Planning Session

Identity and Access Management for the IoT

B. Russell

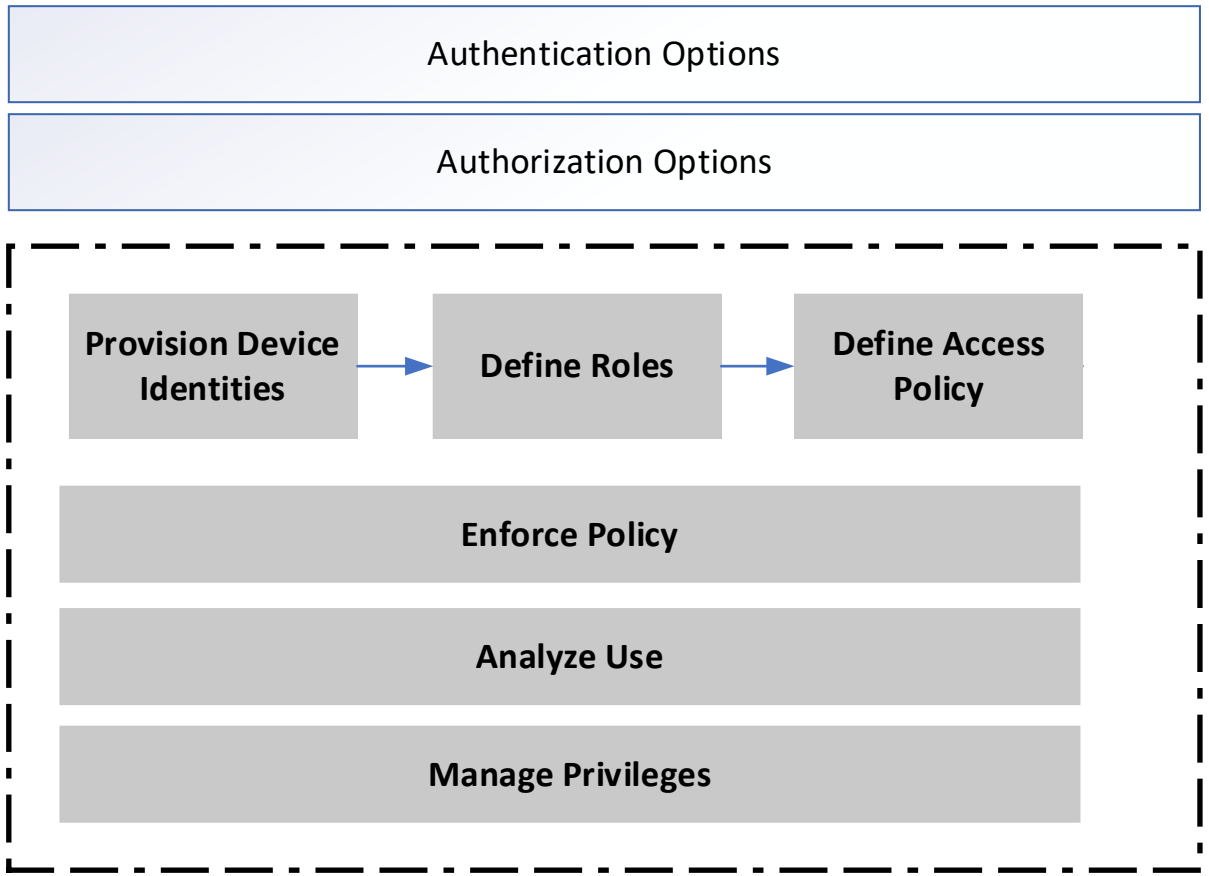
11/11/20

Purpose & Goal

- **Purpose:** Determine scope for CSA IoT Identity and Access Management Project

- **Goal:** Create scope statement for document

General IAM Scope



Each area is complicated

- Many different options
- Could write lots of material for each

Authentication Options

- Depends on use case
  - Could be simple as certificate-based authentication
- Do we include pairing in here
  - Bluetooth Classic / LE
  - ZigBee/Zwave
- WiFi Authentication

- Device to cloud service
- Device to network
- Device to device

Authorization Options

- Oauth 2
- FIDO
- SAML
- UMA
  OpenID 2.0
- Etc

- What do we write about these? If anything? Decision tree/matrix?

Provision Device Identities

- Includes bootstrap process to onboard devices into organization
  - Zero-touch configurations
  - Recent NIST NCCOE guidance- trusted onboarding, etc
  - Physical processes + technology processes
- What format for identities
  - X.509 / IEEE 1609.2 / other
- Lifecycle management of identifiers
  - Certificate renewal
  - Certificate revocation
  - What protocols to use (EST, SCEP, etc)

Define Roles

- Recommend RBAC approach?
- Or, Attribute based access controls?
- Perhaps define a set of standard roles
  - User
  - Admin
  - Auditor
  - etc

Define Access Policy

- Enroll devices into AD OUs?
- What about non-IP devices?
  - How to control access
    - Mutual certificate authentication?
    - Pairing
  - Dive into pairing process (e.g., Recommend Bluetooth Security Levels and Modes?)
- Recommend access policies for device to cloud?
- What about vendor managed devices inside an orgs boundaries?
- What about recommending zero-trust for devices operating on-network?

Enforce Policy

- Many options here depending on authorization options chosen
  - Think policy enforcement points, policy decision points, etc
    - XACML?

Analyze Use

- Cloud IAM systems now analyze how often privileges and accounts are used
  - If not used for period of time, accounts demoted/shut down…

- Our guidance/thoughts?

Manage Privileges

- Local device accounts
  - User vs admin? What privileges to admin? What privileges to user?
    - Complex – different for different types of devices
- User access to devices
  - Specific privileges assigned for specialty functions
    - Audit logging?
  - Case example: Connected car diagnostic port privileges
    - Go to a dealer vs go to repair shop
      - Should repair shop have full access?
        - User granted permissions (UMA)?
- For consumer devices, users should grant permission
  - Granular access controls? On the data and functions?
- For enterprise devices, ??
  - A fleet of cars?

For Discussion

- What area to focus on?
- What format for deliverable?
  - Doesn’t have to be a standard document
    - Cheat sheet, checklist, spreadsheet, etc??
- Try and choose something that can be done relatively quickly?
  - Then iterate and do more?