Building Trust into the IoT
The Role of the Mobile Industry

Mona Mustapha
IoT Technical Specialist

ETSI IoT Week 2019
Over 200 pages of advice and best practice to secure devices, service platforms and networks

85 detailed recommendations

12 principal attack models

3 ‘worked’ examples – wearables, personal drone, automotive

Risk and privacy impact assessments

Supported by:
Worked Examples

- The guidelines contain three worked examples to demonstrate how to use the guidelines
- Shows how generic guidelines can be applied to a multitude of different IoT services because most IoT services are build from the same components
- The worked examples cover both the front-end ‘devices’ and back-end ‘service platforms’
Example Recommendation: Trusted Computing Base
Example Recommendation: Trusted Computing Base

- Secure Hardware Element
- Secure Identity
- Cryptographic Functions
- Credentials

Trust Anchor
Example Recommendation: Trusted Computing Base

- Secure Hardware Element
- Secure Identity
- Cryptographic Functions
- Credentials

- Mutual-authentication of peers
- Provisioning and Personalization
- Separation of Duties
- Executable image validation

Trust Anchor
Example Recommendation: Trusted Computing Base

Secure Hardware Element

Secure Identity

Cryptographic Functions

Credentials

Trust Anchor
Leveraging the SIM to Secure IoT Services

Mobile network operators use SIM Cards to authenticate devices accessing their networks and services. SIM cards can also support additional security capabilities that can be harnessed by Internet of Things (IoT) applications.

The case study shows how mobile operators in the Americas, Asia and Europe are developing and deploying SIM-based IoT security services to support their IoT customers.

Four mini-case studies in one document:

- Secure provisioning and storage of a PKI certificate on a SIM card in a smart meter.
- SIM-based solution to update the passcodes on smart meters once they have been deployed in the field.
- Use of SIM cards to authenticate smart watches and other IoT devices.
- Use of SIM to securely provision an IoT device’s identity and credentials for secure authentication to cloud platforms.

www.gsma.com/iot/case-study-sim-secure-iot-services/
| Title: | Using the SIM as a ‘Root of Trust’ to Secure IoT Applications. |
| Description: | Develop common approaches to leverage SIM security capability for IoT solutions providers. |
| What is the need? | Define solutions that let IoT developers leverage standards based SIM security capabilities - taking the concept of using the SIM to secure IoT services one step closer to commercialisation. |
| What will be done? | The deliverable will define common ways for IoT services to use the capabilities of the SIM to enhance the security of commonly used internet protocols (e.g. D/TLS). |
| Who: How: | Developed and documented by a group of technical experts from (amongst others) network operators, SIM vendors, module vendors and cloud solution providers. |
| When: | To be published in Q4, 2019 |
In one solution we use an IoT Security Applet to:

- Enable the IoT device to securely perform mutual (D)TLS authentication to a server using asymmetric and symmetric security schemes.
- Enable the IoT device to compute shared secrets and keep long term keys secret.
- Enable credential life cycle management from an IoT Security Service.

**Note:** IoT Security Applet shall only use APIs defined by JavaCard, GlobalPlatform and ETSI 102 241.
Using: GSMA IoT Security Assessment

How To Assess Your Solution or Your Suppliers:

- Organisational Procedures
- Service Platform Security
- Communications Security
- Device Security

gsma.com/iotsecurity
GSMA IoT Security Assessment – Backed by Security Experts

Don’t have the resources/knowledge to complete an GSMA IoT Security assessment?
⇒ Then use the services of a security expert, some examples being:
Security Features of LTE-M & NB-IoT Networks

• Highlights the security enabling features and services LTE-M and NB-IoT networks with the purpose of:
  • Explaining how LTE-M & NB-IoT networks are “Secure by Design”
  • Raising awareness and usage of the security features and services provided by mobile operators
  • Driving awareness of the security services and features of Mobile IoT networks within mobile operators who have yet not deployed the features
  • Providing an example of how IoT network security can be promoted by mobile operators to differentiate themselves form other network technologies
