Measurable Security for Sensors - the Driver for Innovation

Josef Noll
Prof. at University Graduate Studies (UNIK), University of Oslo (UiO)
Chief technologist at Movation AS
Steering board member, Norway section at MobileMonday
Oslo Area, Norway
Outline

- Historical dimension
- Measurable Security
  - Application in the IoT
  - threat, goal, architecture
- Approach
  - Ontologies for security, system, component functionality
  - Metrics based assessment
  - context-aware security
- Discussion
  - Specific ontologies for each threat
  - Sensor/device standardisation
  - distributed or universal metrics
- Conclusions
• Research and Education at Kjeller

• The building where the Internet (Arpanet) came to Europe in June 1973

1971 (at which point 23 hosts, at universities and government research centers, were connected to the ARPANET); 29 by August, 1972, and 40 by September, 1973.

At that point, two satellite links, across the Pacific and Atlantic Oceans to Hawaii and Norway (NORSAR) had been added to the network. From Norway, a terrestrial circuit added an IMP in London to the growing network.
The Internet and Scandinavia

• The first connection of Arpanet outside of the USA (and Hawaii) was to **Scandinavia** (Kjeller, June 1973)

• List_of_Internet_pioneers [Wikipedia]
  – Yngvar Lundh, Paal Spilling

• Application development
  – .php, OpenSource, Linux, Skype, Spotify
  – OperaSoftware, FAST Search
  – Nokia, Ericsson
  – Telenor, TeliaSonera

• Mobile Internet:
  – GSM
  – Adaptation
Internet usage in Scandinavia

[Robert Madelin, Directorate-General for Information Society and Media, EU commission, Aug 2011]

* “use of IT in a proper way can increase effectiveness with 30-40%”
* “we are good in technology development. But access to venture capital is bad in Europe as compared to the USA”.
[Aftenposten, 3. October 2011]

The Center for Wireless Innovation Norway - CWIN.no - Enabling Collaborative Research
Internet service usage

- Private homes with broadband
  - Greece: 41
  - Norway: 83
  - EU-average: 61

- Wireless PC used outside of home
  - Greece: 3
  - Norway: 39
  - EU-average: 13

- Internet Banking
  - Greece: 6
  - Norway: 84
  - EU-average: 36

- Online contact to public services
  - Greece: 16
  - Norway: 77
  - EU-average: 41

- eCommerce - bought
  - Greece: 12
  - Norway: 71
  - EU-average: 40

2011 numbers
IoT success, more than technology

• Creating business
  – openness, competitive
  – climate for innovation

• Public authorities
  – trust, confidence
  – demand

• Consumers
  – (early) adapters
  – education

• Infrastructure
  – broadband, mobile
  – competition
IoT paradigm

• From "Internet of PCs" towards the "Internet of Things" with 50 to 100 billion devices connected to the Internet by 2020. [CERP-IoT, 03.2010]

• Things have their own identity, communicate with other things and humans (IoPTS)

"Now (2010) we have roughly 5.2 Mio mobile subscribers. In some year we will have 30...50 Mio devices on the mobile network”
– Hans Christian Haugli, CEO, Telenor Objects
The Semantic Dimension


* security
* privacy
* dependability
* context-aware
* personalised
The IoT technology and application domain
Technology applications in Maritime, Renewables & Electricity, Health Care, Oil & Gas and Food & Water industries
- sensors will drive automated data management
- from passive data to automated decisions
- automated decision tools by 2020

Maritime: «policy driven»
Health care: «trust» on sensor and mobile apps
Security challenges

- heterogeneous infrastructures
  - sensors, devices
  - networks, cloud
  - services, app stores
- Mixed infrastructures / BYOD
  - you can’t control
  - concentrate on the core values
- Internet of People, Things and Service (IoPTS)
  - content aware
  - context aware
  - user centric: “Life Management Platform”
- Measure your values, and add appropriate security
Create a successful ecosystem

- Demand
  - mobile/wireless
  - autonomy
  - “me”, context-/content-aware
- Adaptation
  - infrastructure
  - business environment
  - trust
- Security, privacy
Sensor Network Architecture

- Semantic dimension
  - Application
  - Services
  - Security, QoS,
  - Policies
  - mapping

- System
  - sensor networks
  - gateway
  - base station

Source: Compton et al., A survey of semantic specification of sensors, 2009
newSHIELD.eu approach

- Security, here
  - security (S)
  - privacy (P)
  - dependability (D)
- across the value chain
  - from sensors to services
- measurable security

Diagram:
- System
  - Components and functionalities
  - Could be composed
  - SPD Components, SPD functionalities

Intelligence Overlay
Cloud services
Network
Sensors, Embedded Systems
Traditional approach

Control type

Organisation

Control

of Type

corresponds to

implemented by

Vulnerability

has severity

mitigated by

requires

owned by

Asset/System

requires Level

Threat

threatens gives rise to

exploited by

affects

Security attribute

Threat Source

has origin

Threat Origin

Severity scale

[source: http://securityontology.sba-research.org/]
Limitations of the traditional approach

- Scalability
  - Threats
  - System
  - Vulnerability

- System of Systems
  - sensors
  - gateway
  - middleware
  - business processes

[source: http://www.securityontology.com by SBA]
The nSHIELD approach

- nSHIELD is an JU Artemis project
- focus on “measurable security” for embedded systems

Core concept
- Threat analysis
- Goal definition
- Semantic security description
- Semantic system description
- Security composability

http://newSHIELD.eu
Security description

System Components (Embedded Systems)
- memory
- sensor
- network connection
- ...

SPD Attributes

Security attributes
- availability
- confidentiality
- integrity
- reliability
- safety
- maintainability

Security/Privacy/Dependability relevant functionalities
- authentication
- encryption
- identity
- error control
- ...

System components

Security functionality
Goal description

• based on application specific goal, e.g. high reliability

• Specific parameters for each application?
  - availability = 0.8
  - confidentiality = 0.7
  - reliability = 0.5
  - ...
  - more specific
  - easier to understand

• Common approach?
  - SPD = level 4

  this way?

that way?

• universal approach
  - code “red”
Discussion - major topics

specific application ontologies? -> ontologies for security, systems, functionality

universal threat metrics? -> selection of metrics due to application?

Security attributes:
- availability
- confidentiality
- integrity
- safety
- reliability
- maintainability

Sensor/Device System description?

SensorML
SenML

Semantic Sensor Network (SSN) ontology
Conclusions

• Scandinavia has a long tradition for Internet-based developments
  – First connection, developments
  – Internet is the basis for our welfare

• Measurable Security for IoT systems
  – transferring the implicit Nordic trust to sensors
  – the basis for automated services

• Semantic representation - the SHIELD SPD methodology
  – divided into security attributes, security functionality and system description
  – Metrics based assessment

• Business Expectations
  – involving the shareholders in the value chain
  – communicating the risk based on science
My special thanks to

- JU Artemis and the Research Councils of the participating countries (IT, HE, PT, SL, NO, ES)
- Andrea Fiaschetti for the semantic middleware and ideas
- Inaki Eguia Elejabarrieta, Andrea Morgagni, Francesco Flammini, Renato Baldelli, Vincenzo Suraci for the Metrices
- Przemyslaw Osocha for running the pSHIELD project
- Cecilia Coveri (SelexElsag) for running the nSHIELD project
- Sarfraz Alam (UNIK) and Geir Harald Ingvaldsen (JBV) for the train demo
- Zahid Iqbal and Mushfiq Chowdhury for the semantics
- Hans Christian Haugli and Juan Carlos Lopez Calvet for the Shepherd ® interfaces
- and all those I have forgotten to mention