A Required Security and Privacy Framework for Smart Objects

Antonio Skarmeta

University of Murcia
skarmeta@um.es
Outline

- Introduction
- Motivation
- The Lifecycle of Smart Objects
- IoT-A as a baseline for IoT Architectures
- Integral Security and Privacy Framework
- Conclusions
Introduction

• Current Internet evolving towards a global network of interconnected *smart objects* affecting our *everyday lives*
  – IT developments **accelerating** this trend
  – Unprecedented economic and social **opportunities**

• **Security** and **privacy challenges** as main barriers for broad scale IoT deployment
  – Need to **conciliate** interests from different stakeholders (citizens, governments, companies, ...)
  – It is not all about security and privacy → It is about **SAFETY**
Motivation

• Security and privacy concerns were always there...
  – ... but we need to move from an enterprise-centric, to user-centric approaches to **smart object-centric solutions**
  – IoT testbeds are not labs, but cities involving **citizens** and their devices!

• The data sharing paradox in IoT - **To share or not to share, this is NOT the question**...
  – People want/like/need to share (Facebook, Twitter,...)
  – ... the question is how, what, why and under which circumstances!
Motivation

• The data sharing paradox in IoT - **To share or not to share, this is NOT the question...**
  – I want to share my energy consumption, but not if I am at home!
  – Who **owns** the information on a Smart City? Citizens? City Council?

• Need for **cross** and **multidisciplinary** approaches:
  – **Involvement** of citizens is crucial → Smart Cities are for them!
  – Able to address the **lifecycle** of Smart Objects
  – Security and privacy are **cross** → Operational concerns do not matter if smart objects were given fake credentials!
The Lifecycle of Smart Objects

- **Bootstrapping**: Implies installation and commissioning
  - Need for identification before connecting to the network

- **Registration and Discovery**: Smart Objects must be registered to be discovered by others
  - Need for naming, resolution, networking and addressing features

- **Operation**: Machine-to-Machine (M2M) vs Group communications
  - Need for Privacy by Design (Pbd) and Minimal disclosure principles
The Lifecycle of Smart Objects

• Let’s start from the beginning!
IoT-A as a baseline for IoT Architectures

- IoT-A project was intended to define an Architectural Reference Model (ARM) for IoT systems by providing:
  - **IoT Reference Model (RM)** to promote common understanding at high abstraction level
  - **IoT Reference Architecture (RA)** to describe essential building blocks and build compliant IoT architectures
  - **Best Practices/Guidelines** to help in developing an architecture for a specific system based on the RA
IoT-A as a baseline for IoT Architectures

• Key step to move from “Intranets of Things” to a real “Internet of Things”

• Different architecture views from architecture models
  – Functional View describing functionality and interfaces among Functional Groups (FG) composed by Functional Components (FC)
IoT-A as a baseline for IoT Architectures

- **IoT-A Functional View**
Integral Security and Privacy Framework

- **IoT-A compliant** architecture to promote applicability and interoperability

- **Instantiation** of the Functional Components from the Security FG
  - Definition of functionality and interfaces among Security FCs
  - By considering security and privacy requirements of the lifecycle of Smart Objects
Integral Security and Privacy Framework

• **Extension** of the Security FG to be leveraged by future security and privacy IoT Architectures:
  – **Context Manager**: IoT is pervasive $\rightarrow$ need for *adaptive security and privacy*
  – **Group Manager**: addressing the need for flexible data sharing models among Smart Objects
Integral Security and Privacy Framework

• **Bootstrapping**
  – Smart object must be installed and commissioned **before** sending data
  – How it is identified at the beginning? **root identity/root** of trust
  – Who **imprints** the RI (owner, manufacturer)?
  – Implies authentication and authorization mechanisms

• **Registration and Discovery**
  – One it is bootstrapped, smart object must be registered to be discovered (**self-management** approaches?)
  – Security and privacy concerns → Do I want my car to be discovered by everyone?
Integral Security and Privacy Framework

• **Operation – M2M approaches**
  - **Efficient** and **interoperable** approaches → M can be a cloud server or a sensor!
  - Privacy-preserving mechanisms require **accountability** and **traceability** → We need to trust someone!

