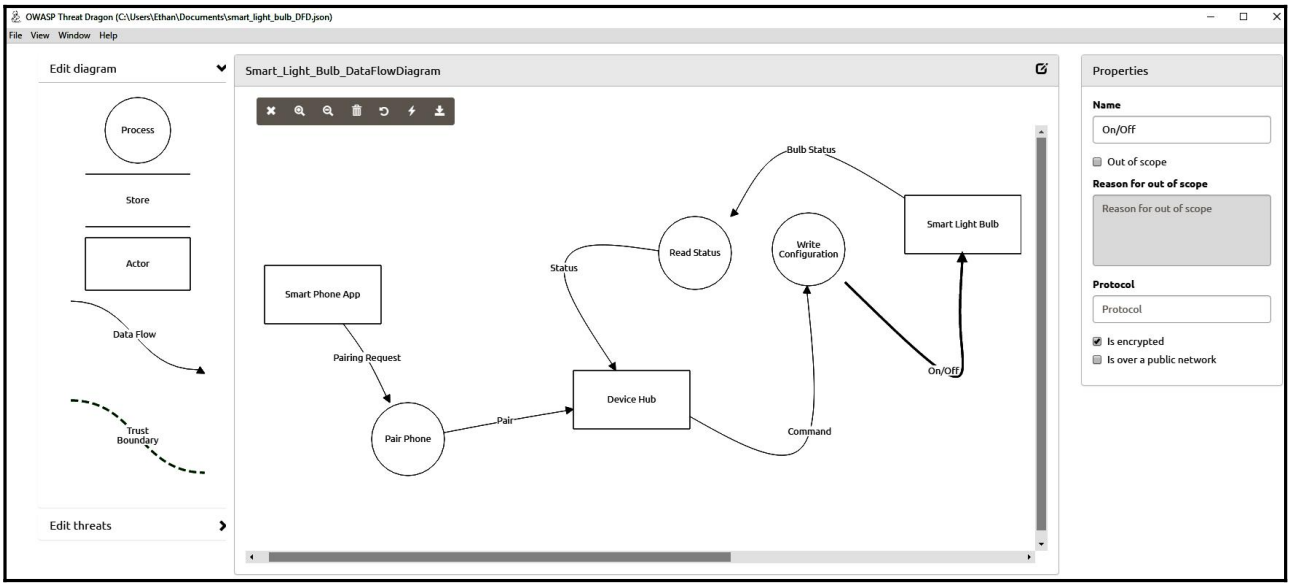
Chapter 3: Secure Development Approach

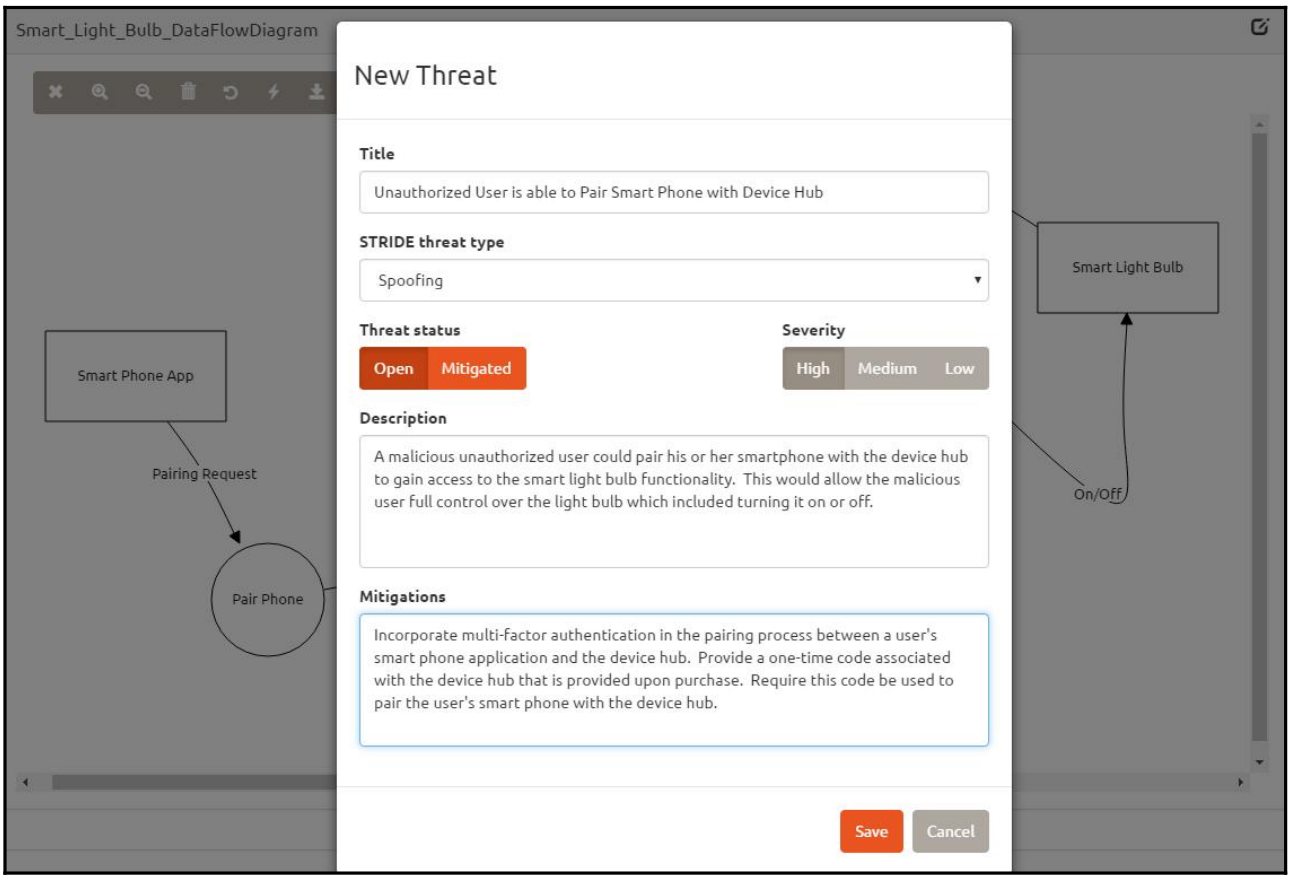



Cumulative cost
Progress
1. Determine objectives
2. Identify and resolve risks
Review
Require-ments plan
Risk analysis
Risk analysis
Risk analysis
Prototype 1
Prototype 2
Operational Prototype
Concept of operation
Concept of require-ments
Require-ments
Draft
Detailed design
Development plan
Verification & Validation
Code
Test plan
Verification & Validation
Integration
Test
4. Plan the next iteration
Release
Implementation
3. Development and Test

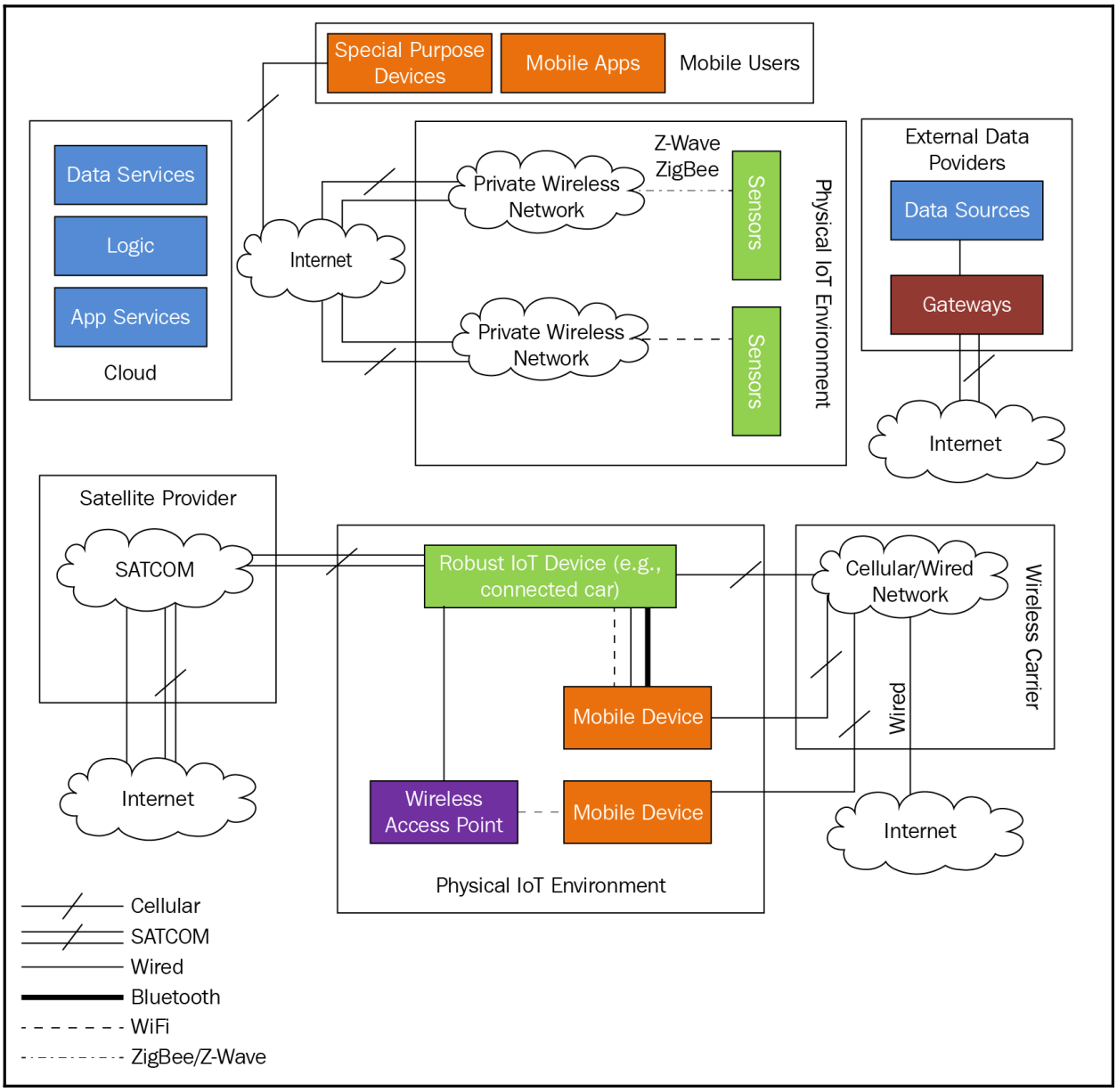

Sources of Security Requirements:
NIST SP 800-53
STIGs/SNACs
Define Security Policies
1.Automate
2.Blend operations, QA and Development
3.Instrument and Provide Continuous Feedback
4.Be Transparent
5.Be Vigilant
Automation Pipeline
Unit Tests
Continuous Monitoring
ACAS
Compliance Scans
Static Analysis
Dynamic Analysis
Configuration Mgmt
Deployment Scripts
Secret Mgmt
Documentation
Confluence
CM
GitLab
Github
CI
Jenkins
QA
sonarQube
Deploy
puppet
ANSIBLE
CHEF
docker
Audit
FORTIFY
ACAS
Enabling Tools
Continuous Deployment
Backlog Grooming
Development
Sprints and Sprint Aheads
Releases
Continuous Automated Testing
Acceptance(PO)
QA/Staging
Virtualized Test Infrastructure
Mirrored Environments
QA/Staging
Automated Deployment/ Configuration
Software Instrumentation
Incident Management
Triage
Fortify Audit Workbench
Continuous Feedback from Operations
Outgoing Authorization
Information Security Continuous Monitoring
Continuous Data
Analyze Data
Respond to Finding
AO
Ongoing Authorization
Input into ICSM


OWASP Threat Dragon (C:\Users\Ethan\Documents\smart_light_bulb_DFD.json)
File View Window Help
Editing: Smart_Light_Bulb
Title
Smart_Light_Bulb
Owner
Brian Russell
Reviewer
Drew Van Duren
High level system description
The Smart Light Bulb is an LED bulb that is limited to white light. The bulb incorporates wireless connectivity to interface with middleware stored on a hub. The hub interfaces with a smartphone application that is controlled by the user. Control options include turning the bulb on and off remotely and scheduling the operation of the bulb.
Contributors
Add a new contributor...
Diagrams
Smart_Light_Bulb_DataFlowDiagram
Remove
Add a new diagram...
Cancel
Reload
Save

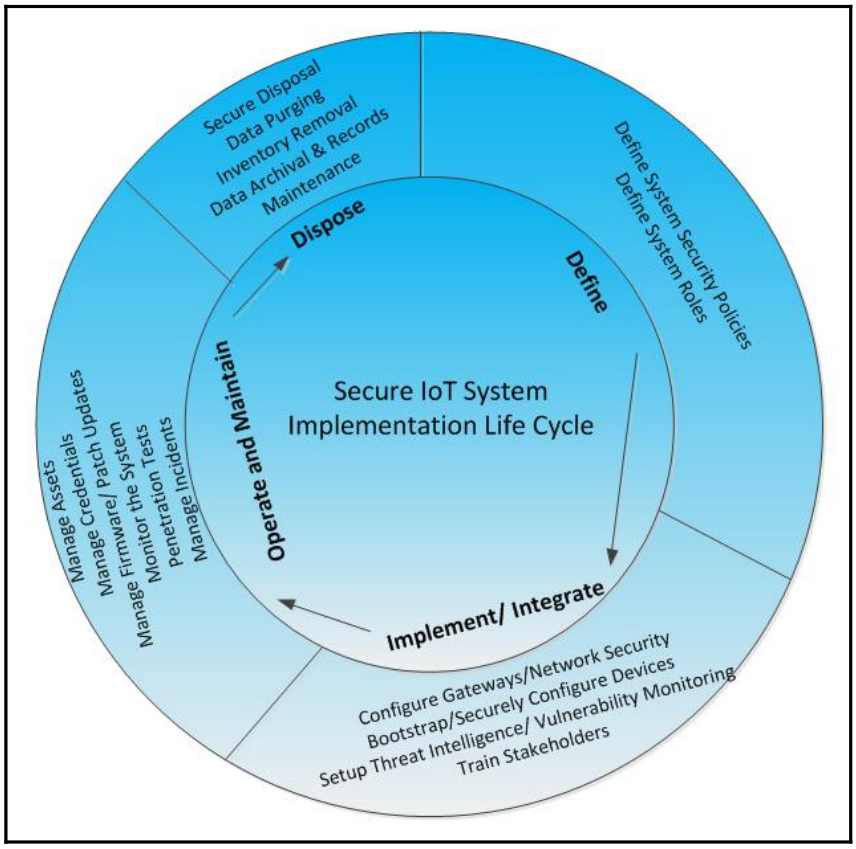

Edit diagram
Process
Store
Actor
Data Flow
Trust Boundary
Edit threats
Smart_Light_Bulb_DataFlowDiagram
Bulb Status
Smart Light Bulb
Read Status
Write Configuration
Status
Smart Phone App
Pairing Request
Device Hub
Pair
Pair Phone
Command
On/Off
Properties
Name
On/Off
Out of scope
Reason for out of scope
Reason for out of scope
Protocol
Protocol
Is encrypted
Is over a public network

