UiO : Department of Technology Systems
University of Oslo

**TEK5530 - Measurable Security for the Internet of Things**

# L12 – Intrusion Detection

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

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

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

# 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

# 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
- Distributed IDS e.g. AIProtection by Asus (TrendMicro)

# 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 necessarely 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 rule

- 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";)
```

# 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 then 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
  - → See the Hydro ransomware case

# Industrial examples, from ICS-CERT

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

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

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 analyise which level the system is can reach.