Security Lifecycle in professional IoT

Sandeep S. Kumar
Philips Research
March 22, 2015

innovation + you

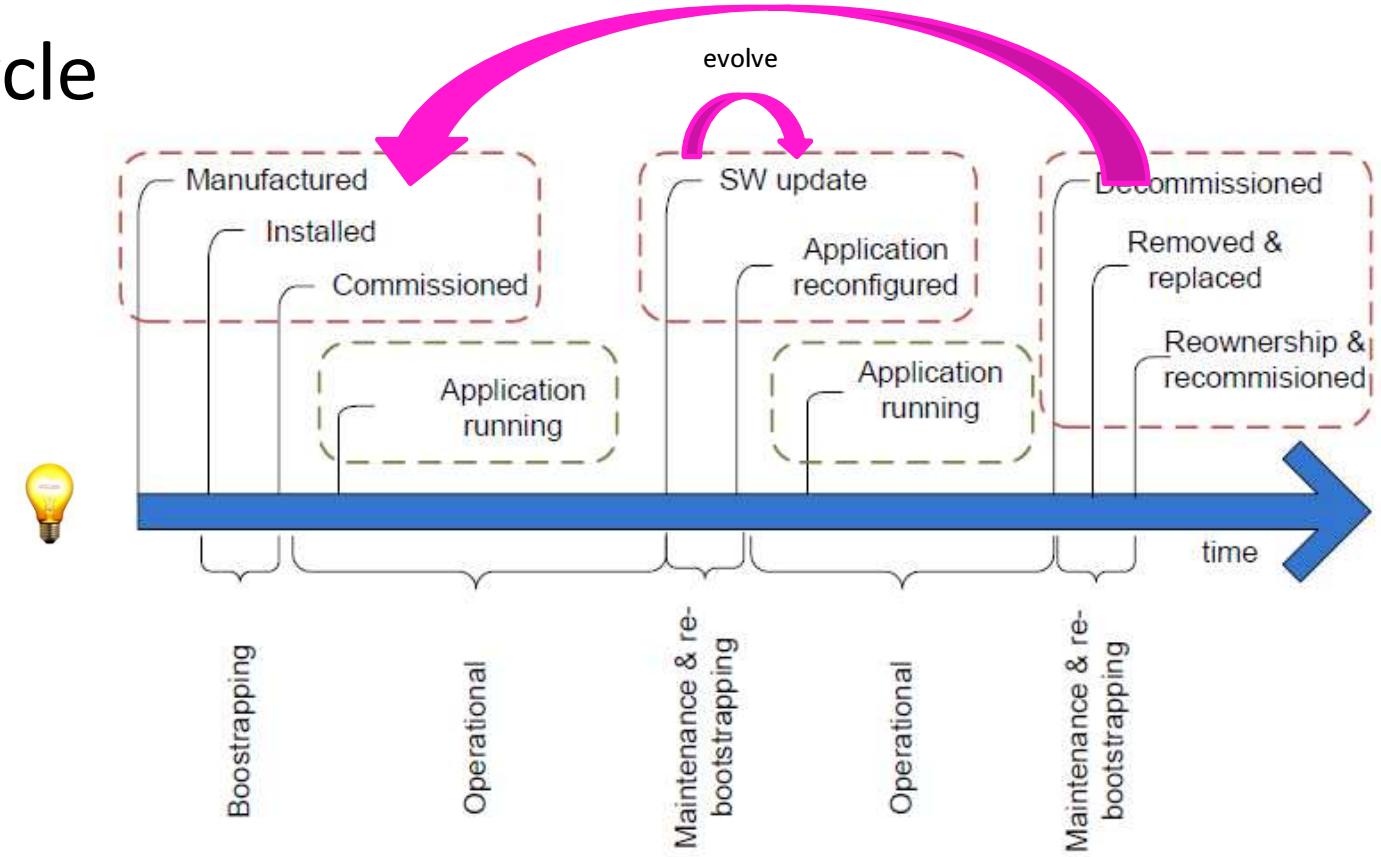
PHILIPS

Focus

- View IoT security in terms of the securing the Lifecycle
- Managed Professional Systems (offices, industrial,..)
  - not home, but could be largely applicable
- Not to provide solutions but to focus on issues that are relevant in the long term

PHILIPS

Lifecycle



- **Device Lifecycle**
  - evolution with software updates and new revisions
- **System Lifecycle**
  - evolution with newer devices in the system and complete system overhauls
- **System-of-Systems (SoS) Lifecycle**
  - evolution with new systems added to SoS

PHILIPS

Issue 1: Reusability

Often memory constrained device
  – Reusable security components across the lifecycle

- **Device Level**
  – Cryptographic algorithms
  – Security protocols
    ▪ Authentication, authorization and bootstrapping

- **System Level**
  – Reuse existing IoT stack where possible also for security
  – Prevent additional layers of security complexity

- **System-of-System Security**
  – Interoperable with existing Internet security protocols
  – Avoid complex middle-boxes