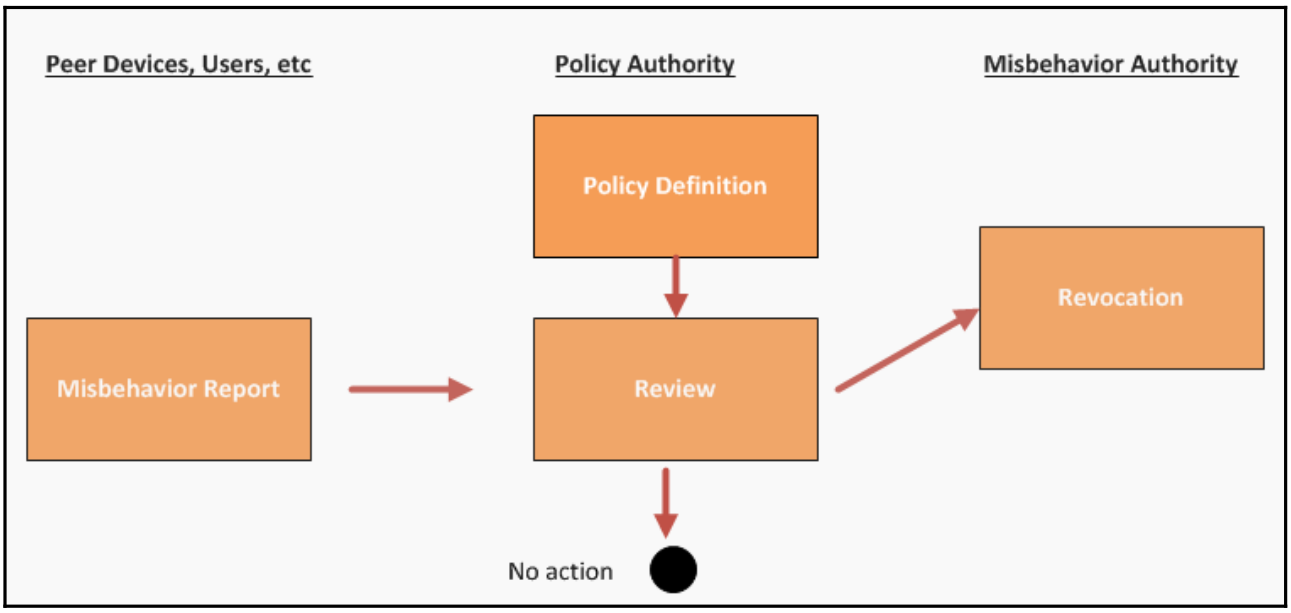

Smart_Light_Bulb_DataFlowDiagram
New Threat
Title
Unauthorized User is able to Pair Smart Phone with Device Hub
STRIDE threat type
Spoofing
Threat status
Open
Mitigated
Severity
High
Medium
Low
Description
A malicious unauthorized user could pair his or her smartphone with the device hub to gain access to the smart light bulb functionality. This would allow the malicious user full control over the light bulb which included turning it on or off.
Mitigations
Incorporate multi-factor authentication in the pairing process between a user's smart phone application and the device hub. Provide a one-time code associated with the device hub that is provided upon purchase. Require this code be used to pair the user's smart phone with the device hub.
Save
Cancel
Smart Phone App
Pairing Request
Pair Phone
Smart Light Bulb
On/Off

Chapter 4: Secure Design of IoT Devices

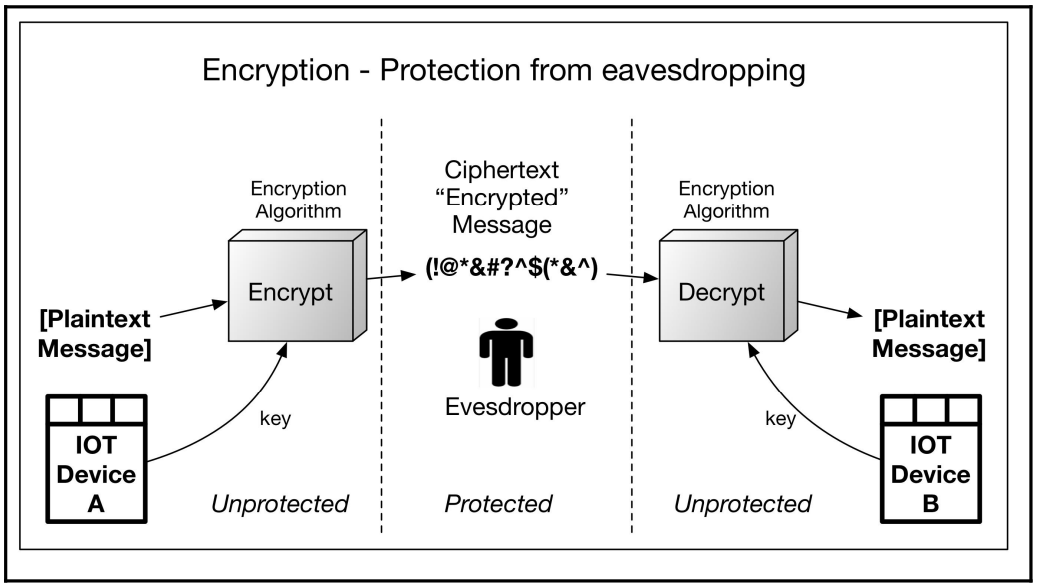


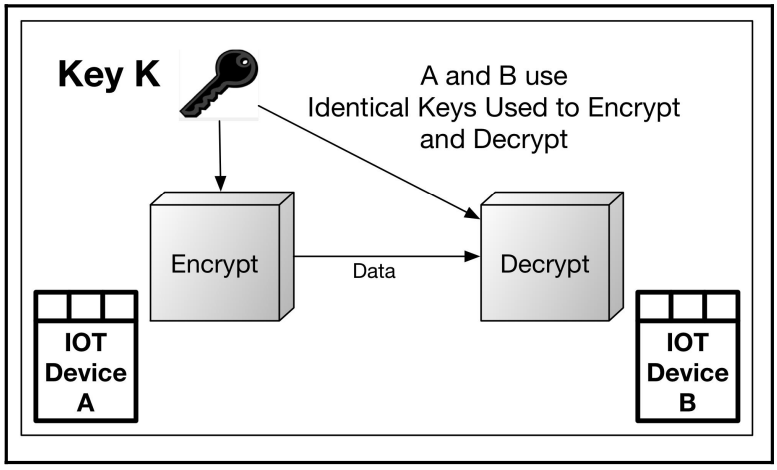
Chapter 5: Operational Security Lifecycle

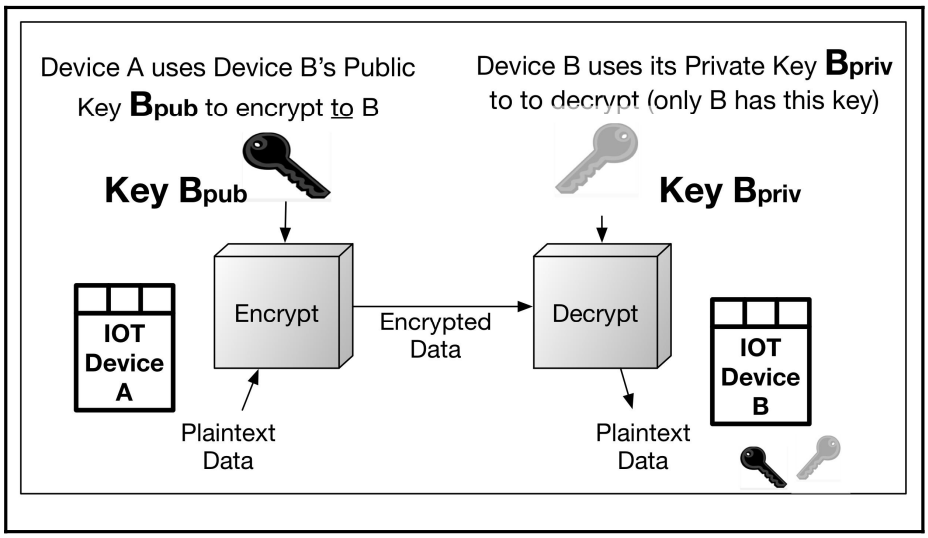


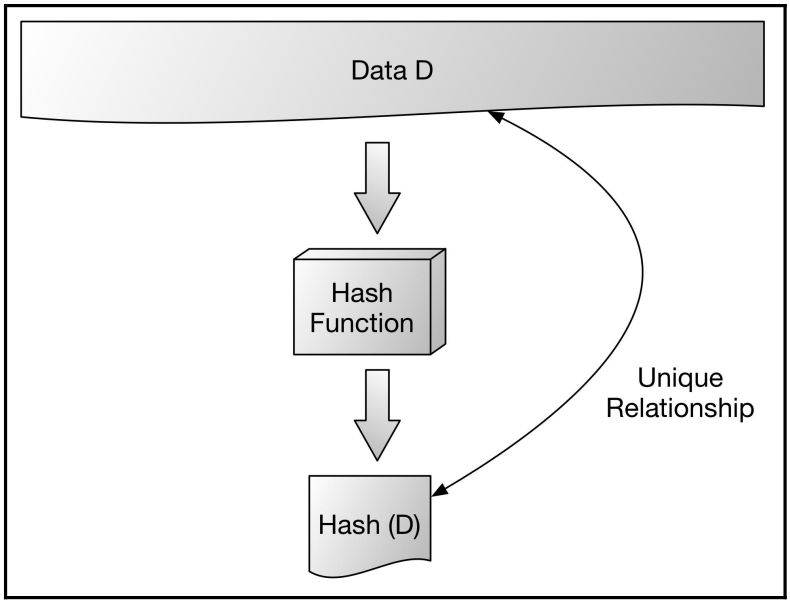

Peer Devices, Users, etc
Policy Authority
Misbehavior Authority
Policy Definition
Revocation
Misbehavior Report
Review
No action

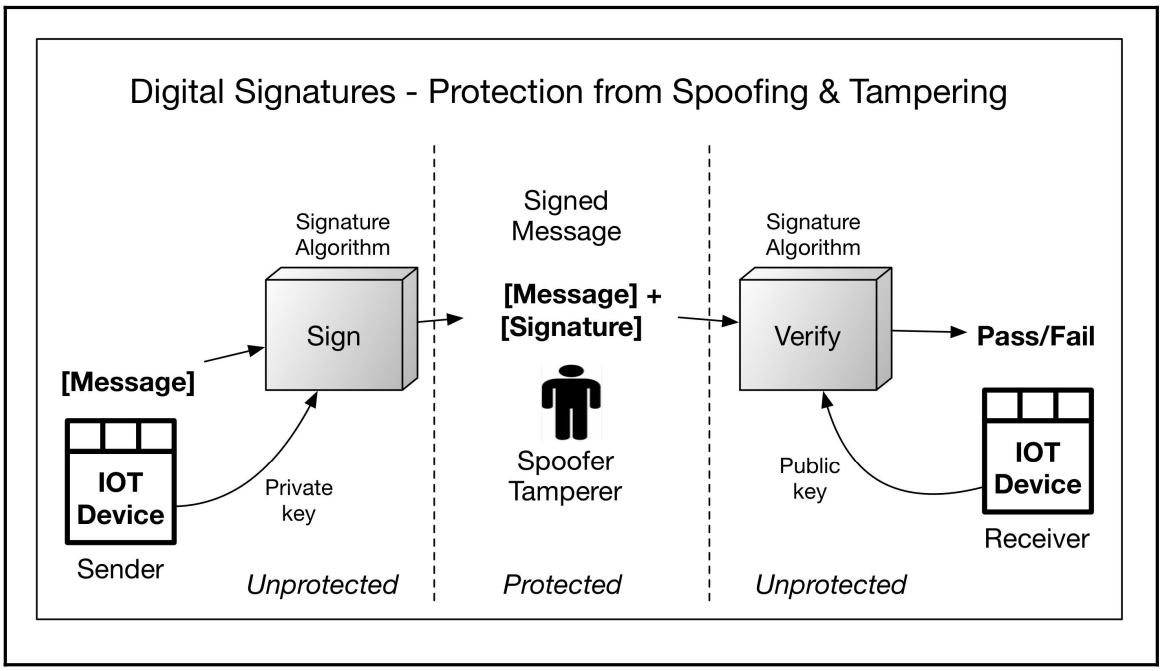
Chapter 6: Cryptographic Fundamentals for IoT Security Engineering

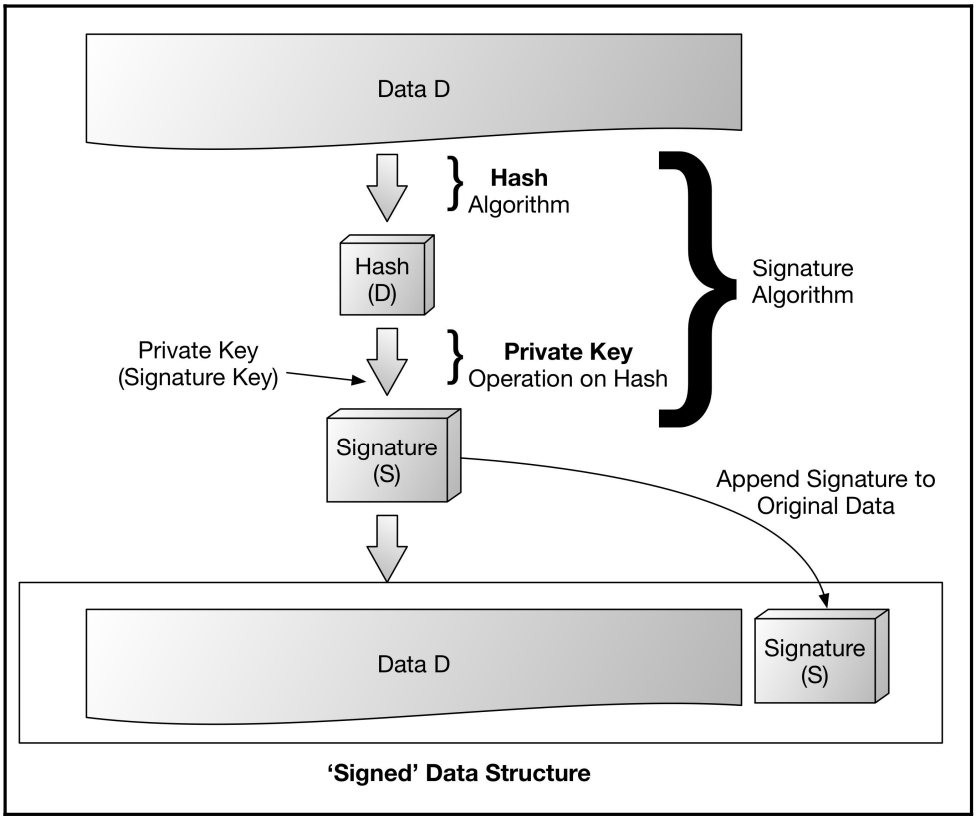


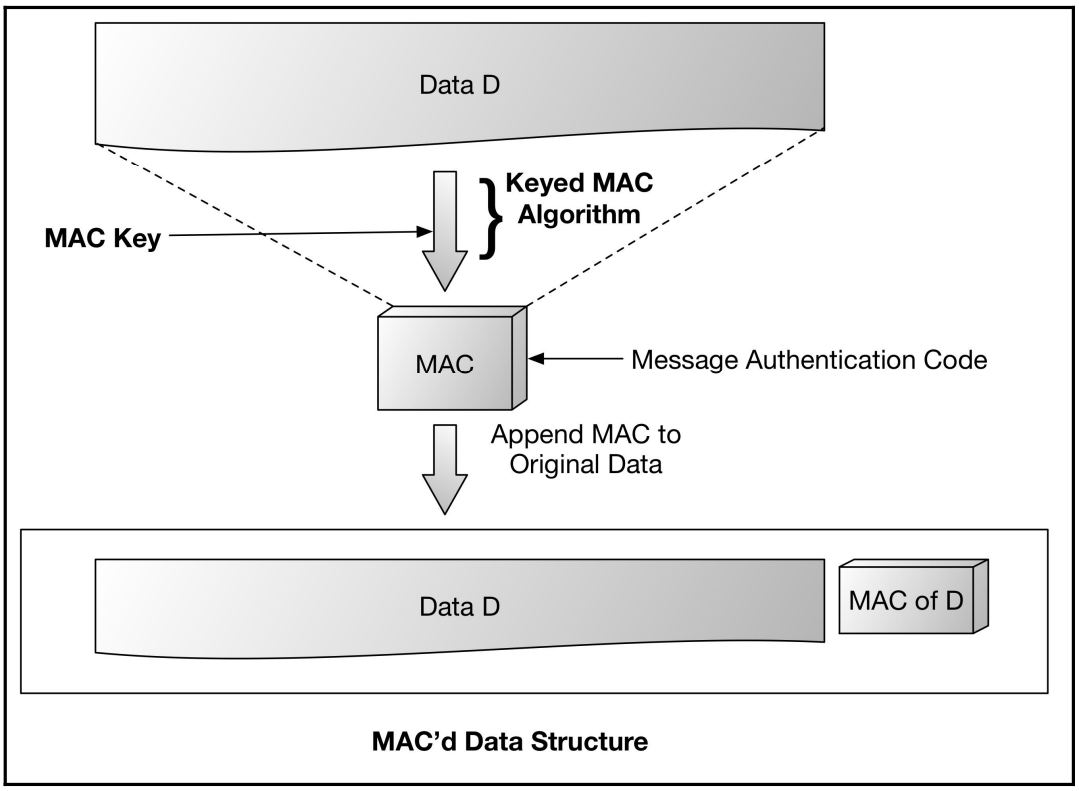


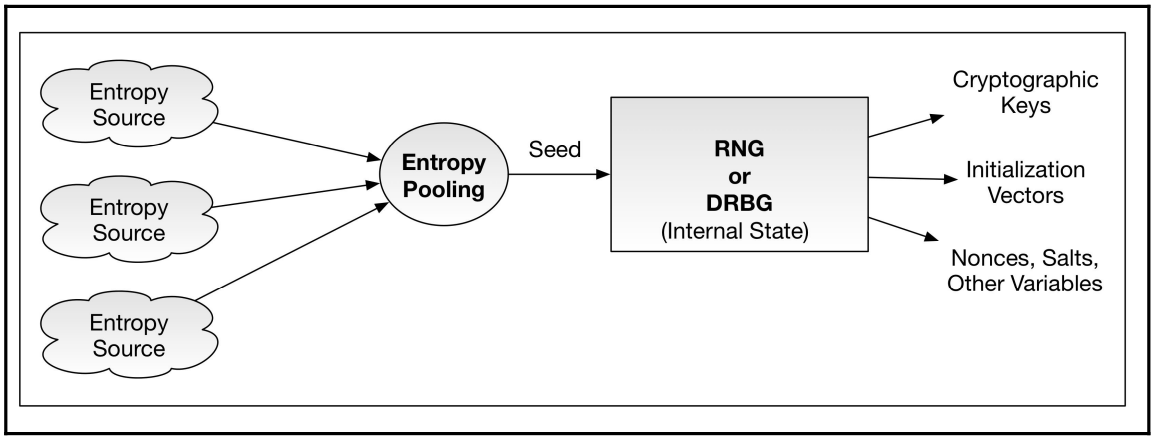

Device A uses Device B's Public Key Bpub to encrypt to B
Device B uses its Private Key Bpriv to to decrypt (only B has this key)
Key Bpub
Key Bpriv
IOT Device A
Encrypt
Encrypted Data
Decrypt
IOT Device B
Plaintext Data
Plaintext Data

