



UNIK4750 - Measurable Security for the Internet of Things

L17 – Wrap-up

György Kálmán,
Mnemonic/NTNU/UiO ITS
gyorgy.kalman@its.uio.no

Josef Noll
UiO ITS
josef.noll@its.uio.no

Exam preparation



- It is recommended to check the presentations on the wiki
- Focus on the concepts, there will be no question on googleable detail like bits in the header
- Be prepared to answer questions related to the group work, have a clear view on your contribution



Lessons learned

- ⌘ What we mean with IoT
- ⌘ Domains being addressed
 - Things
 - Semantics
 - Internet
- ⌘ Security and privacy challenges
- ⌘ Architecture components
- ⌘ Services and Ecosystem
- ⌘ Provide examples of challenges in IoT with focus on services, security and privacy
- ⌘ Analyse security and privacy requirements in an example scenario



Lessons learned

- ⌘ Converged infrastructure
- ⌘ IoT expands the attack surface
- ⌘ Security requirements do also depend on type of data processed
- ⌘ Devices with multiple interfaces present a risk
- ⌘ End-to-end security and life-cycle support is key
- ⌘ Privacy
- ⌘ Why is this all good for the user?

Lessons learned

- ⌘ Services in IoT have an implication typically in the communication and security domain of IT
- ⌘ The QoS requirements are more "hard" than in non-automation cases
- ⌘ The metrics used at OT and at IT do differ, but with some reason we can convert them
- ⌘ Big systems require a standardized, structured approach for planning infrastructure services
- ⌘ Following up requirements is important as:
 - Unnecessary requirements might lead to either not feasible projects or higher cost
 - Necessary requirements shall be taken into account (and only those)
 - Following aggregated resource usage in the infrastructure is important
- ⌘ Non-functional requirements are less typical in M2M systems

Lessons learned

- ⌘ Services in IoT have an implication typically in the communication and security domain of IT
- ⌘ Main challenge is the lack of understanding
- ⌘ Sub-challenges are life-cycle management, status monitoring, continuous evaluation of QoS
- ⌘ Don't believe in the IoT explosion?
Consider this: – How many MAC Addresses did you use in 1998?
Typically less than 5: • Work computer, home computer, a laptop. . .
Move to 2017. Now how many MAC Addresses do you use?
Typically 15 to 20: • Cell phone, IP phone, laptop (2 – 1 for wired, 1 for wireless), laser printer (2 – same reason), set top box (2), TV, tablet, computer at home (2), gaming console, thermometer, weather station, wireless AP

Lessons learned

- explain components of the Smart Grid (AMS) System of Systems
- can explain the difference between functional, non-functional and security components
- provide examples of security challenges in IoT
- explain the difference between the web, the semantic web, web services and semantic web services
- explain the core elements of the Semantic Web
- apply semantics to IoT systems
- provide an example of attribute based access control
- discuss the shortcomings of the traditional threat-based approach
- list the main elements of the semantic descriptions of s,p,d functionalities
- perform a semantic mapping of s,p,d attributes
- **Further readings**
- <https://plus.google.com/u/0/+MarcelEggum/posts/9kbGFHA972J> (about the Semantic Web)
- <http://www.slideshare.net/SergeLinckels/semantic-web-ontologies> (on Ontologies)

Lessons learned

- ⌘ Security, Privacy, and Dependability (SPD) assessment
- ⌘ Social Mobility Use-Case: loan a car
 - «behave» - full privacy awareness -> $SPD_{goal} = (s, 80, d)$
 - «speeding» - limited privacy -> $SPD_{goal} = (s, 50, d)$
 - «accident» - no privacy -> $SPD_{goal} = (s, 5, d)$
- ⌘ Configuration assessment

Lessons learned



- ⌘ Intrusion Detection is an example, where a collection of parameters will serve as an input to a fuzzy system
- ⌘ Industrial systems might be quite well suited for «sharp» heuristics
- ⌘ The main difference is the physical process back (both plus and minus)
- ⌘ Evaluation of the detection system is very much in line with the classification examples shown in previous lectures: one can define a set of metrics and analyse which level the system is can reach.



Lessons learned

- ⌘ Performed a review on security and security classes
 - ⌘ Examples: server rating, ssh security
- ⌘ Privacy and identity
 - ⌘ ongoing discussion on privacy enforcement

- ⌘ can we really draw conclusions?

Example questions

- ⌘ What are the differences between an IT infrastructure and an operational control infrastructure with respect to connectivity, network posture, security solutions, and the response to attacks?
- ⌘ What is special with security of the Internet of Things?
- ⌘ Comparing IT and automation equipment, what would you see as main difference?
- ⌘ What are the main issues in Smart Grids?
- ⌘ What do you see as main security problems for an automated meter reader?
- ⌘ Why is QoS is an important question in automation?
- ⌘ What is meant by Defence-In-Depth?
- ⌘ What is an Intrusion Detection System?

Doodle poll to exam timeslots



& <http://doodle.com/poll/bwuiuahgiebvad87>