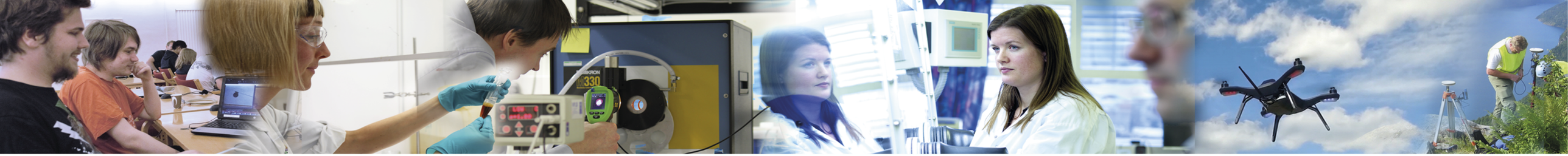

UiO : Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L15 – Recent topics and rehearsal

György Kálmán,
UiO
gyorgy.kalman@its.uio.no

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

https://its-wiki.no/wiki/TEK5530

TEK5530: Lecture plan

- **21.01**
  - L1: Introduction (Josef Noll)
  - L2: Internet of Things (Josef Noll)
- 28.01 (Gyorgy Kalman)
  - L3: Security of IoT + Paper list
  - L4: Smart Grid, Automatic Meter Readings
- 04.02 (Josef Noll)
  - L5: Practical implementation of ontologies
  - L6: Multi-Metrics Method for measurable Security
- 11.02 (Josef Noll)
  - L7: Multi-metrics
  - L8: System Security and Privacy Analysis
- 18.02 (Josef Noll, Gyorgy Kalman)
  - L9: Paper analysis with 25 min presentation
  - L10: Security Controls
- 25.02 (Gyorgy Kalman)
  - L11: Communication in Smart grid, home and IoT
  - L12: Intrusion Detection Systems
- 04.03 (Gyorgy Kalman)
  - L13: Cloud Basics
  - L14: Cloud security and IoT
- **11.03**
  - **L15: Selected recent topics from IoT security**
  - **Rehearsal**
- 25.03
  - Exam

Recent topics in IoT

- SolarWinds
- Oldsmar water treatment plant
- SSA-541017: Embedded TCP/IP Stack Vulnerabilities
- SweynTooth Bluetooth Low Energy
- Outofcontrol

SunBurst – attack on SolarWinds

- Supply chain attack
- SolarWinds is a leading supplier of network management solutions
- Backdoor in the IT management product Orion.
- Source code directly modified and patch distributed through usual distribution channels
- Sophisticated coding with code placed in right context, matching coding and naming style
- Supernova, one of the malicious components associated with the attack, is a .NET web shell backdoor that presents itself as a legitimate SolarWinds web service handler. It is a second-stage payload in the attack.

- https://www.solarwinds.com/solutions/orion
- https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/
- https://e24.no/teknologi/i/9O6P7l/norske-kraftselskaper-beroert-av-solarwinds-hacking
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/additional-analysis-into-the-sunburst-backdoor/

SunBurst – attack on SolarWinds

- Kaspersky's recommendations for possible victims of the SolarWinds compromise:
- Check whether backdoored SolarWinds versions are installed. Known affected versions include software builds 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF1.
- Check for known indicators of compromise (IOCs). CISA has published Alert AA20-35A with an extensive list
- If you have detected a compromised SolarWinds installation or related IOCs, initiate a security incident investigation and launch an incident response procedure, considering all possible attack vectors:
  - Isolate assets that are known to be compromised, while keeping the system operable
  - Prevent IOCs that could be useful for the investigation from being deleted
  - Check all network logs for suspicious network activity
  - Check system logs and journals for illegitimate user account authentication
  - Locate suspicious process activity, investigate memory dumps and associated files
  - Check historical command-line data associated with suspicious activity

Oldsmar water treatment plant

- Attack on water treatment plant to change amount of chemicals in the water
- Used TeamViewer
- Detected by onsite operator
- Additional defenses were in place to limit chemical level

- https://threatpost.com/florida-water-plant-hack-credentials-breach/
- https://us-cert.cisa.gov/ncas/alerts/aa21-042a
- https://ics-cert.kaspersky.com/reports/2020/11/05/attacks-on-industrial-enterprises-using-rms-and-teamviewer-new-data/
- https://www.aftenposten.no/oslo/i/RRard/klorutslipp-har-utradert-livet-i-akerselva