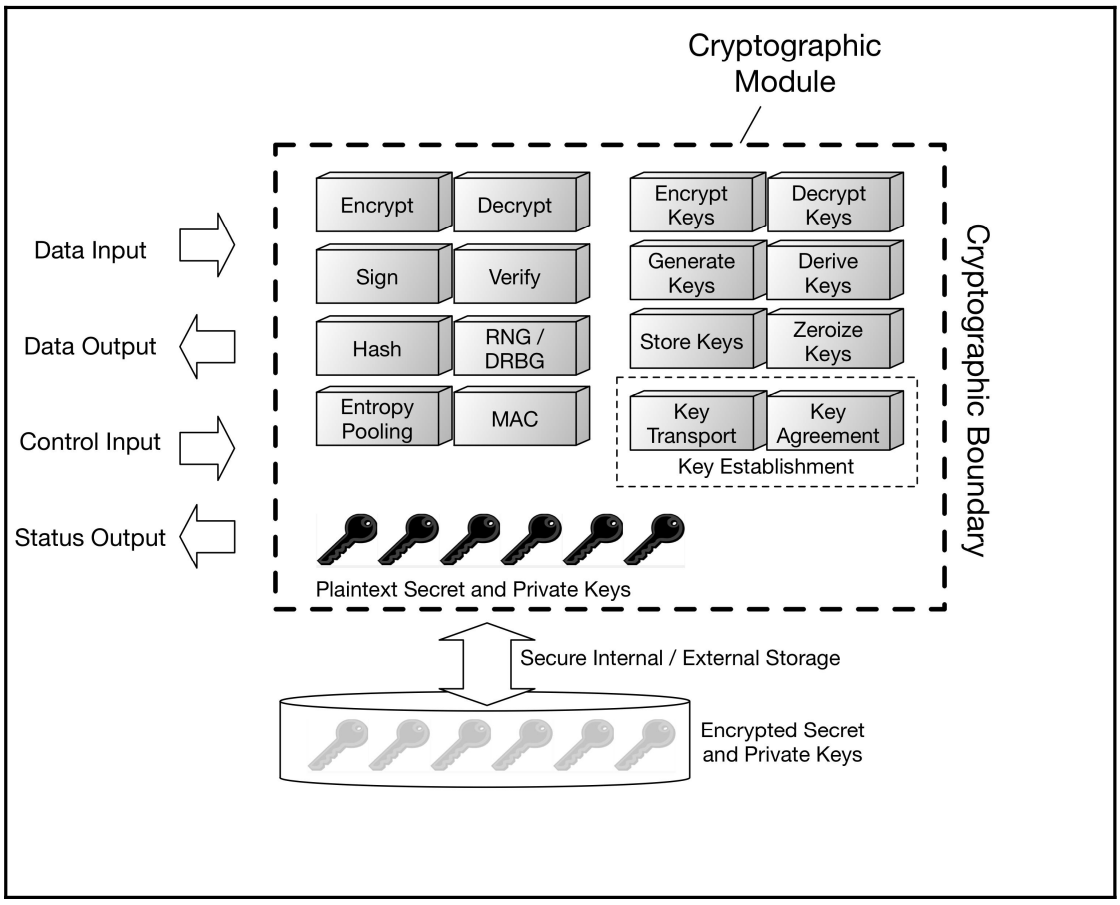

Data D
Hash Function
Unique Relationship
Hash (D)

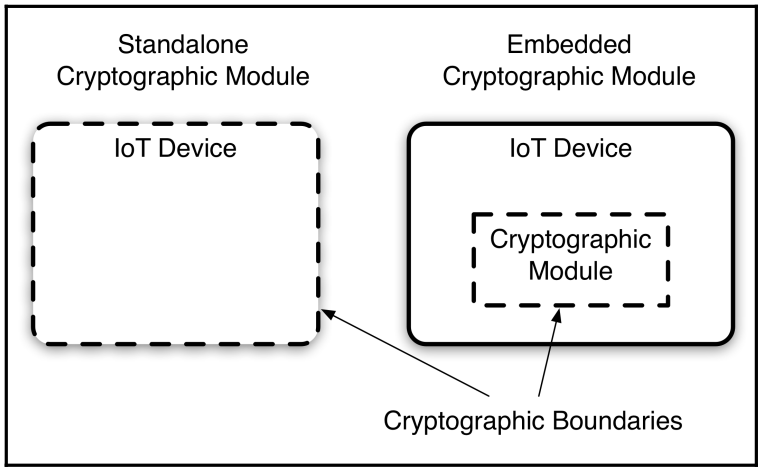

Digital Signatures - Protection from Spoofing & Tampering
Signature Algorithm
Sign
[Message]
IOT Device
Private key
Sender
Unprotected
Signed Message
[Message] + [Signature]
Spoofer Tamperer
Protected
Signature Algorithm
Verify
Pass/Fail
Public key
IOT Device
Receiver
Unprotected

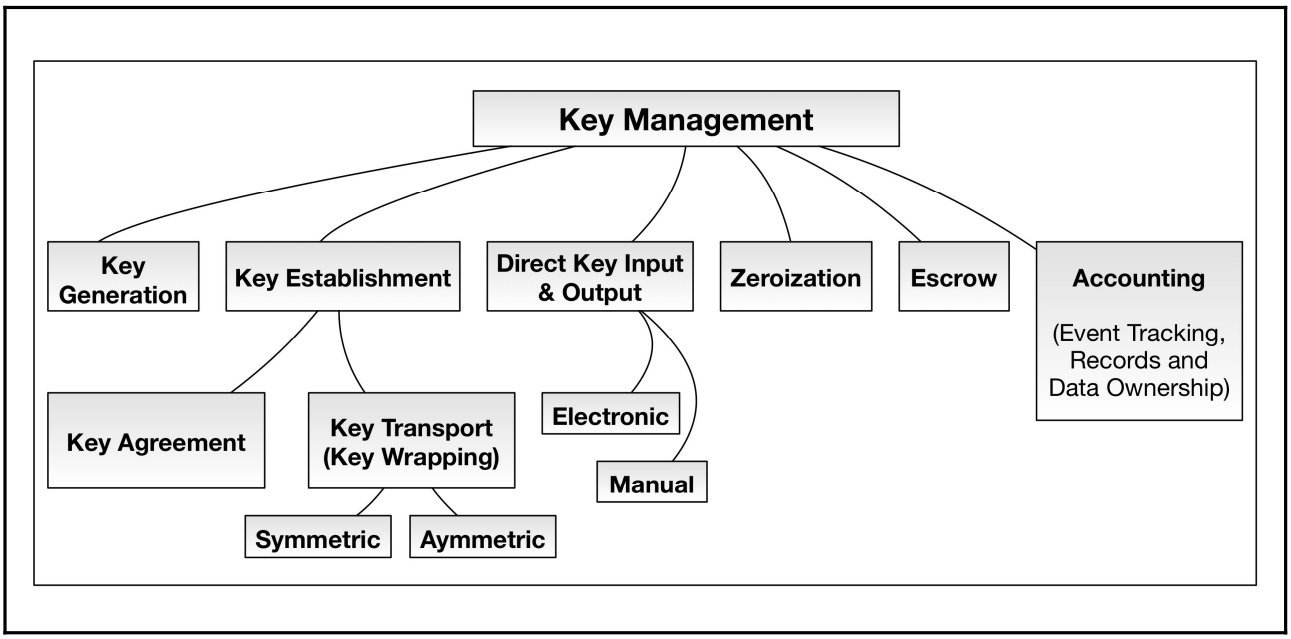

Data D
Hash Algorithm
Hash (D)
Private Key (Signature Key)
Private Key Operation on Hash
Signature Algorithm
Signature (S)
Append Signature to Original Data
Data D
Signature (S)
'Signed' Data Structure

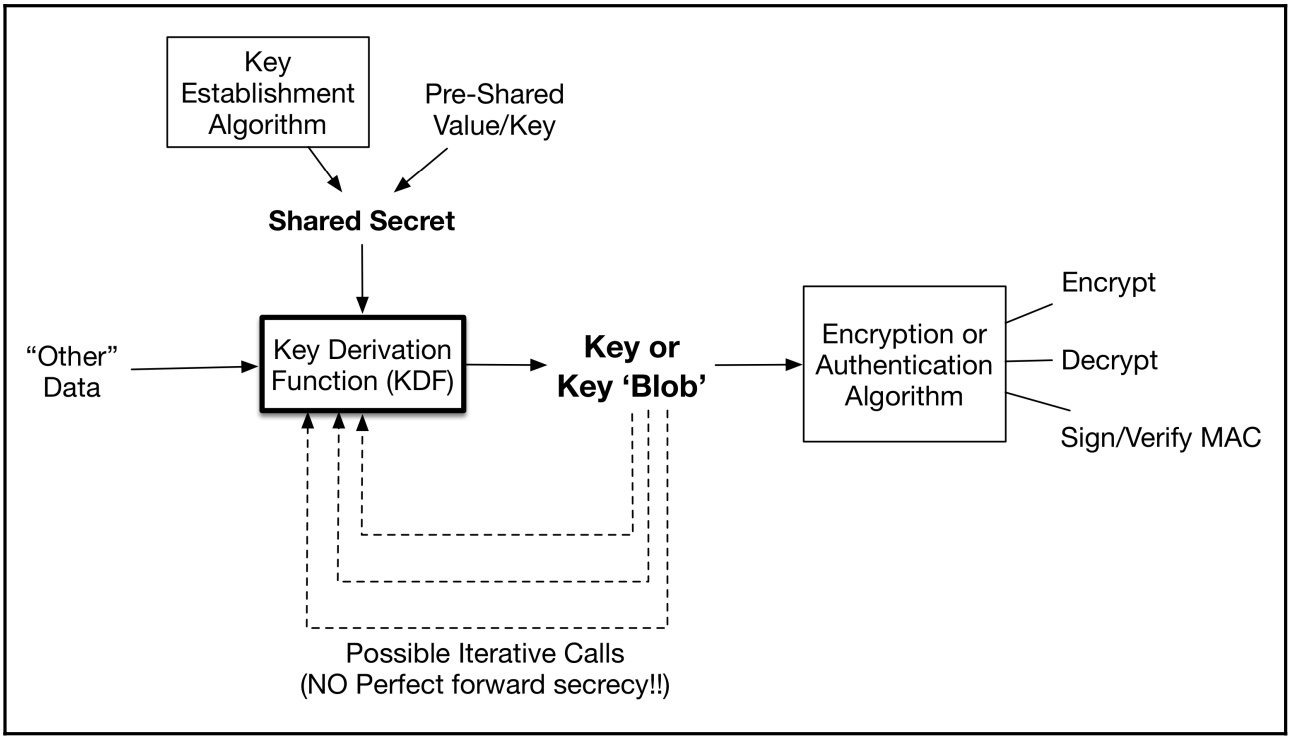

Data D
Keyed MAC Algorithm
MAC Key
MAC
Message Authentication Code
Append MAC to Original Data
Data D
MAC of D
MAC'd Data Structure

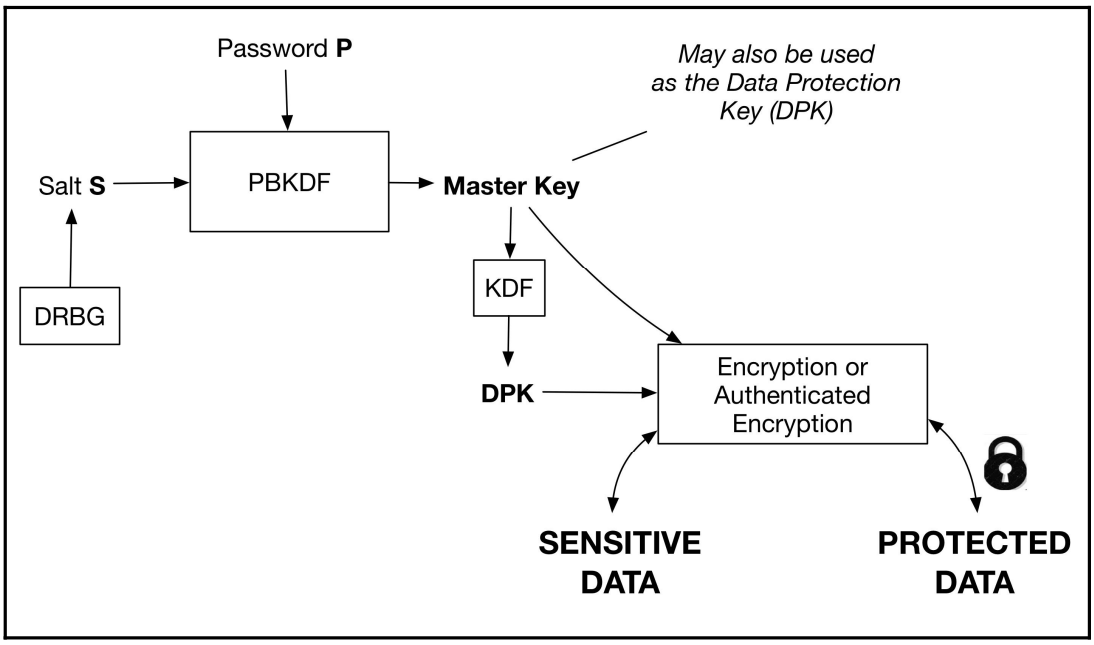

Entropy Source
Entropy Source
Entropy Source
Entropy Pooling
Seed
RNG or DRBG (Internal State)
Cryptographic Keys
Initialization Vectors
Nonces, Salts, Other Variables


Cryptographic Module
Data Input
Data Output
Control Input
Status Output
Encrypt
Decrypt
Sign
Verify
Hash
RNG / DRBG
Entropy Pooling
MAC
Encrypt Keys
Decrypt Keys
Generate Keys
Derive Keys
Store Keys
Zeroize Keys
Key Transport
Key Agreement
Key Establishment
Cryptographic Boundary
Plaintext Secret and Private Keys
Secure Internal / External Storage
Encrypted Secret and Private Keys