PHILIPS

Issue 2: Key management

- Key generation, update, revocation for the various lifecycle stages

- Manage keys when transitioning from one lifecycle stage to next
  - Secure bootstrapping
  - Allow for multiple stakeholders (manufacturers, operators, end-users)
  - Flexible to cater to systems with devices in different stages of evolution

- Distributed vs Centralized Key management
  - Largely deployment specific

- System-of-System key management
  - Federation across systems belonging to different stakeholders
  - Managing differing security levels between the systems

PHILIPS

Issue 3: Usability

- Usable security for multiple stakeholders
  - installers, commissioners, operators, end-users
  - varying security competence levels

- Secure handover between stakeholders from one lifecycle stage to next
  - Very much dependent on existing workflows
  - How far can workflows evolve in the future?

PHILIPS

Issue 4: Data security and privacy

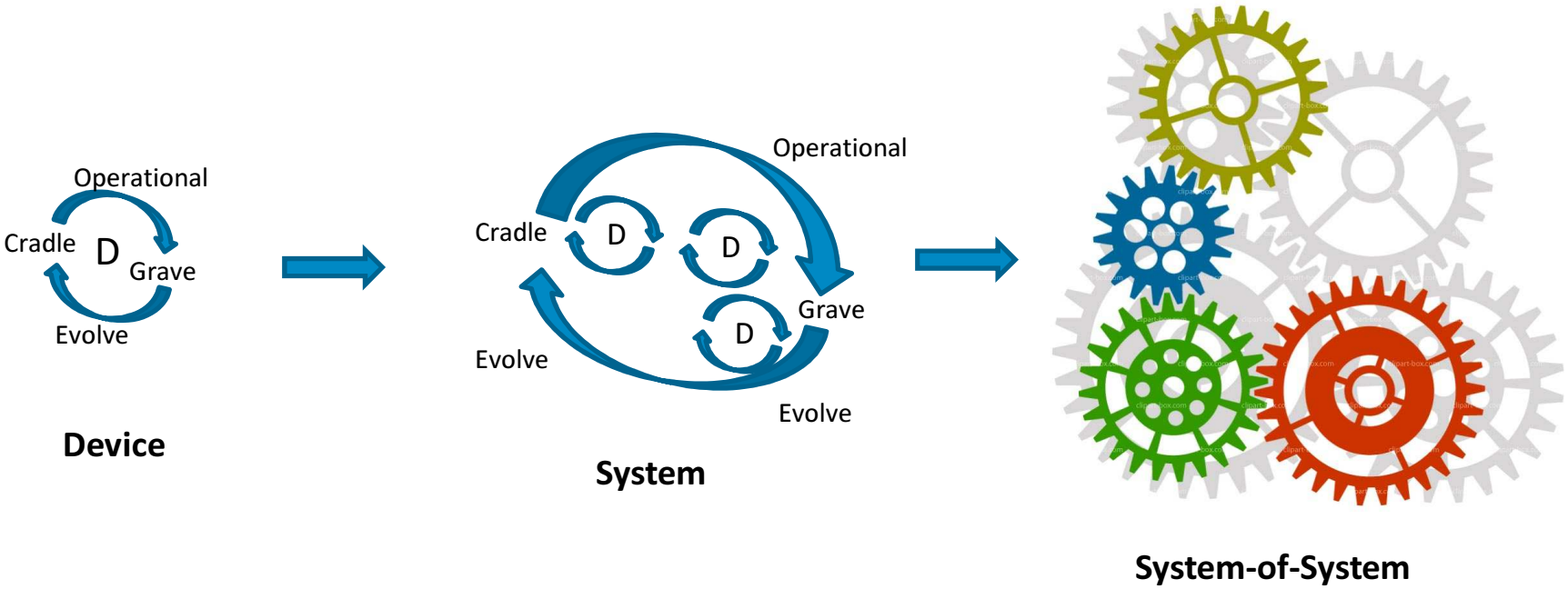
- Individual data points may not seem privacy intrusive
- However easy collection becomes privacy intrusive
  - Data collection over long time -> patterns
  - Data collection on a large scale -> profiling
  - Additional side channel information -> identifiable

- Data lifecycle and its security/privacy
  - Capture, Storage, Usage, Disposal

- Handling data securely in multiple stages of the lifecycle
  - Installation data
  - Commissioning data
  - Operational data

PHILIPS

Issue 5: Evolving Complexity



- Not all devices/systems may be at the same stage of evolution
- Handling legacy devices (and systems) securely will be the most complex issue

(Legacy from non-IoT devices is already a concern in todays professional systems)

PHILIPS

Conclusions

- Future **professional IoT** will be a complex mix of different devices/systems in various stages of lifecycle evolution

- **Main challenges** for security and privacy in such an environment
  - Making smart choices in **reusable components**
  - **Key management** continues to be a “Holy Grail”
  - **Usable Security** to make informed choices
  - **Data privacy** issues with widespread adoption of IoT in professional
  - Complexity management with **legacy devices**

PHILIPS