UNIK4750 - Measurable Security for the Internet of Things

L17 – Wrap-up

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

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

http://cwi.unik.no/wiki/UNIK4750, #IoTSec, #IoTSecNO

TEK5530: Lecture plan

- 17.01 L1: Introduction
- 24.01
  - L2: Internet of Things
- 31.01
  - L3: Security of IoT + Paper list
- 07.02
  - L4: Smart Grid, Automatic Meter Readings
  - L5: Service implications on functional requirements
- 14.02
  - L6: Technology mapping
  - L9: Top 20 critical security controls
- 21.02 --- Winter holiday
  - «homework» see recording of

  L7: Practical implementation of ontologies
- 28.02
  - L8: Paper analysis with 25 min presentation
  - L10: Intrusion detection
- 07.03
  - L13: Communication and security in current industrial automation
  - L14: Cloud basics and cloud architecture
- 14.03
  - L11: Multi-Metrics Method for measurable Security
  - L12: Multi-Metrics Weighting of an AMR sub-system
- 21.03
  - L15: AWS Cloud security, Cloud monitoring, automation and incident response
  - L16: AWS IoT
- 28.03
  - L17: Wrap-up of the course ,
    Selected recent topics from IoT security
- 04.04 ---- No lecture, prepare for exam, consultation possibility
- 11.04 ---- group work presentation?
- 18.04 ---- Easter holiday, no lecture
- 25.04 ---- Exam

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

- 20% paper presentation, 20% group work, 60% exam

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
- Cloud and IoT
  - Shared responsibility
  - Cloud security

Lessons learned

- Converged infrastructure
- IoT expands the attack surface
- Security requirements do also depend on type of data processed
- Devices with multiple intefaces 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, continous evaluation of QoS
- Don't believe in the IoT explosion?
  Consider this: – How many MAC Addresses did you use in 2005?
  Typically less than 5: • Work computer, home computer, a laptop, 1-2 smart phones. . .
  Move to 2019. 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, smart lighting, smart power outlets

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 -> S**P**D$_{goal}$ = (s,**80**,d)
  - «speeding» - limited privacy -> S**P**D$_{goal}$ = (s,**50**,d)
  - «accident» - no privacy -> S**P**D$_{goal}$ = (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 analyise which level the system is can reach.

Lessons learned

- Cloud deliveries
- Shared responsibility
- Elasticity
- Challenges related to multi-tenancy
- Logging, adapting logging to technical possiblities
- Control concepts
- IoT in the cloud: processing, split of functionality
- AWS IoT value chain
- Different controls we can implement
- IAM
- AWS GreenGrass

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

- https://doodle.com/poll/ktkshxmbbq4ndthb

- Choose one slot, we might be faster than that, try to be on site 1 hour before. Please take a slot close to the others so, that we are not getting 2 hour holes in the schedule
- Mark if you are a phd student

Recent issues in IoT

- OWASP IoT Top10: https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf
- WatchOut – vulnerabilties and non-existent security in tracking-watches (2017)
- Slingshot – malware dormant for 6 years, mikrotik routers
- Alexa – recording conversations unintended
- Samsung SmartThings Hub – multiple vulnerabilities
- Robot vacuum

Watch Out

- Klokkene svikter på flere områder
- **Alvorlige sikkerhetsbrister**
  Det er mulig for uvedkommende å få tilgang på andre brukeres opplysninger (Xpora, Gator2 og Viksfjord/SeTracker-klokkene). Fremmede kan med enkle grep ta kontroll over klokkene for å spore hvor barnet beveger seg, gi inntrykk av at barnet er et annet sted eller kommunisere med barnet (Viksfjord/SeTracker-klokkene og Gator2). Personopplysninger sendes dessuten ukryptert (Gator2).
- **Falsk trygghet**
  SOS-funksjonen i Gator 2, og listen over godkjente telefonnummer i Viksfjord, er særlig dårlig implementert
- **Ulovlige og manglende vilkår**
  Enkelte av appene som er knyttet til klokkene mangler brukervilkår. Det er heller ikke mulig å slette egne data eller brukerkonto. Dette er opplagte brudd på både markedsførings- og personopplysningsloven.
- **Urimelig binding**
  Pepcall lar ikke brukere av Xplora-klokken bytte til annet telefonselskap etter 12 måneder. Det er ellers svært vanskelig å skifte SIM-kort i Gator 2, noe som gjør terskelen for å bytte operatør høy.
- https://www.mnemonic.no/no/nyheter/2017/watchout/

Slingshot – mikrotik routers

- Was dormant for 6 years!
- Slingshot would load a number of modules onto the victim device, including two huge and powerful ones: Cahnadr, the kernel mode module, and GollumApp, a user mode module. The two modules are connected and able to support each other in information gathering, persistence and data exfiltration.
- The most sophisticated module is GollumApp. This contains nearly 1,500 user-code functions and provides most of the above described routines for persistence, file system control and C&C communications.
- Canhadr, also known as NDriver, contains low-level routines for network, IO operations and so on. Its kernel-mode program is able to execute malicious code without crashing the whole file system or causing Blue Screen - a remarkable achievement. Written in pure C language, Canhadr/Ndriver provides full access to the hard drive and operating memory despite device security restrictions, and carries out integrity control of various system components to avoid debugging and security detection.
- https://securelist.com/apt-slingshot/84312/

Alexa spying

- A chain of events led to Alexa sending a record of a conversation to a person in the contact list
- https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974
- *"Echo woke up due to a word in background conversation sounding like 'Alexa.' Then, the subsequent conversation was heard as a "send message" request. At which point, Alexa said out loud 'To whom?' At which point, the background conversation was interpreted as a name in the customer's contact list. Alexa then asked out loud, '[contact name], right?' Alexa then interpreted background conversation as 'right.' As unlikely as this string of events is, we are evaluating options to make this case even less likely."*

Samsung SmartThings Hub

- https://internetofbusiness.com/iot-security-vulnerabilities-samsung-smart-things-hub/
- Cisco Talos:discovered firmware vulnerabilities that made it possible for an attacker to take control of the Hub and, by extension, access sensitive information, monitor and control devices within the home, and perform other unauthorised activities – with potentially devastating consequences.
- using the exploit, smart locks under the control of the SmartThings Hub could be unlocked
- Security systems could also be disabled, including motion sensors and smoke detectors.

Robot vacuum

- https://threatpost.com/iot-robot-vacuum-vulnerabilities-let-hackers-spy-on-victims/134179/
- The first bug (CVE-2018-10987) is a remote code execution issue that resides in the REQUEST_SET_WIFIPASSWD function (UDP command 153) of the vacuum.
- “This vulnerability allows attackers to obtain superuser rights on the vacuum, meaning they can control it remotely, viewing video and images, and physically moving the vacuum,” Galloway told Threatpost. “It can also be used in a botnet for DDoS attacks or for bitcoin mining.”
- An attacker can discover the vacuum on the network by obtaining its media access control (MAC) address – an unique identifier assigned for communications at the data link layer of a network.
- They can then send a specially-crafted user datagram communications protocol (UDP) request, which results in execution of a command with superuser rights on the vacuum. A crafted UDP packet runs “/mnt/skyeye/mode_switch.sh %s” with an attacker controlling the %s variable.
- “To succeed, the attacker must authenticate on the device—which is made easier by the fact that many affected devices have the default username and password combination (admin:888888),” researchers said.
- A second vulnerability (CVE-2018-10988) would also allow superuser rights, but additionally, could enable crooks to steal unencrypted data, including photos, video and emails, sent from other devices on the same Wi-Fi network.