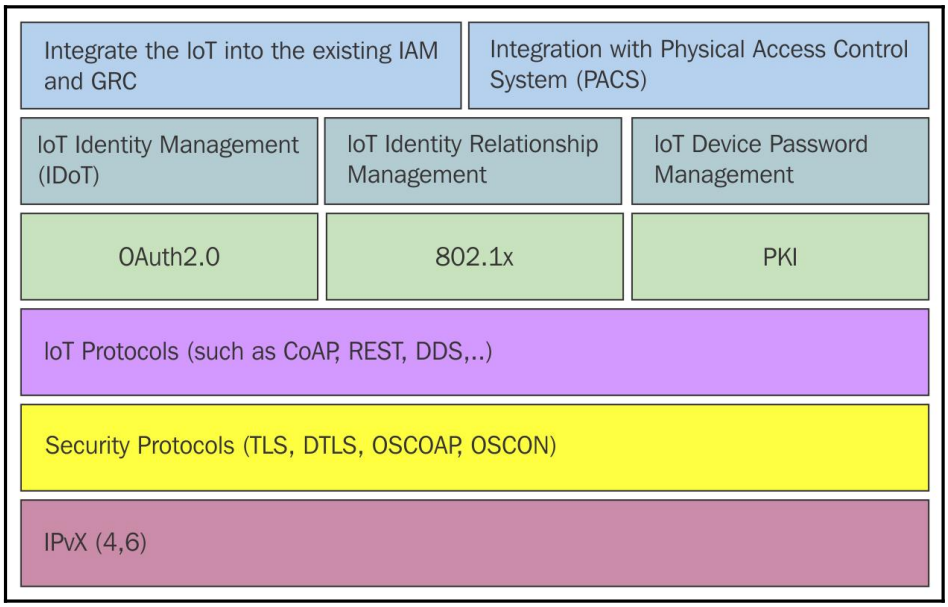

Standalone Cryptographic Module
Embedded Cryptographic Module
IoT Device
IoT Device
Cryptographic Module
Cryptographic Boundaries

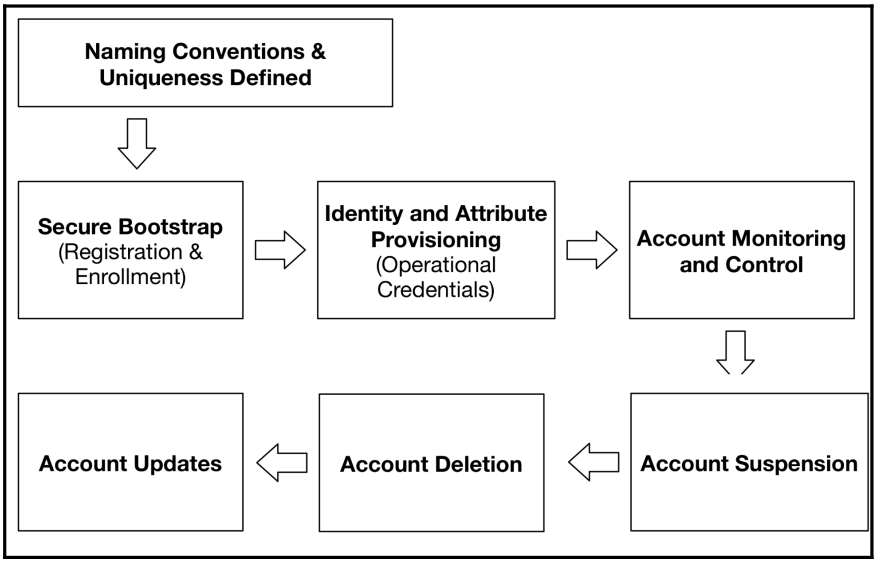

Key Management
Key Generation
Key Establishment
Direct Key Input & Output
Zeroization
Escrow
Accounting
(Event Tracking, Records and Data Ownership)
Key Agreement
Key Transport (Key Wrapping)
Electronic
Manual
Symmetric
Aymmetric

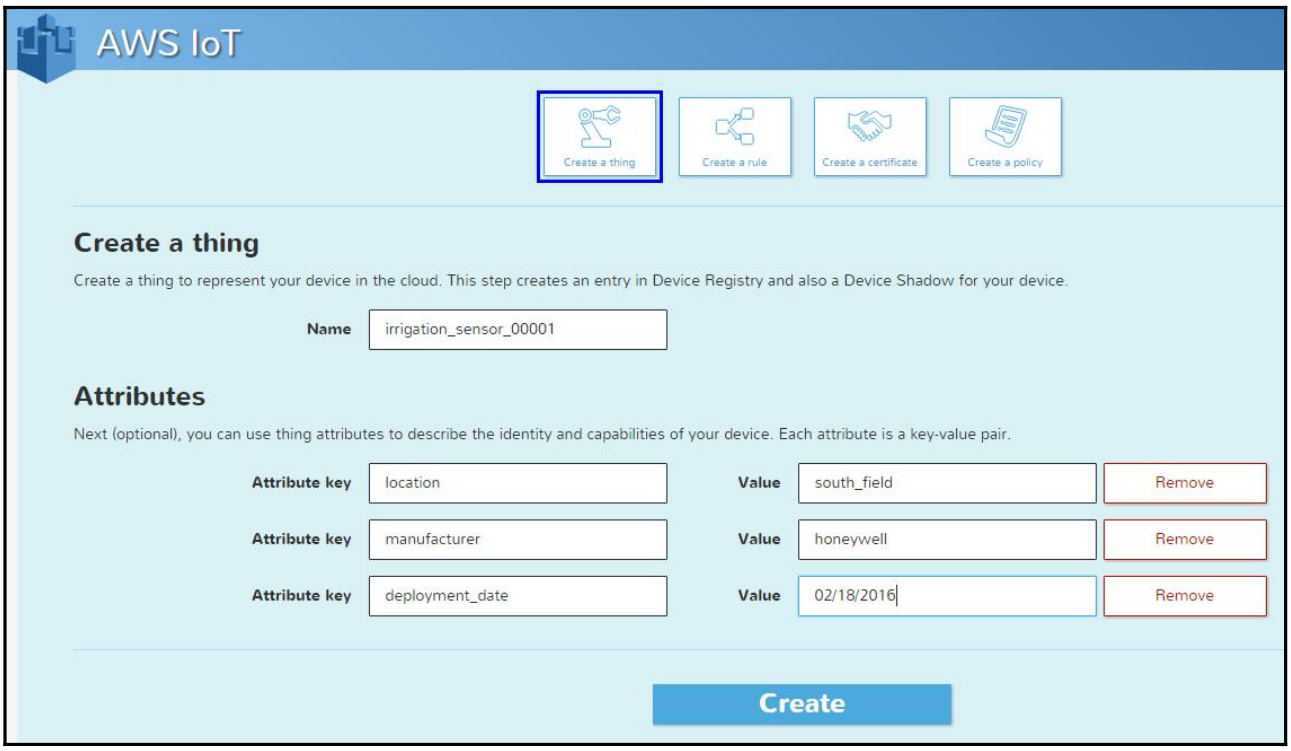

Key Establishment Algorithm
Pre-Shared Value/Key
Shared Secret
"Other" Data
Key Derivation Function (KDF)
Key or Key 'Blob'
Encryption or Authentication Algorithm
Encrypt
Decrypt
Sign/Verify MAC
Possible Iterative Calls
(NO Perfect forward secrecy!!)

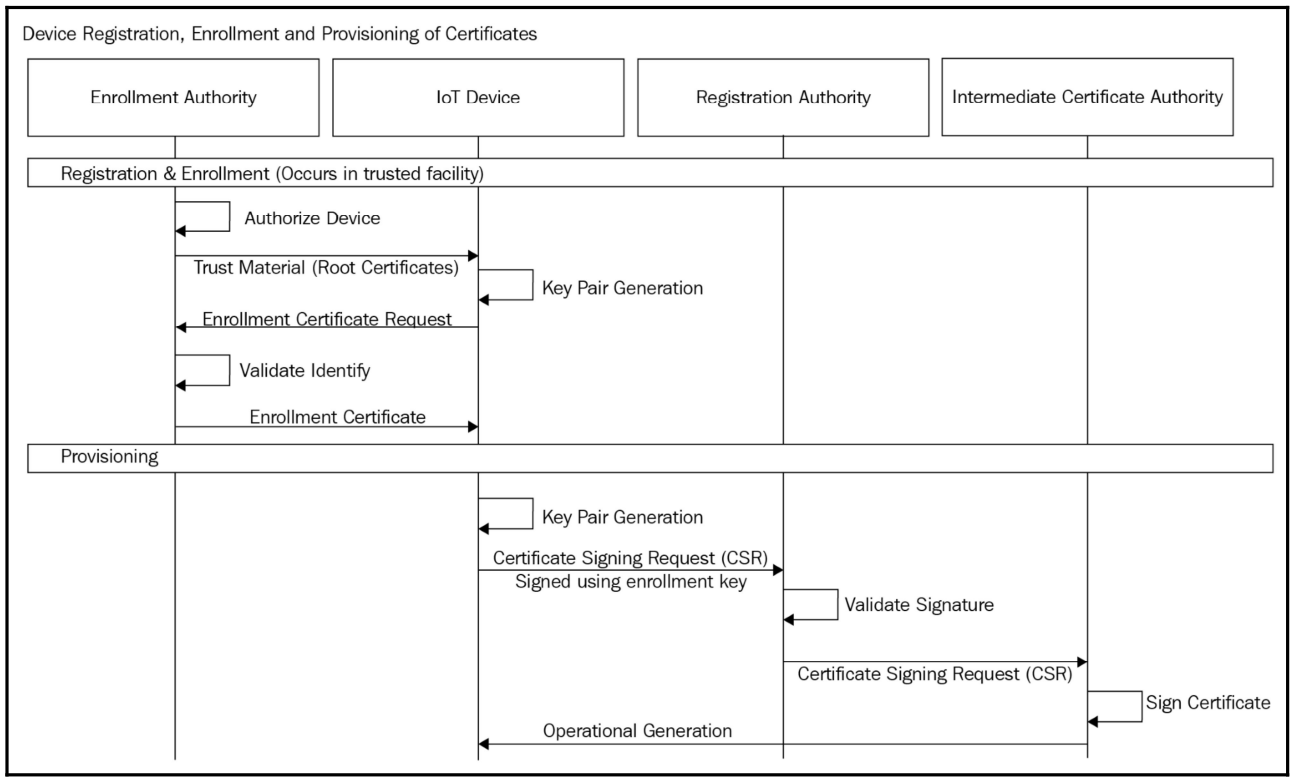

Password **P**
May also be used as the Data Protection Key (DPK)
Salt **S**
PBKDF
Master Key
KDF
DRBG
DPK
Encryption or Authenticated Encryption
SENSITIVE DATA
PROTECTED DATA

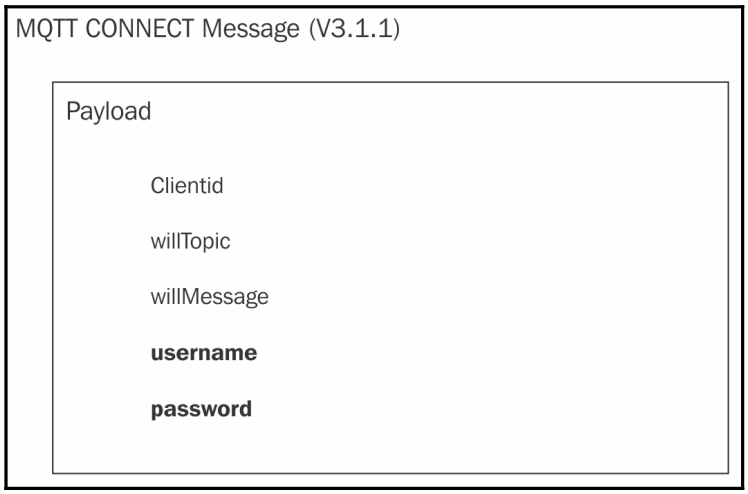
Chapter 7: Identity and Access Management Solutions for the IoT

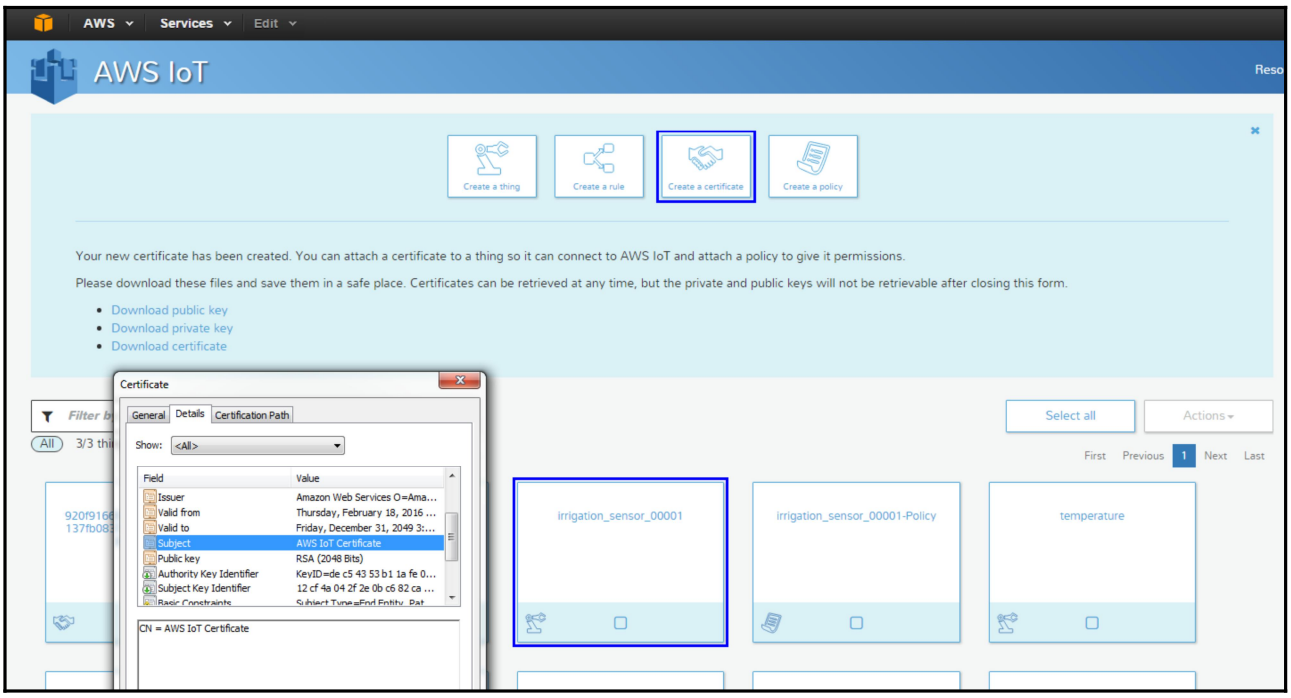


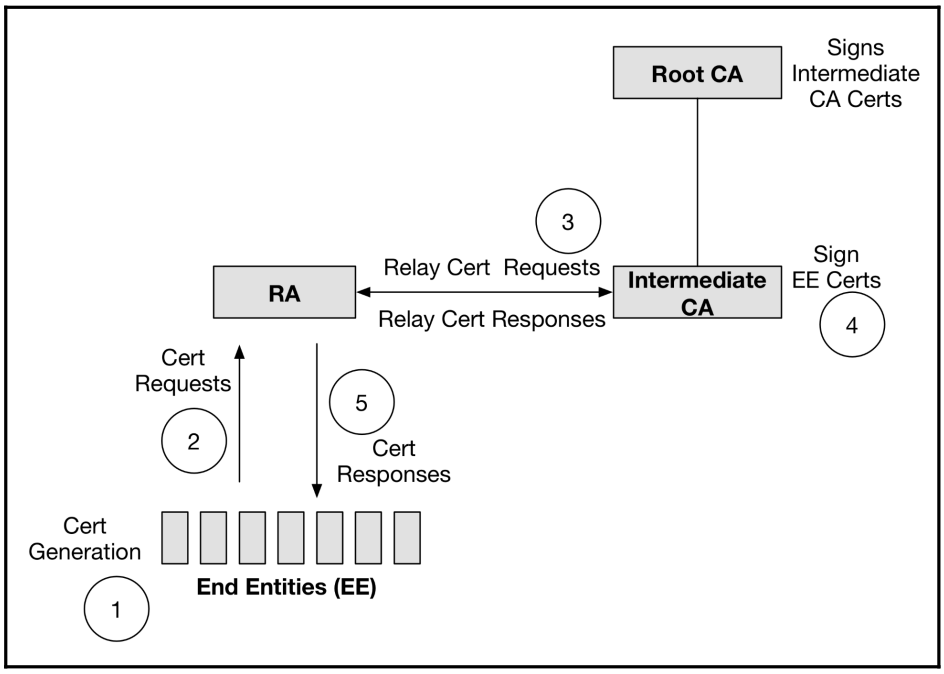


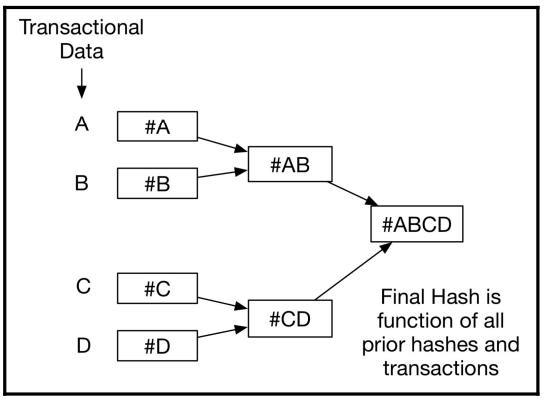

AWS IoT
Create a thing
Create a rule
Create a certificate
Create a policy
Create a thing
Create a thing to represent your device in the cloud. This step creates an entry in Device Registry and also a Device Shadow for your device.
Name
irrigation_sensor_00001
Attributes
Next (optional), you can use thing attributes to describe the identity and capabilities of your device. Each attribute is a key-value pair.
Attribute key
location
Value
south_field
Remove
Attribute key
manufacturer
Value
honeywell
Remove
Attribute key
deployment_date
Value
02/18/2016
Remove
Create