SSA-541017: Embedded TCP/IP Stack Vulnerabilities

- 33 vulnerabilities in several open-source TCP/IP stacks for embedded devices, also known as “AMNESIA:33”
- Remote code execution (RCE) to take control of a target device
- Denial of service (DoS) to impair functionality and impact business operations
- Information leak (Infoleak) to acquire potentially sensitive information
- DNS cache poisoning to point a device to a malicious website

- https://www.forescout.com/research-labs/amnesia33/
- https://www.forescout.com/company/resources/amnesia33-identify-and-mitigate-the-risk-from-vulnerabilities-lurking-in-millions-of-iot-ot-and-it-devices/
- https://cert-portal.siemens.com/productcert/pdf/ssa-541017.pdf

SweynTooth Bluetooth Low Energy

- multiple Bluetooth Low Energy (BLE) vulnerabilities with proof-of-concept (PoC) exploit code affecting a large number of IOT, Smart-home, wearable, and medical devices
- The vulnerabilities expose flaws in specific BLE SoC implementations that allow an attacker in radio range to trigger deadlocks, crashes, buffer overflows, or the complete bypass of security.

- https://asset-group.github.io/disclosures/sweyntooth/
- https://us-cert.cisa.gov/ics/alerts/ics-alert-20-063-01

Type	*Vulnerability Name*	*Affected Vendors*	*CVE*
Crash	Link Layer Length Overflow	Cypress NXP	CVE-2019-16336 (6.1) CVE-2019-17519 (6.1)
	Truncated L2CAP	Dialog Semiconductors	CVE-2019-17517 (6.3)
	Silent Length Overflow	Dialog Semiconductors	CVE-2019-17518 (6.4)
	Public Key Crash	Texas Instruments	CVE-2019-17520 (6.6)
	Invalid L2CAP Fragment	Microchip	CVE-2019-19195 (6.8)
	Key Size Overflow	Telink Semiconductor	CVE-2019-19196 (6.9)
	Invalid Sequence Memory Corruption	Zephyr Project	CVE-2020-10061 (6.13)
	Invalid Channel Map	Zephyr Project Espressif Systems	CVE-2020-10069 (6.14) CVE-2020-13594 (6.14)
Deadlock	LLID Deadlock	Cypress NXP	CVE-2019-17061 (6.2) CVE-2019-17060 (6.2)
	Sequential ATT Deadlock	STMicroelectronics	CVE-2019-19192 (6.7)
	Invalid Connection Request	Texas Instruments	CVE-2019-19193 (6.5)
	HCI Desync	Espressif Systems	CVE-2020-13595 (6.12)
	Invalid Channel Map*	Microchip ON Semiconductor	CVE-2020-13594 (6.14) CVE-2020-13594 (6.14)
Security Bypass	Zero LTK Installation	Telink Semiconductor ON Semiconductor	CVE-2019-19194 (6.10) CVE-2019-19194 (6.10)
	DHCheck Skip	Texas Instruments ON Semiconductor	CVE-2020-13593 (6.11) CVE-2020-13593 (6.11)

outofcontrol

- The ten apps were observed communicating with at least 135 distinct third-party companies involved in advertising and/or behavioural profiling
- The Android advertising ID, which allows advertisers to track a specific device across different services, was transferred to at least 45 different third parties involved in advertising and/or behavioural profiling. All of the apps shared the advertising ID with multiple third parties, and all except one shared additional data.
- Additional data sharing included elements such as exact GPS location, IP address, device information, and personal attributes including gender and age.

- https://www.forbrukerradet.no/out-of-control/
- https://www.mnemonic.no/news/2020/out-of-control/

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
- See the TEK5530 wiki for info on the exam

  Part 1: Present your group-work (8 min) - *assessment of Security Classes for IoT* or *Applying Multi-metrics Method*

  Part 2: Questions to group work (7 min)

  Part 3: Random questions from the lectures (10 min). **Media:TEK5530_List_of_Questions_2021.pdf** (*you will pick 3-5 questions*)

Lessons learned

- What we mean with IoT
- Domains being addressed
  - Things
  - Semantics
  - Internet
- Security and privacy challenges
- Smart Grid and AMS
- 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

- 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?

- 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
- life-cycle management, status monitoring, continous evaluation of QoS

- 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

- Present features and usability of the MS Threat Modeling tool

- 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

- 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.

- 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, device shadow
- Different controls we can implement
- IAM
- AWS GreenGrass

Example questions

see all at: https://its-wiki.no/images/7/73/TEK5530_List_of_Questions_2021.pdf

- 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?