• **Operation – Group approaches**
  - It will be often smart objects will operate as a group (smartphones, sensors, drones,...) → how to **manage** with billions of heterogeneous devices?
Integral Security and Privacy Framework

- A plethora of technologies intended to be “IoT”, which to pick?
  - Different ITU, ETSI or IETF WG are there
  - **Heterogeneous** environments demand heterogeneous solutions
  - Many of them will **coexist** at different lifecycle stages

- **Framework approach**
  - Smart Objects as information **producers/consumers**
  - **Infrastructure** components enabling smart objects to be registered, discovered and provisioned for secure and privacy-aware (M2M and group) operation
Integral Security and Privacy Framework

- Framework Interactions
Integral Security and Privacy Framework (Bootstrapping)

- *Root identity* as a root of trust: symmetric key/certificate

- Anonymous and group credentials derived from *root identity* → accountable and traceable anonymity

- Based on **PANA** (RFC 5191) as a starting point to define the *bootstrapping for IoT*
  - Currently used by **ZigBee Alliance** and **ETSI M2M**
  - **Extension** of the *Authentication/Authorization* phase
  - **Addition** of new AVPs to carry anonymous and group credentials
Integral Security and Privacy Framework (Registration)

- **Registration** in infrastructure as a consequence of a successful (authenticated/authorized) bootstrapping

- Based on the **Handle** System (RFC 3650):
  - Smart Objects represented as *Digital Objects* (DO)
  - **Supporting** naming, resolution and addressing
  - **Instantiating** IoT Service and IoT Service Resolution IoT-A FC
  - **Favoring** addition of security and privacy features
Integral Security and Privacy Framework (Registration)

- Different handles representing different security and privacy aspects:
  - Derivation of anonymous credentials based on Handle attributes during registration
  - Flexible approach enabling producers to make subsets of services available to subsets of consumers (selective discovery)
Integral Security and Privacy Framework (Discovery and Provisioning)

- Privacy-aware discovery enabling *consumers* to discover *producers* through the use of anonymous credentials previously obtained

- **Provisioning** as an additional previous step to get credentials (keys, tokens,...) to use them against the discovered smart object
  - *Extended semantics* of PANA notification message during the Access phase
  - *Addition* of new AVPs to carry such credentials
  - Use of lightweight and flexible tokens based on DCapBAC to be used even in constrained environments
Integral Security and Privacy Framework (Operation)

• Based on **lightweight** and **flexible** security approaches to make them available even for M2M **constrained environments** (CE):
  – IETF ACE, DICE WGs focused on security for CE
  – Use of the *Constrained Application Protocol* (**CoAP** - RFC 7252) as an application protocol
  – Use of Datagram Transport Layer Security (**DTLS**) (RFC 6347) based on *ECC Raw Public Keys* for authentication
  – Use of the *Distributed Capability-Based Access Control* (**DCapBAC**) approach for authorization
Integral Security and Privacy Framework (Operation)

- Use of advanced and flexible cryptographic schemes enabling secure group communications:
  - Based on certificateless public key cryptography (CP-ABE)
  - CP-ABE keys obtained during the registration associated to smart object’s attributes

- Additional use of partial identities for minimal PII disclosure → integration Proof-of-Possession (PoP) based on anonymous credentials systems (e.g. Idemix) with DCapBAC tokens
Conclusions

• Security and Privacy are a **MUST** for IoT adoption
  – Different stakeholders → different views on them
  – Security + Privacy in IoT → The Internet of MY Things
  – But People care about privacy? In IoT, your car or health devices will be connected! Need for **education** on it.

• Security and privacy demand different concerns during the **lifecycle** of IoT devices
  – It is not all about **technology** → we need **cross** and **multidisciplinary** approaches!

• Our framework to provide a holistic view on IoT security and privacy
  – Developed under **SocIoTal** and **SMARTIE** EU Projects
  – Different developments on **FI-WARE** platform
THANKS FOR YOUR ATTENTION

Antonio Skarmeta
Computer Science Faculty, University of Murcia (Spain)
skarmeta@um.es