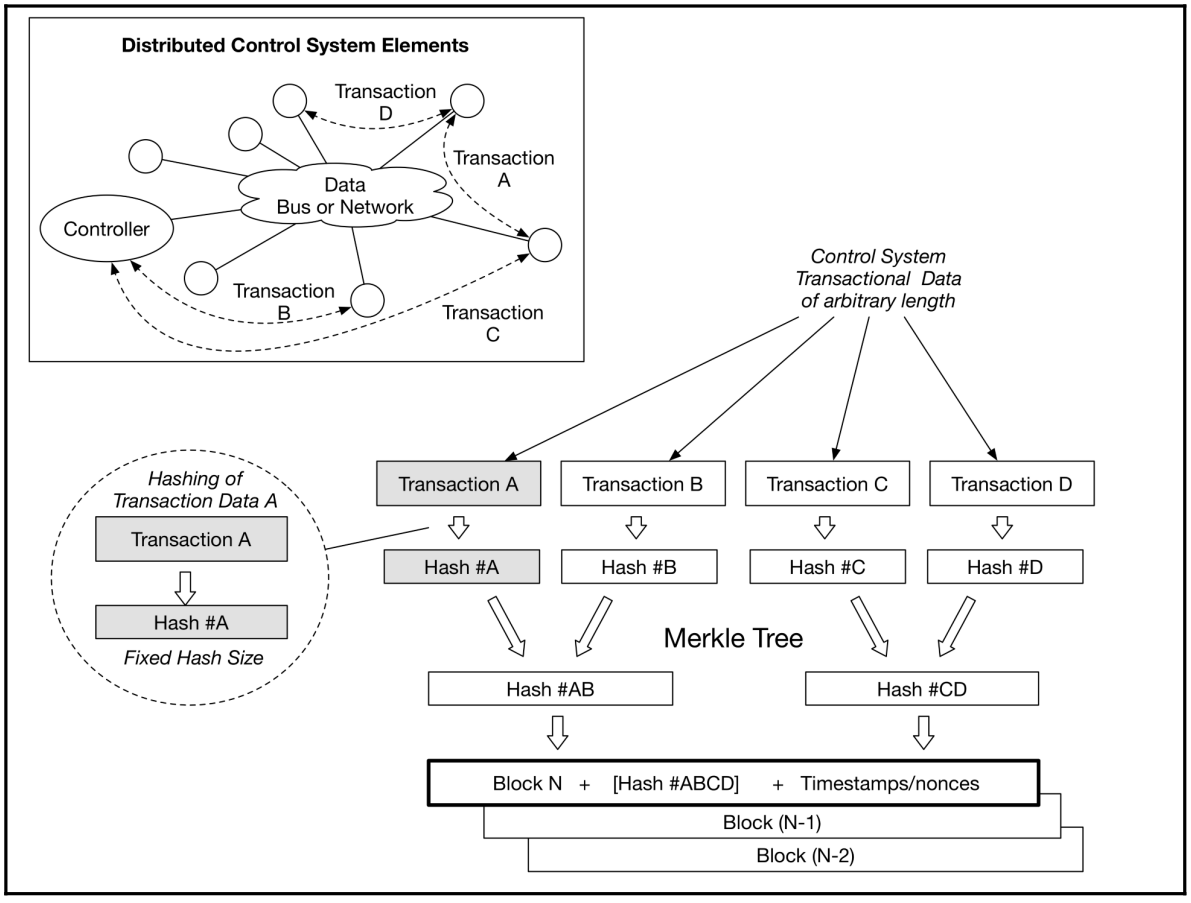

Device Registration, Enrollment and Provisioning of Certificates
Enrollment Authority
IoT Device
Registration Authority
Intermediate Certificate Authority
Registration & Enrollment (Occurs in trusted facility)
Authorize Device
Trust Material (Root Certificates)
Key Pair Generation
Enrollment Certificate Request
Validate Identify
Enrollment Certificate
Provisioning
Key Pair Generation
Certificate Signing Request (CSR)
Signed using enrollment key
Validate Signature
Certificate Signing Request (CSR)
Sign Certificate
Operational Generation


MQTT CONNECT Message (V3.1.1)
Payload
Clientid
willTopic
willMessage
username
password

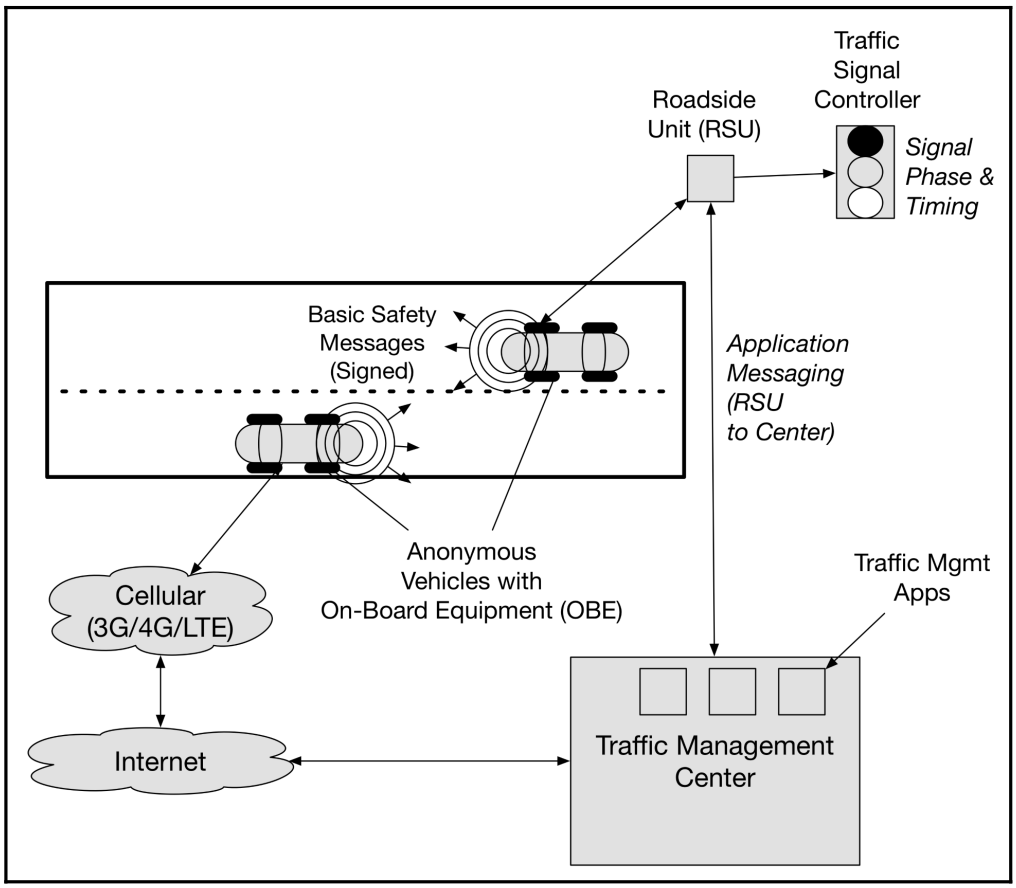

AWS
Services
Edit
AWS IoT
Create a thing
Create a rule
Create a certificate
Create a policy
Your new certificate has been created. You can attach a certificate to a thing so it can connect to AWS IoT and attach a policy to give it permissions.
Please download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys will not be retrievable after closing this form.
Download public key
Download private key
Download certificate
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Issuer
Amazon Web Services O=Ama...
Valid from
Thursday, February 18, 2016 ...
Valid to
Friday, December 31, 2049 3:...
Subject
AWS IoT Certificate
Public key
RSA (2048 Bits)
Authority Key Identifier
KeyID=de c5 43 53 b1 1a fe 0...
Subject Key Identifier
12 cf 4a 04 2f 2e 0b c6 82 ca ...
CN = AWS IoT Certificate
Select all
Actions
First
Previous
1
Next
Last
irrigation_sensor_00001
irrigation_sensor_00001-Policy
temperature

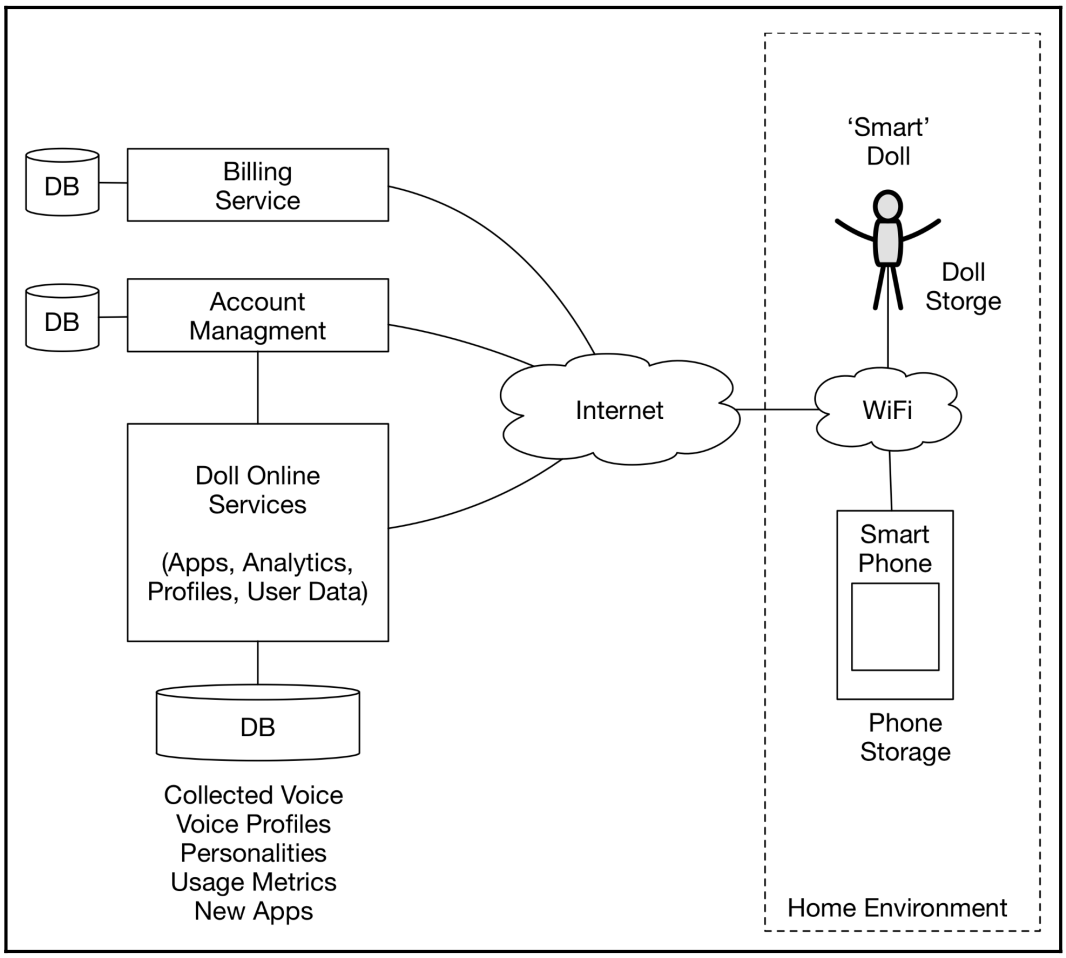

Root CA
Signs Intermediate CA Certs
3
RA
Relay Cert Requests
Relay Cert Responses
Intermediate CA
Sign EE Certs
4
Cert Requests
2
5
Cert Responses
Cert Generation
1
End Entities (EE)

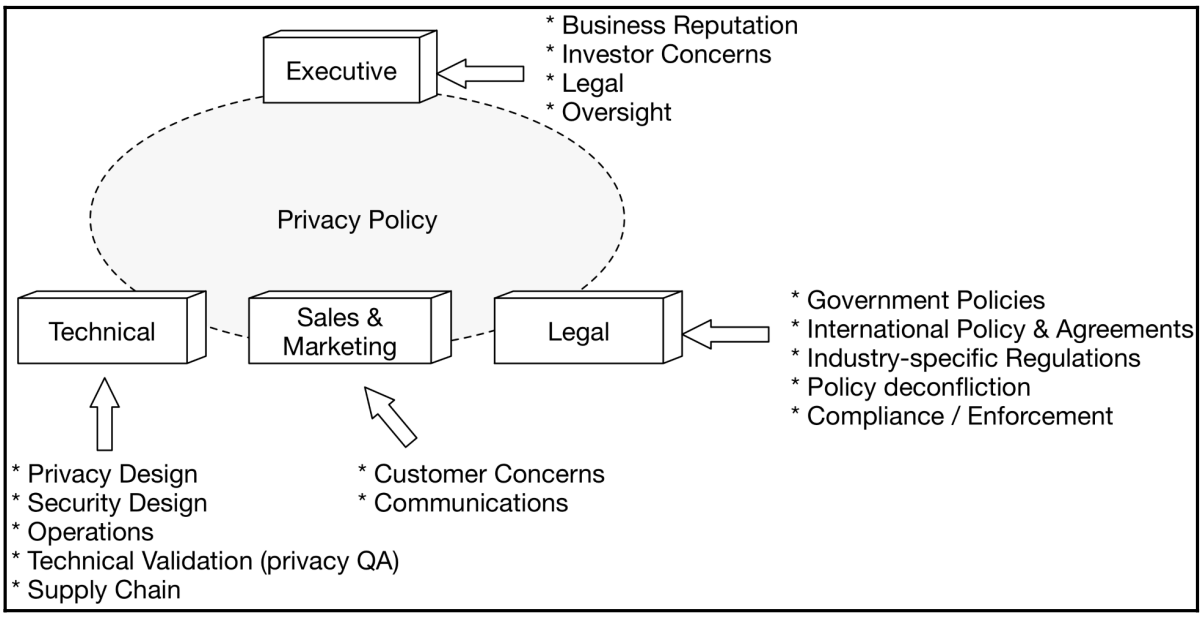

Transactional
Data
A
#A
B
#B
#AB
#ABCD
C
#C
#CD
D
#D
Final Hash is
function of all
prior hashes and
transactions


Distributed Control System Elements
Transaction
D
Transaction
A
Data
Bus or Network
Controller
Transaction
B
Transaction
C
Control System
Transactional Data
of arbitrary length
Hashing of
Transaction Data A
Transaction A
Hash #A
Fixed Hash Size
Transaction A
Transaction B
Transaction C
Transaction D
Hash #A
Hash #B
Hash #C
Hash #D
Merkle Tree
Hash #AB
Hash #CD
Block N + [Hash #ABCD] + Timestamps/nonces
Block (N-1)
Block (N-2)

