Security for the Digital Economy – An Industrial Research View

Agenda

The Digital Economy

Technology Trends and Security Challenges

An IoT Use Case

Cf. http://www.digitalistmag.com/

Agenda

The Digital Economy

Technology Trends and Security Challenges

An IoT Use Case

Technology Trends

Hyperconnectivity

Supercomputing

Cloud Computing

Smarter World

Cybersecurity

Security and Privacy Challenges

Distributed ownership and processing of data (cloud-based offers)

Limited trust is ecosystem entities and technology

Extended attack surface

Secure / privacy-friendly sharing of data (→ ecosystem)

Adequate security and privacy (no demand for “high-end” solutions if not necessary, no compromise on utility)

Every use case is different – meet individual security and privacy requirements

A Business Case for Computing on Encrypted Data?

Respond to changing threat model

Can well address requirements related to distribution, lack of trust, sharing

- Support fast adoption of digital business

Need to be tailored to the individual use case and risk assessment

- e.g., technology solution vs. SLA
- Adequate (i.e.,“good enough” and “right”) security

Pragmatic aspects are important

- Deployment
- Key Management
- Integration

Agenda

The Digital Economy

Technology Trends and Security Challenges

An IoT Use Case

Secure Predictive Maintenance @ Antibes

Monitor water distribution network, **predict** failures, and proactively **optimize their finance and controlling**

Motivation

- Connect operational levels to finance and controlling
- High resolution management
- WhatIf scenario

Technical characteristics

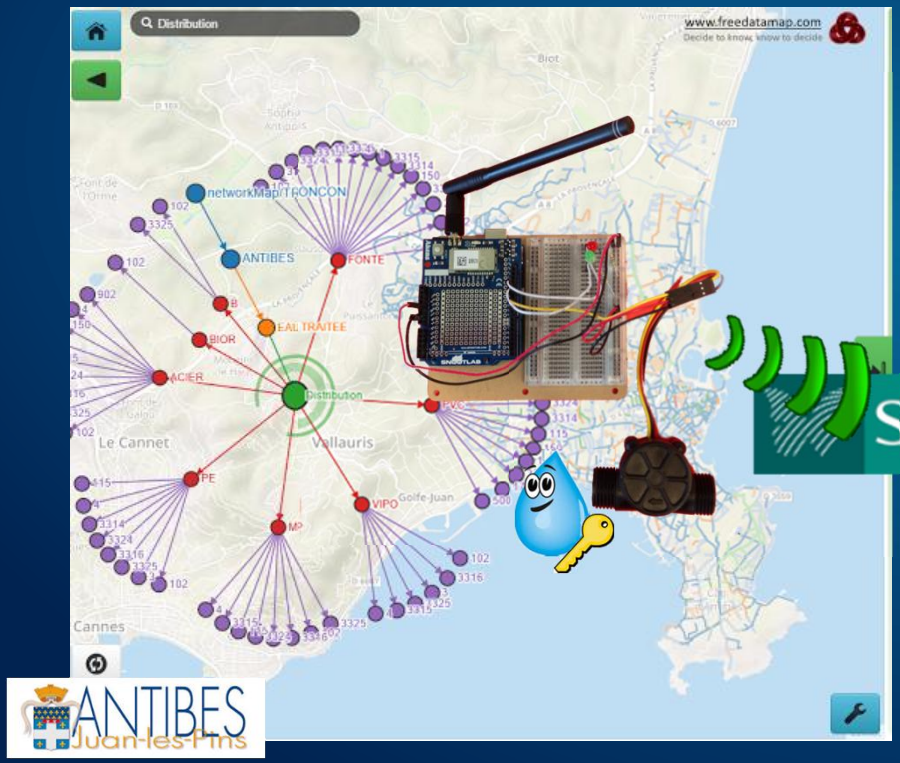
- 2000 sensors instrumenting the network
- Low bandwidth and powered PLCs
- No physical access to devices
- Low throughput
- No personal data

