



TEK5530 - Measurable Security for the Internet of Things

L10– Intrusion Detection

*György Kálmán,
DNB/UiO ITS*

gyorgy.kalman@its.uio.no

*Josef Noll
UiO ITS*

josef.noll@its.uio.no

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: Cloud security, IoT and service examples from AWS
 - L16: Cloud monitoring, automation and incident response
- 🔗 28.03
 - L17: Selected recent topics from IoT security
 - L18: Wrap-up of the course
- 🔗 04.04 ---- No lecture, prepare for exam, consultation possibility
- 🔗 11.04 ---- No lecture, prepare for exam, consultation possibility or Exam (depending on what we agree on)
- 🔗 18.04 ---- Easter holiday, no lecture
- 🔗 25.04 ---- Exam

Intrusion Detection and Prevention

- ⌘ What is an Intrusion Detection System
- ⌘ Flavours of IDS
- ⌘ Industrial case
 - Comparison to generic cases
 - Physical process and safety
- ⌘ Industrial examples
- ⌘ Conclusion

Definitions – as requested – both definitions by ISACA

- ⌘ Information security: "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)
- ⌘ Privacy: The rights of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived
- ⌘ I think, both security and privacy is easier to see from the other way around:
 - ⌘ Compromised security and privacy.
 - ⌘ If you loose information security: then you loose confidentiality of important data or the possibility to check its integrity or just can't access it.
 - ⌘ Same with privacy: if you loose it, then you can not control any more what is happening with private information

What is an Intrusion Detection System

- ⌘ This is a practical example on fuzzy evaluation of different criteria and taking decisions by evaluating multi-dimension problems
- ⌘ What is an intrusion: an attempt to break or misuse the system
- ⌘ Might be internal or external source and can be physical, system or remote
- ⌘ It is typically a set of entities distributed in the network and monitoring some network parameters

How an intrusion works

- ⌘ Exploit different programming errors (e.g.: buffer overflow, no input validation)
- ⌘ Unexpected input (e.g.: tamper with TCP checksum, fragmentation)
- ⌘ Combination with creating special circumstances
- ⌘ IDS need a baseline to work properly
- ⌘ Baseline creation very much depends on the use
- ⌘ We always assume, that they who attack behave differently

IDS flavours

⌘ IDS can be based on:

- Anomaly detection (heuristics) – challenge is good training and right set of sensitivity
- Signature-based – challenge is to deal with new attacks
- Typically we use a combination

⌘ Or by location:

- Host-based: the host os or application is running the logging, no additional hardware
- Network-based: filters traffic, independent of clients

IDS in industrial environments

- ⌘ Two important factors: much more clean traffic baseline is possible and relation to physical process and safety
- ⌘ We can't design a system to be secure forever – count with failure: fail-safe, fail-operational, graceful state changes
- ⌘ Tamper detection and evidence
- ⌘ The only difference between systems that can fail and systems that cannot possibly fail is that, when the latter actually fail, they fail in a totally devastating and unforeseen manner that is usually also impossible to repair(1)
- ⌘ In an industrial environment the assumption that attackers will behave differently is not necessarily true

IDS in industrial environments

- ⌘ IDS is a system: evaluation of logs, evaluation of network traffic, maintenance on firewall and IDS infrastructure (software+taps)
- ⌘ Getting a reaction is actually easier in the industrial environment: typical to have 24 hours staffing somewhere, also physical security and safety
- ⌘ Challenges with shared infrastructure and suppliers
- ⌘ Possible approach: whitelisting, stateful payload analysis (operational envelope)

Example rules

⌘ There are different ways, but take this snort rule as an example:

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 \  
  (content:"|00 01 86 a5|"; msg:"external mountd access");
```

⌘ Dynamic rule example (both examples are from the snort manual):

```
activate tcp !$HOME_NET any -> $HOME_NET 143 (flags:PA; \  
  content:"|E8C0FFFFFF|/bin"; activates:1; \  
  msg:"IMAP buffer overflow!");  
dynamic tcp !$HOME_NET any -> $HOME_NET 143 (activated_by:1; count:50;)
```

Industrial attacks

- ⌘ No difference here: injection, man-in-the-middle, replay etc.
- ⌘ Long life, high utilization of equipment and legacy support open for more attacks than in an office case
- ⌘ SCADA compared to DCS/PCS
- ⌘ Resilience and restoration
- ⌘ Because of the use of COTS products, you actually might use the very same exploits, like windows on HMI

Industrial examples, from ICS-CERT (6)

Davis-Besse Nuclear Power Plant [2003]

- ✧ The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant
- ✧ Disabled a safety monitoring system for nearly five hours
- ✧ Power plant was protected by a firewall
- ✧ In 1998 the same plant was hit by a tornado (natural disaster)

Industrial examples, from ICS-CERT (6)

Maroochy Shire Sewage Spill [2000]

- ✧ First recorded instance of an intruder that “deliberately used a digital control system to attack public infrastructure”
- ✧ Software on his laptop identified him as “Pumping Station 4” and after suppressing alarms controlled 300 SCADA nodes
- ✧ Disgruntled engineer in Queensland, Australia sought to win the contract to clean up the very pollution he was causing
- ✧ He made 46 separate attacks, releasing hundreds of thousands of gallons (264,000) of raw sewage into public waterways

Industrial examples, from ICS-CERT (6)

CSX Train Signaling System [2003]

- ❧ Sobig virus blamed for shutting down train signaling systems throughout the east coast of the U.S.
- ❧ Virus infected Florida HQ shutting down signaling, dispatching, and other systems
- ❧ Long-distance trains were delayed between four and six hours

Conclusions on Intrusion Detection



- ⌘ 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.



References - Classification

- ⌘ Cybersecurity classes:
http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf
- ⌘ IAEA: Computer Security at Nuclear Facilities: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf
- ⌘ Red Tiger Security: mapping security controls to standards:
<http://redtigersecurity.com/services/scadaics-security-consulting/scada-security-maturity-model/>
- ⌘ Standards for Security Categorization of Federal Information and Information Systems, <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

References – Intrusion Detection



1. <https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Zanero.pdf>
2. <http://www.digitalbond.com/tools/quickdraw/>
3. <https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127>
4. <http://commons.erau.edu/cgi/viewcontent.cgi?article=1071&context=discovery-day>
5. https://www.truststc.org/conferences/10/CPSWeek/papers/scs1_paper_8.pdf