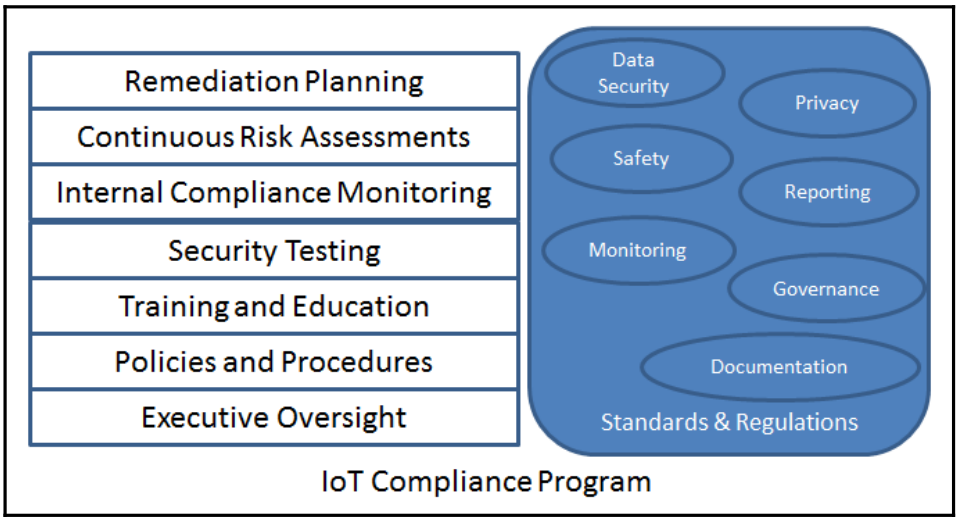
Chapter 8: Mitigating IoT Privacy Concerns

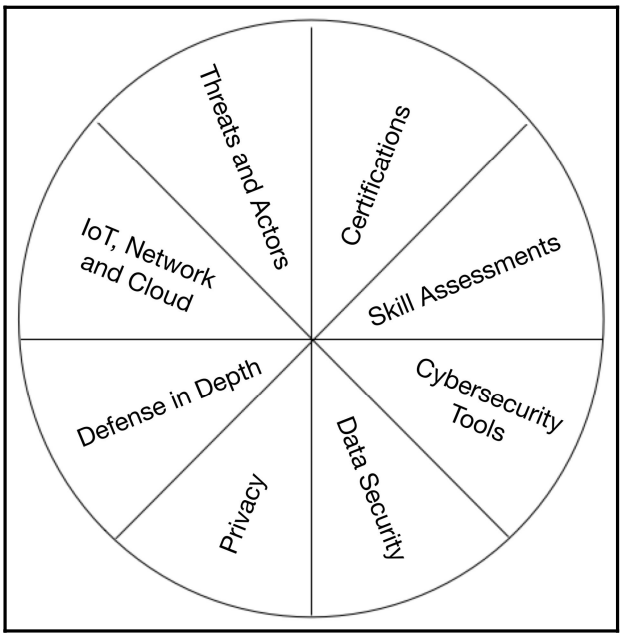


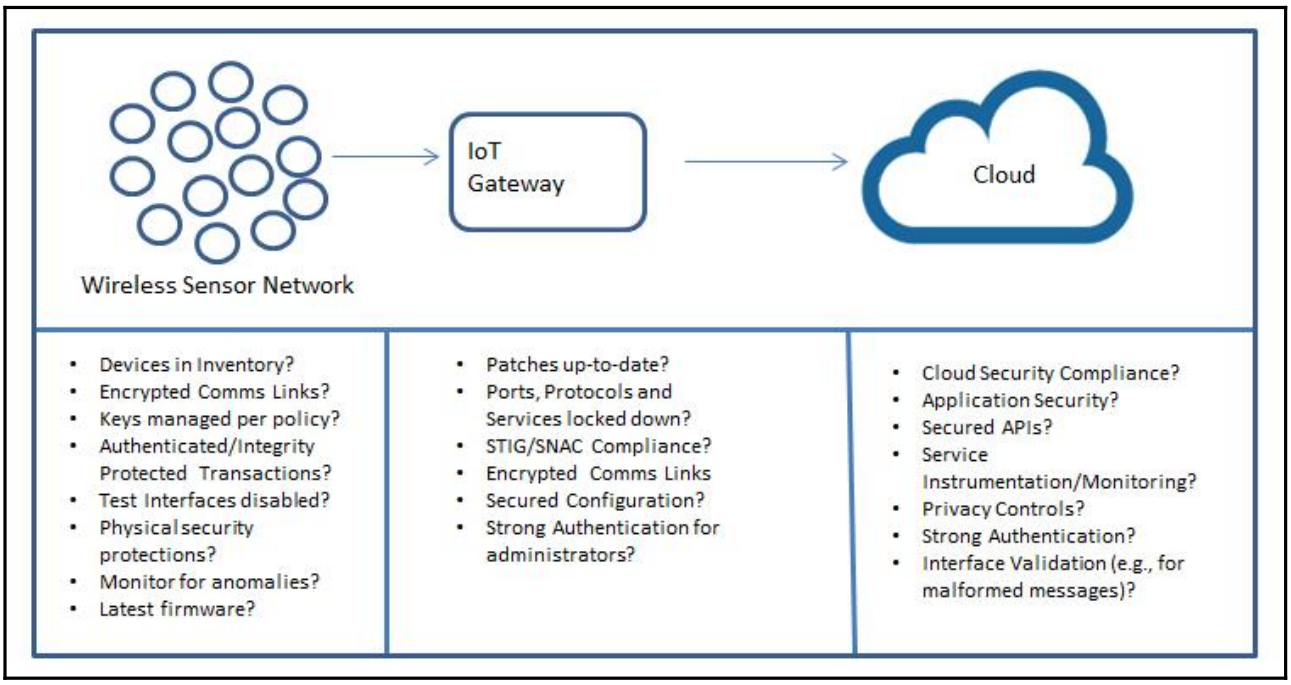

DB
Billing Service
DB
Account Managment
Doll Online Services
(Apps, Analytics, Profiles, User Data)
DB
Collected Voice
Voice Profiles
Personalities
Usage Metrics
New Apps
Internet
'Smart' Doll
Doll Storge
WiFi
Smart Phone
Phone Storage
Home Environment


Executive
* Business Reputation
* Investor Concerns
* Legal
* Oversight
Privacy Policy
Technical
Sales & Marketing
Legal
* Government Policies
* International Policy & Agreements
* Industry-specific Regulations
* Policy deconfliction
* Compliance / Enforcement
* Privacy Design
* Security Design
* Operations
* Technical Validation (privacy QA)
* Supply Chain
* Customer Concerns
* Communications

Chapter 9: Setting Up a Compliance Monitoring Program for the IoT



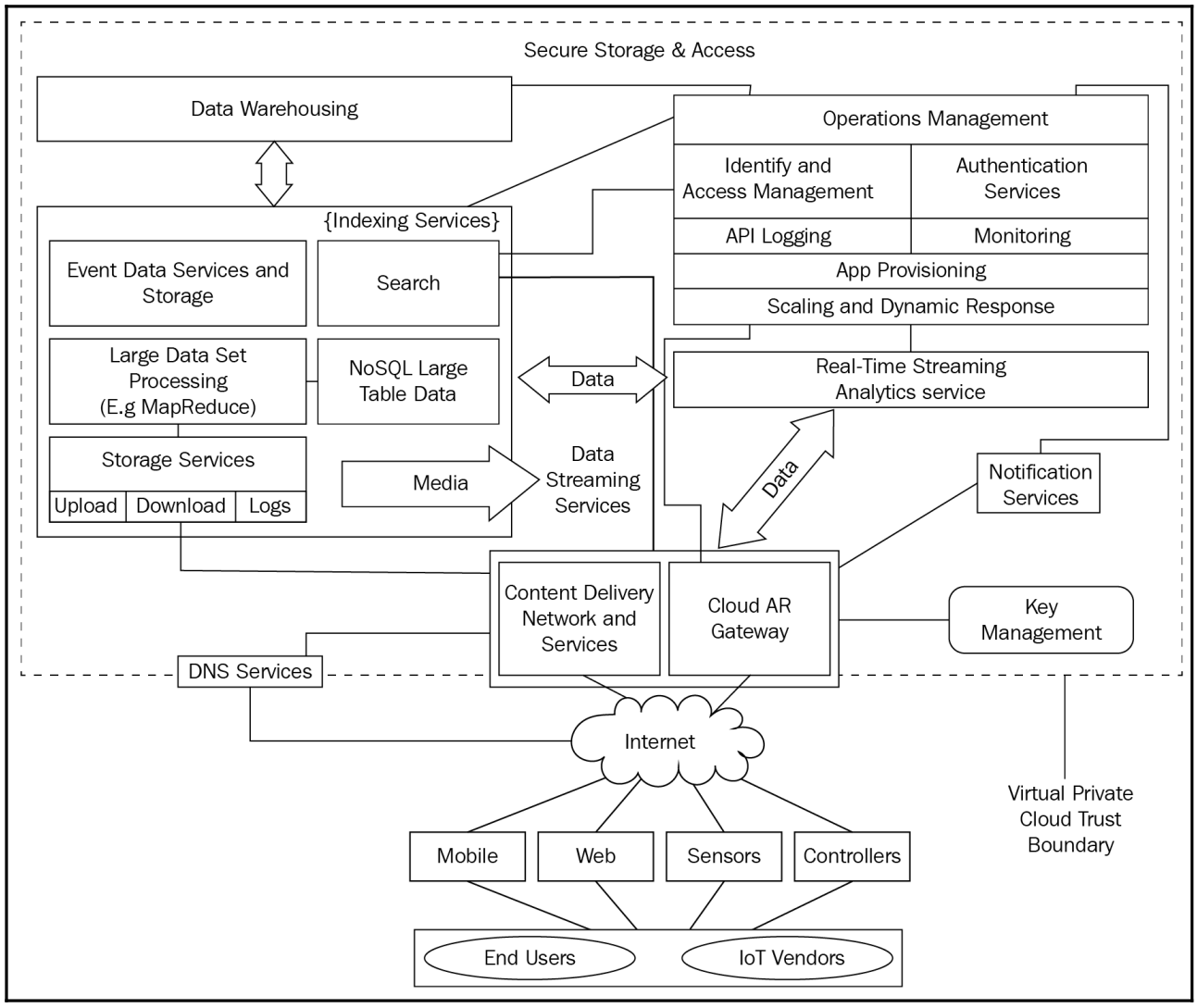


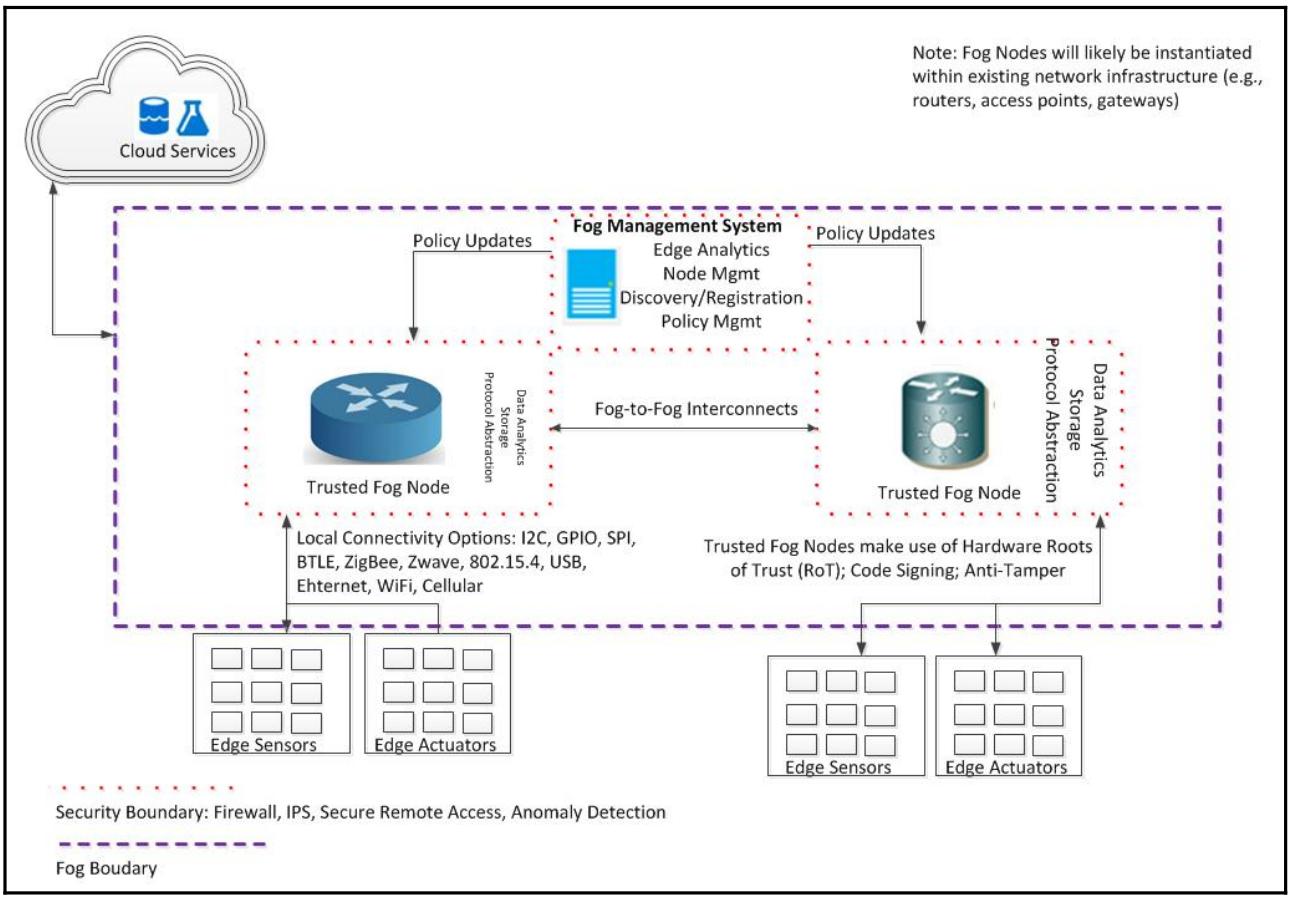


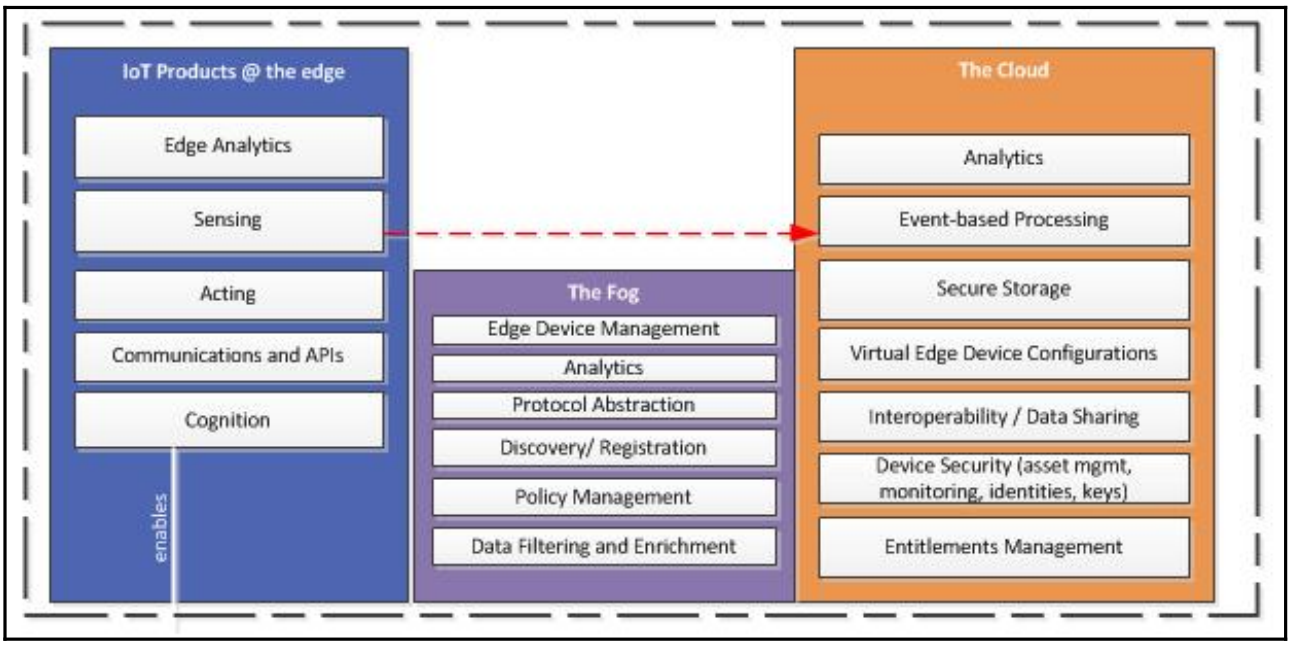
The RMF Process

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor

Chapter 10: Cloud Security for the IoT




Note: Fog Nodes will likely be instantiated within existing network infrastructure (e.g., routers, access points, gateways)
Cloud Services
Fog Management System
Edge Analytics
Node Mgmt
Discovery/Registration
Policy Mgmt
Policy Updates
Policy Updates
Fog-to-Fog Interconnects
Trusted Fog Node
Trusted Fog Node
Protocol Abstraction
Storage
Data Analytics
Local Connectivity Options: I2C, GPIO, SPI, BTLE, ZigBee, Zwave, 802.15.4, USB, Ehternet, WiFi, Cellular
Trusted Fog Nodes make use of Hardware Roots of Trust (RoT); Code Signing; Anti-Tamper
Edge Sensors
Edge Actuators
Edge Sensors
Edge Actuators
Security Boundary: Firewall, IPS, Secure Remote Access, Anomaly Detection
Fog Boudary