Security requirements expressed by Antibes

- End to end data confidentiality
- Secure alerting
- Data integrity

Data privacy is out of the scope as no personal data is manipulated

Overview



SIGFOX

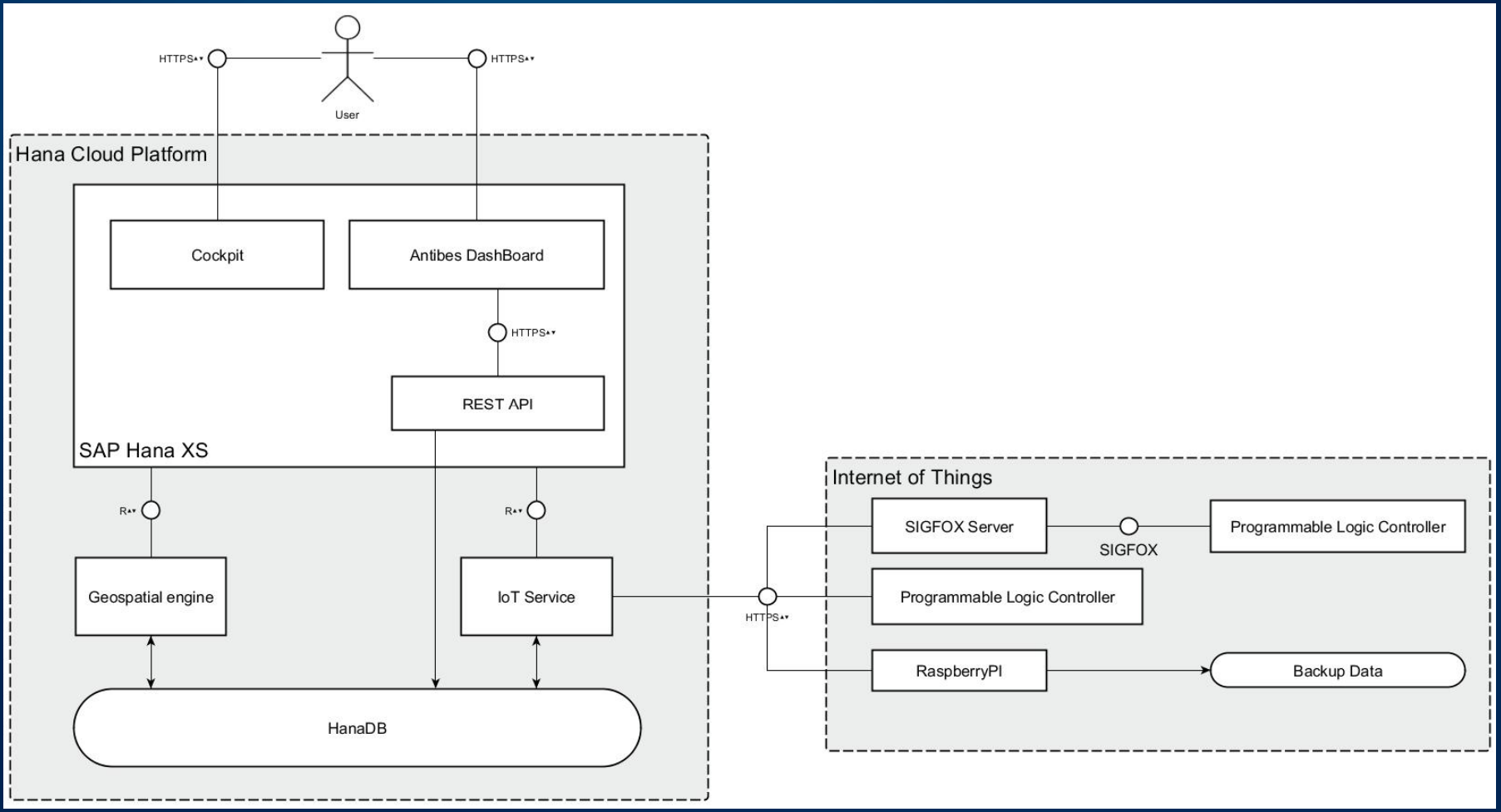
Predictive Maintenance @Antibes DashBoard

SQL MDX R JSON Open Connectivity

SAP HANA

Extended App Services (Web Server)	Java Script	HTML	OData
	Procedural App Logic		
DB Server	DB-oriented Logic		
Geospatial Engine	R Integration		
Predictive Analytics	Business Rules		
IoT Service	Application Library		
	SQL Scripts		

Architecture



Access Control to Sensor Data

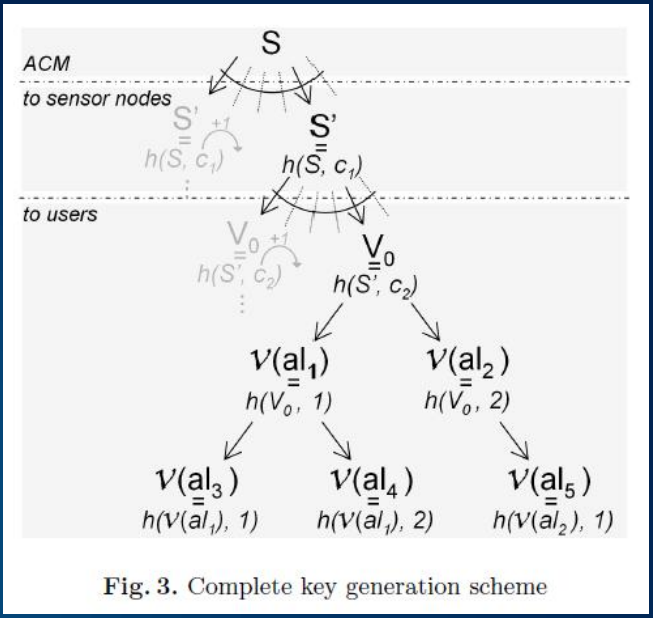


Fig. 3. Complete key generation scheme

Sensor data are encrypted from the device to the application.

Hierachical tree of symetric cryptographic keys

- One key each level
- Allowing derivation

Use of Message Authentication Codes (MAC) to create a tree of values

It is basically a bivariate hash h : {0, 1}* x {0, 1}* → {0, 1}n

for instance HMAC [Bellare96]

Encryption scheme is one-time-pad

$$K_{al_i, ID, seq} \oplus data = encrypted_{data}$$

$$K_{al_i, ID, seq} \oplus encrypted_{data} = data$$

Order Preserving Encryption

Order Preserving Encryption

$$\forall \alpha, \beta \in \mathrm{M}, \alpha \geq \beta \Leftrightarrow \varepsilon(\alpha) \geq \varepsilon(\beta)$$

Use for secure alerting

Trigger alert whenever a data value reaches a given threshold without disclosing it.

Implementation on Raspberry PI 2

Java based implementation

Reference: http://www.cc.gatech.edu/~aboldyre/papers/bclo.pdf

Thank You!

volkmar.lotz@sap.com