Securing the Internet of Things

Marc-Oliver Pahl (TUM) | s2labs.org | pahl@tum.de
Why do we need a secure IIoT?
User (un)aware monitoring

Who?
With whom?
Preferences?
How often?
When?
Weight?
What?
Where?

@work
Orchestration
Distributed

Foto: Steve Jurvetson (Flickr)
https://www.flickr.com/photos/jurvetson/7408451314
Security Challenges include

Privacy
Reliability
How can we achieve a secure IIoT?
The usual suspects

• Authentication
• Authorization
• Confidentiality
Why is it challenging?
Whom to trust?

• Hardware?

• Software Services?

• My answer: no-one but the components you design as enabler for the IoT: MIDDLEWARE.
Security by-design
Data Centric IoT
Smart Space

Knowledge Agent

Context

Repository

Context Manager

Adaptation

Actuator Sensor

Adaptation

Service

UI Service

Service

Service

Heterogeneous

Smart Devices

Orchestration

Workflows, etc.

Virtual State Layer

Bidirectional Adaptation

Physical World

Interface Devices

People

Interface Devices

Orchestration

Workflows, etc.

Context Management

Virtual State Layer

Bidirectional Adaptation

Heterogeneous

Smart Devices

Physical World
Data Centric IoT

Orchestrating Workflows, etc.

Virtual State Layer

Context Management

Bidirectional Adaptation

Heterogeneous Smart Devices

Physical World

Level of Abstraction

People

Interface Devices

Orchestration Workflows, etc.

Virtual State Layer

Context Management

Bidirectional Adaptation

Heterogeneous Smart Devices

Physical World

Level of Abstraction

People

Interface Devices

Orchestration Workflows, etc.

Virtual State Layer

Context Management

Bidirectional Adaptation

Heterogeneous Smart Devices

Physical World

Level of Abstraction

People

Interface Devices

Orchestration Workflows, etc.

Virtual State Layer

Context Management

Bidirectional Adaptation

Heterogeneous Smart Devices

Physical World

Level of Abstraction

People

Interface Devices

Orchestration Workflows, etc.

Virtual State Layer

Context Management

Bidirectional Adaptation

Heterogeneous Smart Devices

Physical World

Level of Abstraction

People

Interface Devices

Orchestration Workflows, etc.

Virtual State Layer

Context Management

Bidirectional Adaptation

Heterogeneous Smart Devices

Physical World

Level of Abstraction
A Data Centric IoT

Needs *autonomous management!*
The Virtual State Layer

Services
- Gateway
- Advanced Reasoning
- Orchestration
- User Interface

VSL Overlay
- Knowledge Agent

Hardware Underlay
- Sensor
- Actuator

DS2OS Site Local
- Logical Connectivity
- Physical Connectivity
- Gateway Services
- Other Services

Global
- Central Model Repository
- App Store
How to achieve Security-by-Design?
Two approaches

1. Handling security in the middle in a non-circumventable way
2. Retrofitting Security
For me everything is a service
“Crowdsourced” Development

Edge

Internet

IoT space

Store

IoT space

IoT space

IoT space

Developers

Users
1. Handling security in the middle in a non-circumventable way
Distributed Smart Space Orchestration System

VSL Middleware

- SLCA
- KA
- SLSM
- SVC

IoT Site

- KA
- NLSM

Global

- CA
- global

Service Package

- executable
- metadata
- cert

Site-Local Certificate Authority

- Site-Node Local Service Manager
- NLSM
- VSL Middleware
- Computing Node
- Middleware Interface
- Private Key
- Signature
- Service Certificate
Distributed Revocation via Short Lifetime Certificates and fully automated Renewal
Costs: Energy

![Graph showing energy costs and CPU usage over time. The graph plots input current (A) and CPU usage (%) against time from 00:00 to 30:00.](image-url)
2. Retrofitting Security
Approach in a

- Blackbox assumption
- Passive traffic monitoring
- Behavior modeling
- Anomaly detection
- Firewalling
Approach

Service Communication Monitor, Analyzer, and Firewall

μS Model Federation Service

Microservice

Inter-Node Comm. Interface

Service Runtime Environment
Who talks to whom?

Graph showing the number of edges and vertices over time with different phases labeled:
- First learning phase
- Learning phase at the addition of services
- Anomalous behavior needing user

Number of vertices and edges increase over time.
**Clustering Periodicities**

**Outgoing traffic from a washing machine service**

- **Write to battery1**
- **Read to battery1**
- **Write to battery2**
- **Read to battery2**
- **Read to thermometer**
- **Read to movement**

---

**Packet arrival**

- **All the traffic**
- **Battery read**
- **Battery write**
- **Thermometer write**
- **Movement write**

**Inter-arrival duration (s)**

- Time (s)
Quality

Classification errors over time

- False Positive
- False Negative
- Total number of packets

Service update

\[\text{anomaly value too low}\]

DoS attack

\[\text{DoS attack}\]

Time in hours

Number of classification errors

Total number of packets
Summary


Securing the Internet of Things

Marc-Oliver Pahl (TUM) | s2labs.org | pahl@tum.de