IoT Products @ the edge
Edge Analytics
Sensing
Acting
Communications and APIs
Cognition
enables
The Fog
Edge Device Management
Analytics
Protocol Abstraction
Discovery/ Registration
Policy Management
Data Filtering and Enrichment
The Cloud
Analytics
Event-based Processing
Secure Storage
Virtual Edge Device Configurations
Interoperability / Data Sharing
Device Security (asset mgmt, monitoring, identities, keys)
Entitlements Management

Introducing AWS IoT Device Management

AWS IoT Device Management makes it easy to securely manage IoT devices at scale throughout their lifecycle -- from initial setup to ongoing software updates. Learn more about device management features and pricing

Onboard many devices

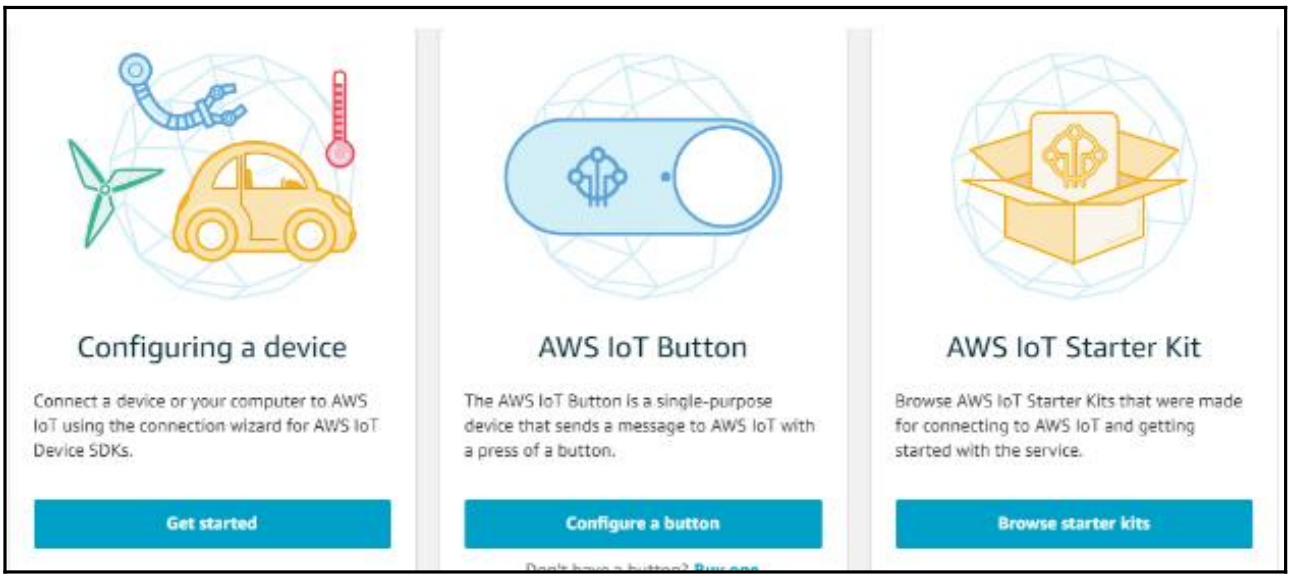
Bulk registration simplifies the onboarding of your entire device fleet.

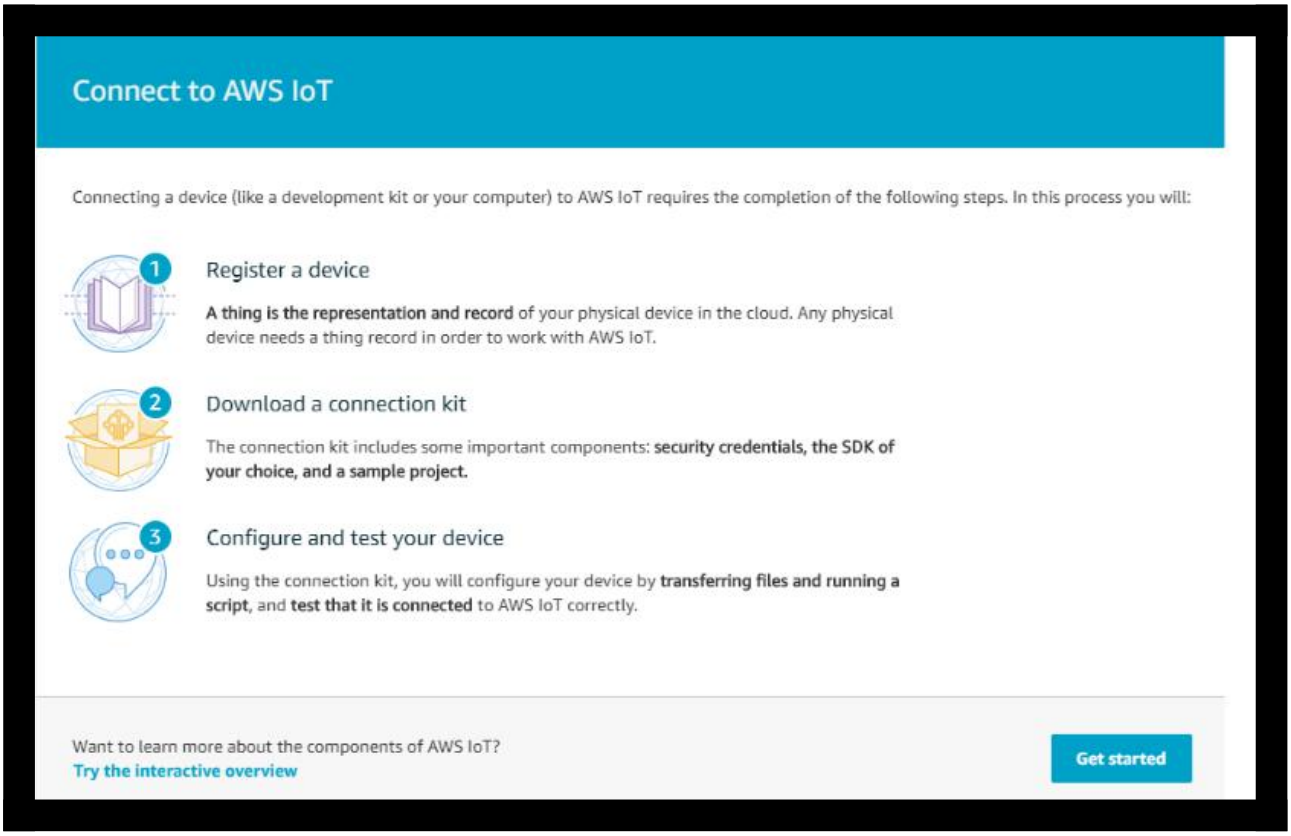
Index and search your device fleet

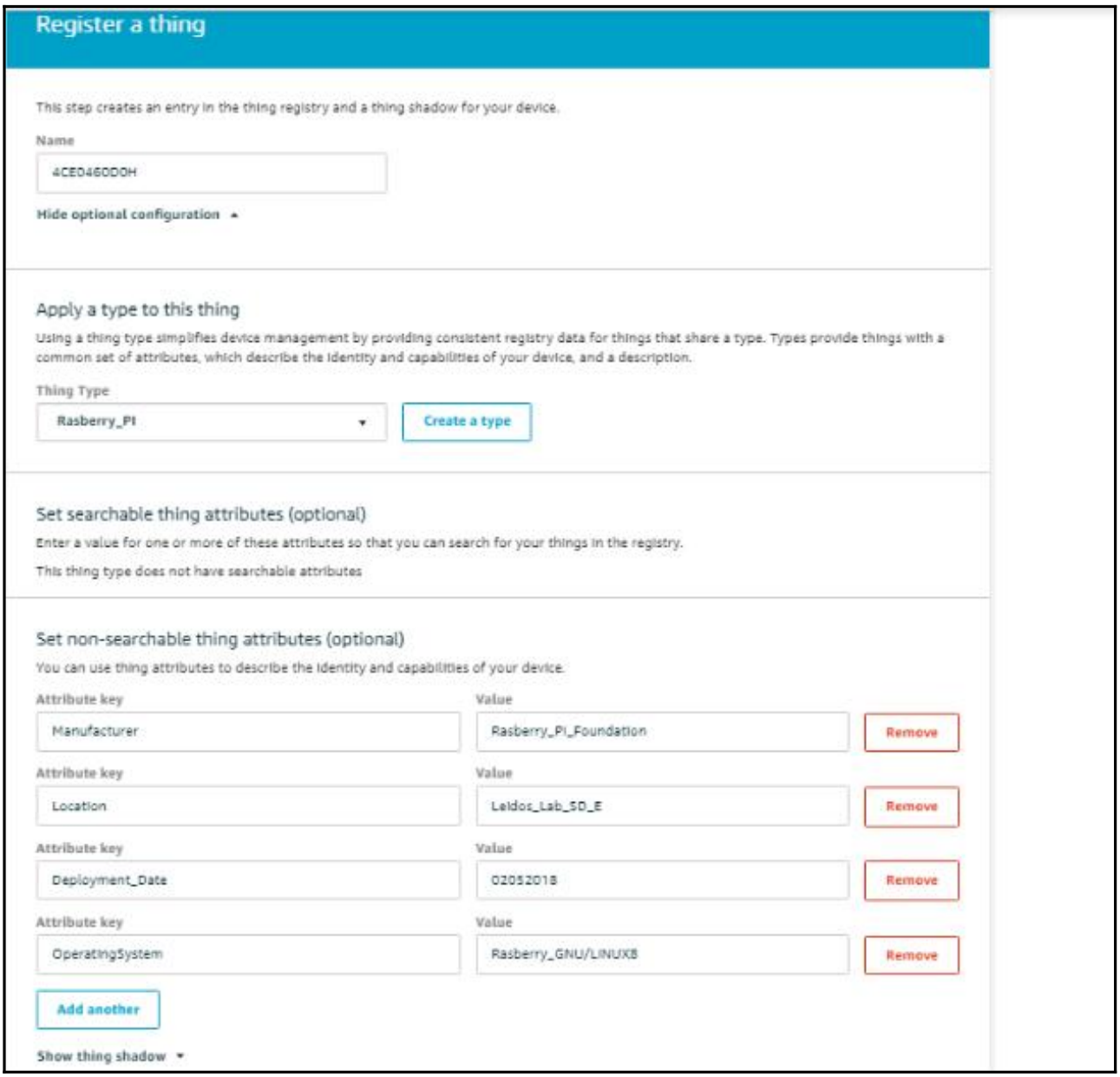
Fleet indexing and search enables you to find the information and state of your devices across your entire device fleet in near real-time.

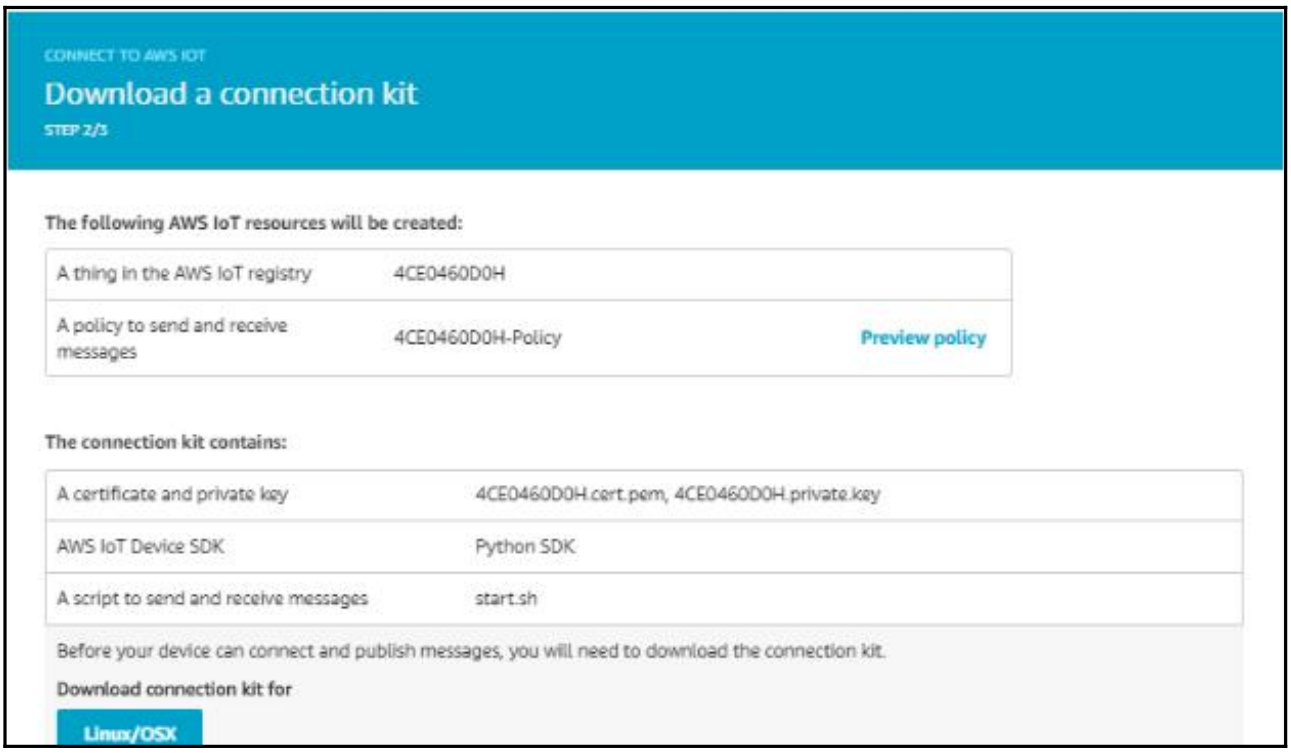
Manage devices remotely

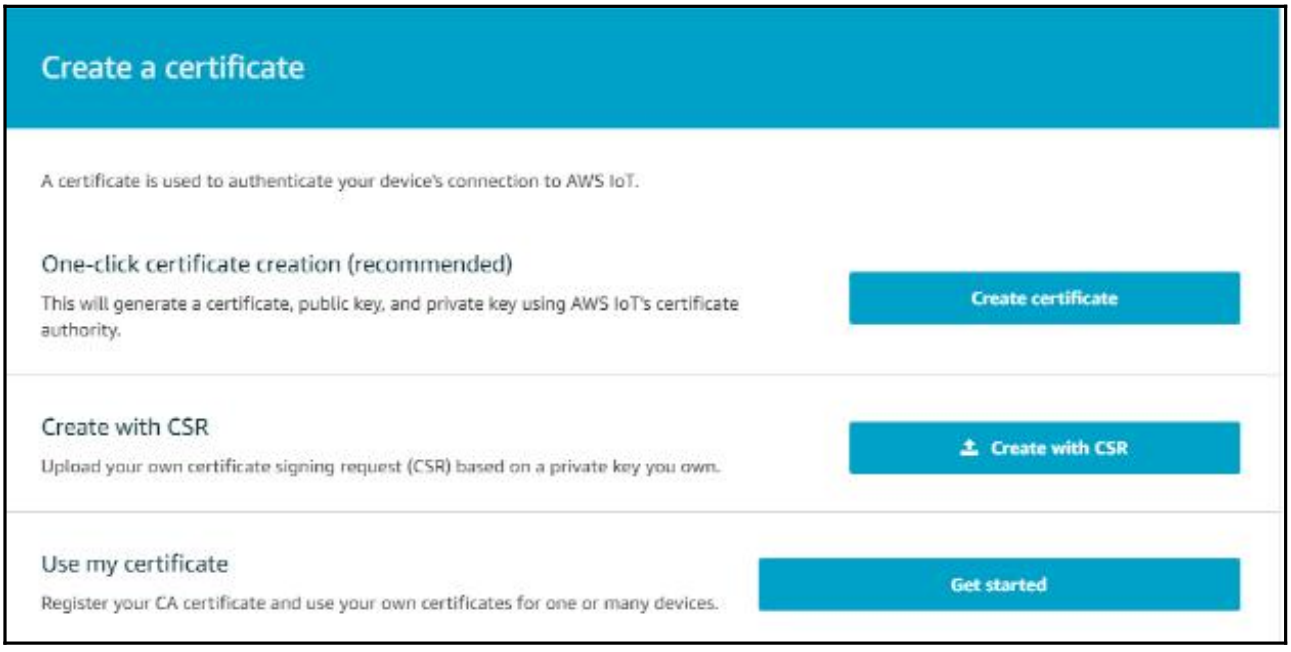
Jobs automate software and firmware updates to patch security and performance vulnerabilities, and improve device functionality.

