How IoT standards fit together

• Many recent & developing standards in IoT Security
  • SUIT
  • RATS
  • TEEP
  • MUD
  • FDO / LwM2M Bootstrap / BRSKI
  • CoSWID

• But what does an implementer actually need? What is the whole-system view?
Fundamental questions

• What software is my device running?
• What is the provenance of my device's software
• Who is authorised to initiate a software update and under what circumstances
• How should my device connect to a network?
• With which systems should my device communicate?
• How should my device update its trusted software?
Where is the trust?

Network Access Requirements

3rd-Party Network Access Requirements Provider

Network Operator

Device Operator

Provision Trust Anchors

Device trustworthiness

True state of Application

Application details

Application

NOTE: TEEP not included
IoT Security Standards

NOTE: TEEP not included
Recommendations for IoT deployments

• What Devices SHOULD do:
  • attest their application
  • support secure remote update
  • use a secure onboarding protocol
  • use TEEs to protect valuable assets

• What Application developers SHOULD do:
  • issue a SBOM with each update
  • issue model attestation evidence with each update
  • issue network access requirements with each update

• What Verifiers SHOULD do:
  • consume model attestation evidence

• What Network Operators SHOULD do:
  • place devices in a DMZ until an attestation report is received
  • apply restrictive network policies to devices that are out-of-policy (e.g. need update)
  • enable network access requirements based on attestation reports