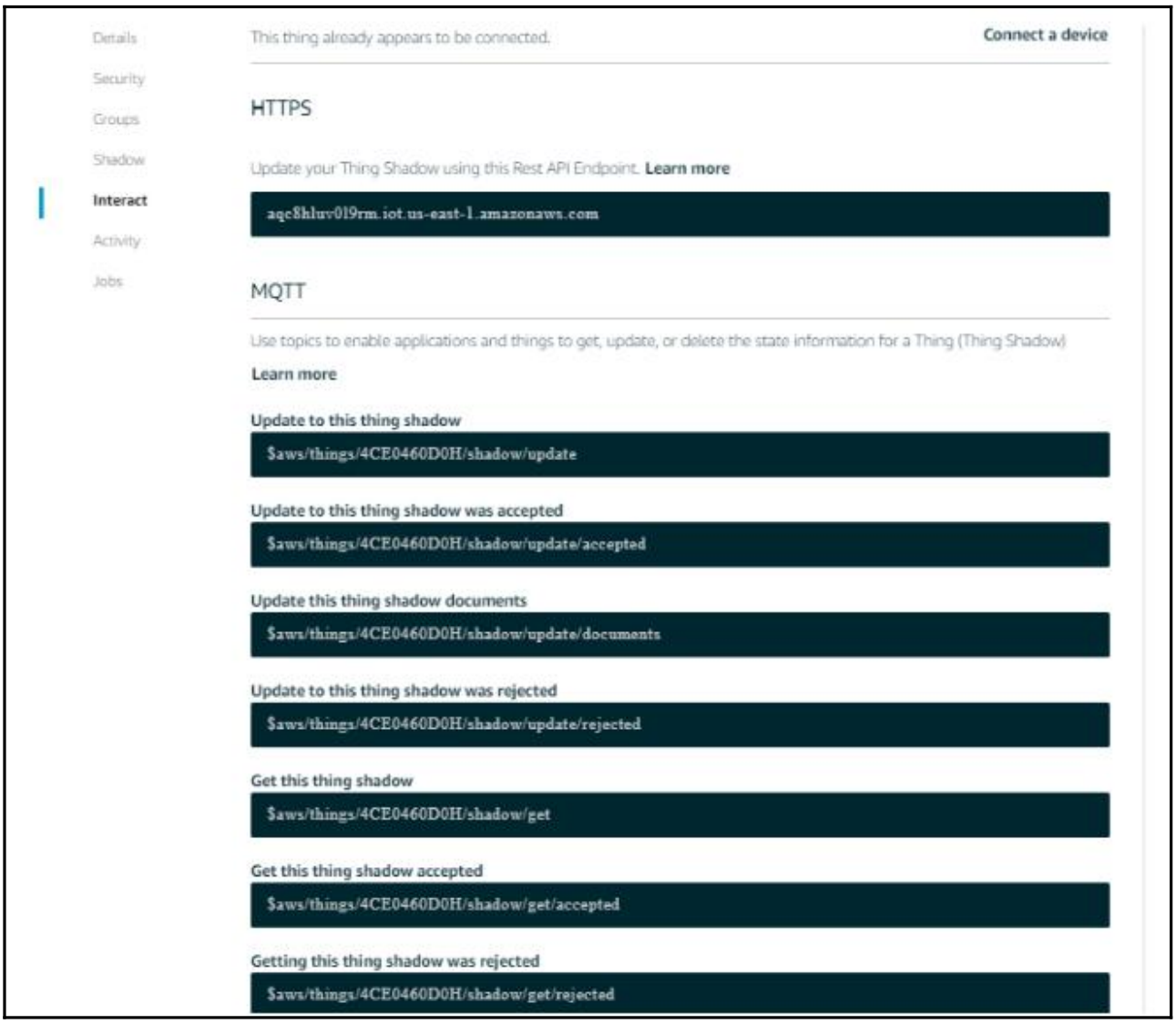

Configuring a device
Connect a device or your computer to AWS IoT using the connection wizard for AWS IoT Device SDKs.
Get started
AWS IoT Button
The AWS IoT Button is a single-purpose device that sends a message to AWS IoT with a press of a button.
Configure a button
AWS IoT Starter Kit
Browse AWS IoT Starter Kits that were made for connecting to AWS IoT and getting started with the service.
Browse starter kits


Connect to AWS IoT
Connecting a device (like a development kit or your computer) to AWS IoT requires the completion of the following steps. In this process you will:
1
Register a device
A thing is the representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT.
2
Download a connection kit
The connection kit includes some important components: security credentials, the SDK of your choice, and a sample project.
3
Configure and test your device
Using the connection kit, you will configure your device by transferring files and running a script, and test that it is connected to AWS IoT correctly.
Want to learn more about the components of AWS IoT?
Try the interactive overview
Get started

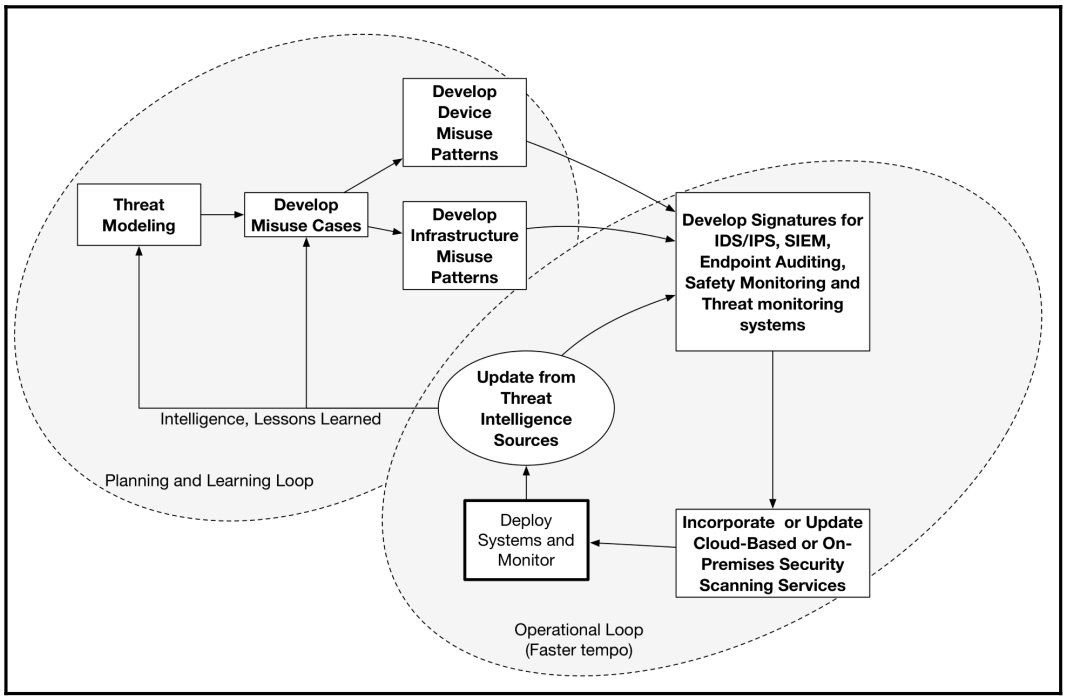

Register a thing
This step creates an entry in the thing registry and a thing shadow for your device.
Name
4CE0460D0H
Hide optional configuration
Apply a type to this thing
Using a thing type simplifies device management by providing consistent registry data for things that share a type. Types provide things with a common set of attributes, which describe the identity and capabilities of your device, and a description.
Thing Type
Rasberry_PI
Create a type
Set searchable thing attributes (optional)
Enter a value for one or more of these attributes so that you can search for your things in the registry.
This thing type does not have searchable attributes
Set non-searchable thing attributes (optional)
You can use thing attributes to describe the identity and capabilities of your device.
Attribute key
Value
Manufacturer
Rasberry_PI_Foundation
Remove
Attribute key
Value
Location
Leidos_Lab_SD_E
Remove
Attribute key
Value
Deployment_Date
02052018
Remove
Attribute key
Value
OperatingSystem
Rasberry_GNU/LINUX8
Remove
Add another
Show thing shadow

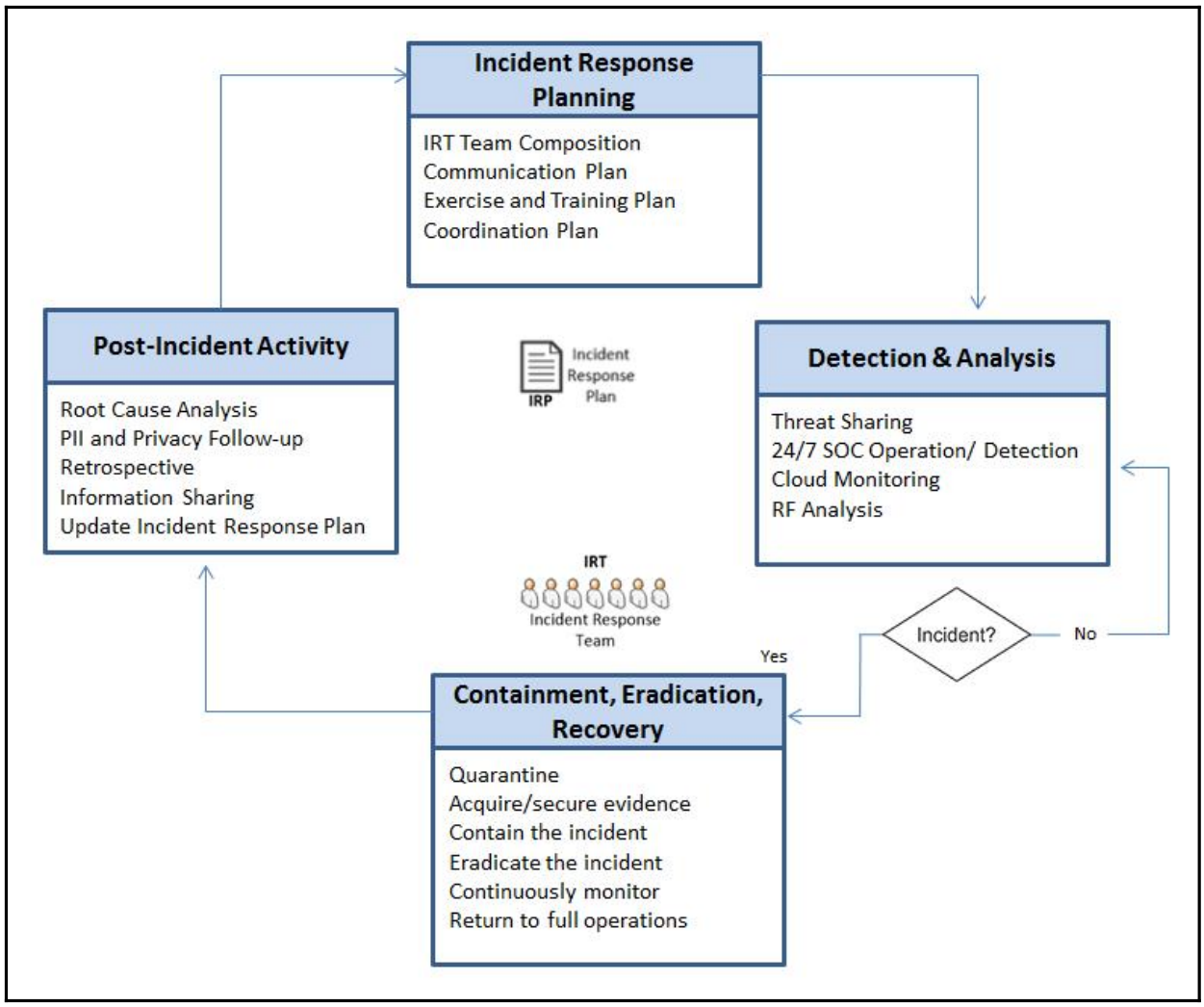

CONNECT TO AWS IOT
Download a connection kit
STEP 2/3
The following AWS IoT resources will be created:
A thing in the AWS IoT registry
4CE0460D0H
A policy to send and receive messages
4CE0460D0H-Policy
Preview policy
The connection kit contains:
A certificate and private key
4CE0460D0H.cert.pem, 4CE0460D0H.private.key
AWS IoT Device SDK
Python SDK
A script to send and receive messages
start.sh
Before your device can connect and publish messages, you will need to download the connection kit.
Download connection kit for
Linux/OSX


Create a certificate
A certificate is used to authenticate your device's connection to AWS IoT.
One-click certificate creation (recommended)
This will generate a certificate, public key, and private key using AWS IoT's certificate authority.
Create certificate
Create with CSR
Upload your own certificate signing request (CSR) based on a private key you own.
Create with CSR
Use my certificate
Register your CA certificate and use your own certificates for one or many devices.
Get started


Details
Security
Groups
Shadow
Interact
Activity
Jobs
This thing already appears to be connected.
Connect a device
HTTPS
Update your Thing Shadow using this Rest API Endpoint. Learn more
aqc8hluv019rm.iot.us-east-1.amazonaws.com
MQTT
Use topics to enable applications and things to get, update, or delete the state information for a Thing (Thing Shadow)
Learn more
Update to this thing shadow
$aws/things/4CE0460D0H/shadow/update
Update to this thing shadow was accepted
$aws/things/4CE0460D0H/shadow/update/accepted
Update this thing shadow documents
$aws/things/4CE0460D0H/shadow/update/documents
Update to this thing shadow was rejected
$aws/things/4CE0460D0H/shadow/update/rejected
Get this thing shadow
$aws/things/4CE0460D0H/shadow/get
Get this thing shadow accepted
$aws/things/4CE0460D0H/shadow/get/accepted
Getting this thing shadow was rejected
$aws/things/4CE0460D0H/shadow/get/rejected

Chapter 11: IoT Incident Response and Forensic Analysis




Incident Response Planning
IRT Team Composition
Communication Plan
Exercise and Training Plan
Coordination Plan
Post-Incident Activity
Root Cause Analysis
PII and Privacy Follow-up
Retrospective
Information Sharing
Update Incident Response Plan
IRP
Incident Response Plan
Detection & Analysis
Threat Sharing
24/7 SOC Operation/ Detection
Cloud Monitoring
RF Analysis
IRT
Incident Response Team
Incident?
No
Yes
Containment, Eradication, Recovery
Quarantine
Acquire/secure evidence
Contain the incident
Eradicate the incident
Continuously monitor
Return to full operations

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.