UT DALLAS

Network Monitoring on Industrial Control Systems

Alvaro Cardenas, PhD.

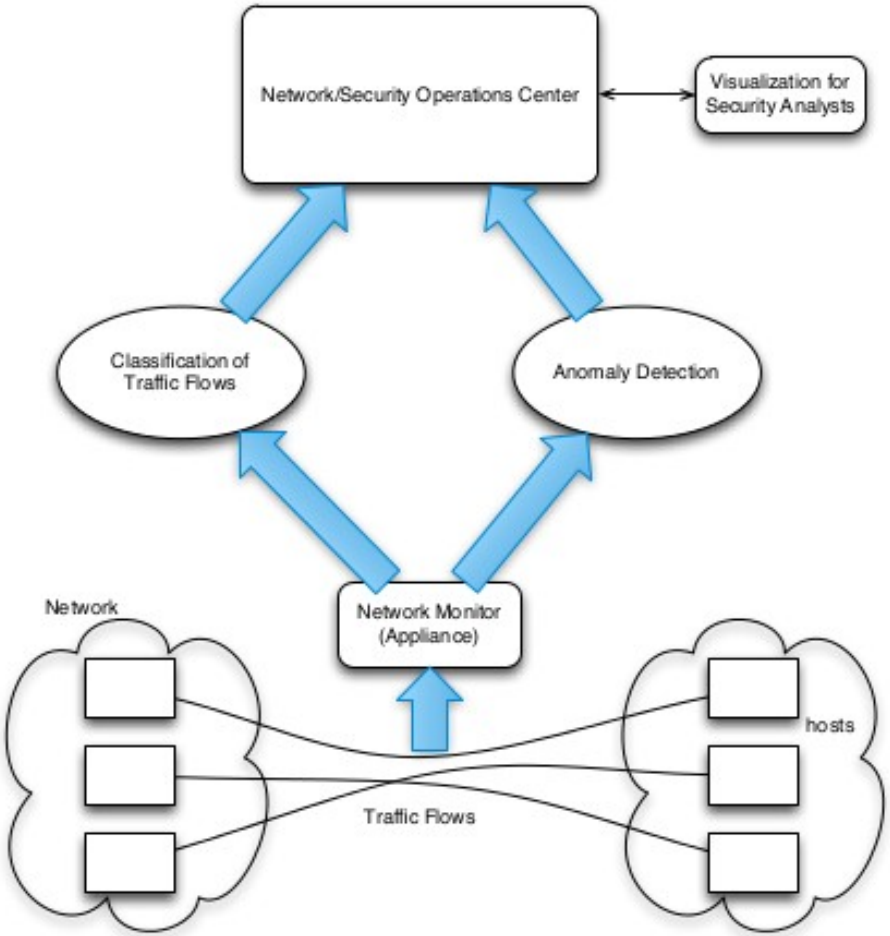
David I Urbina, PhD. candidate

- Introduction of NSM
- Long term goals
- Current Research
  - ICS Traffic Analysis
  - Intrusion Detection
- Some Tools for NSM

Network Security Monitoring *is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions.*

-Informit

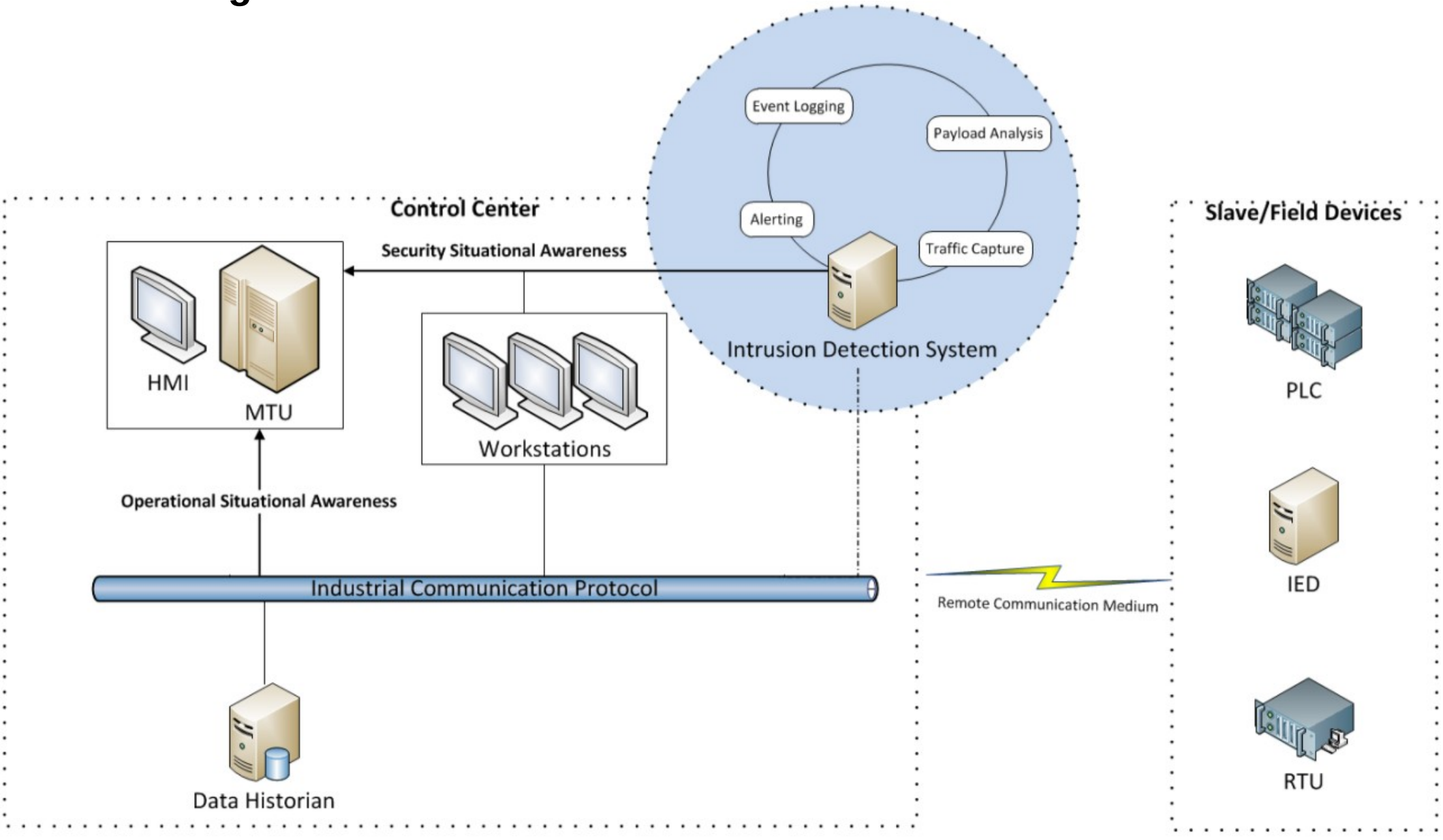
Network Security Monitoring in ICS



Long term goals

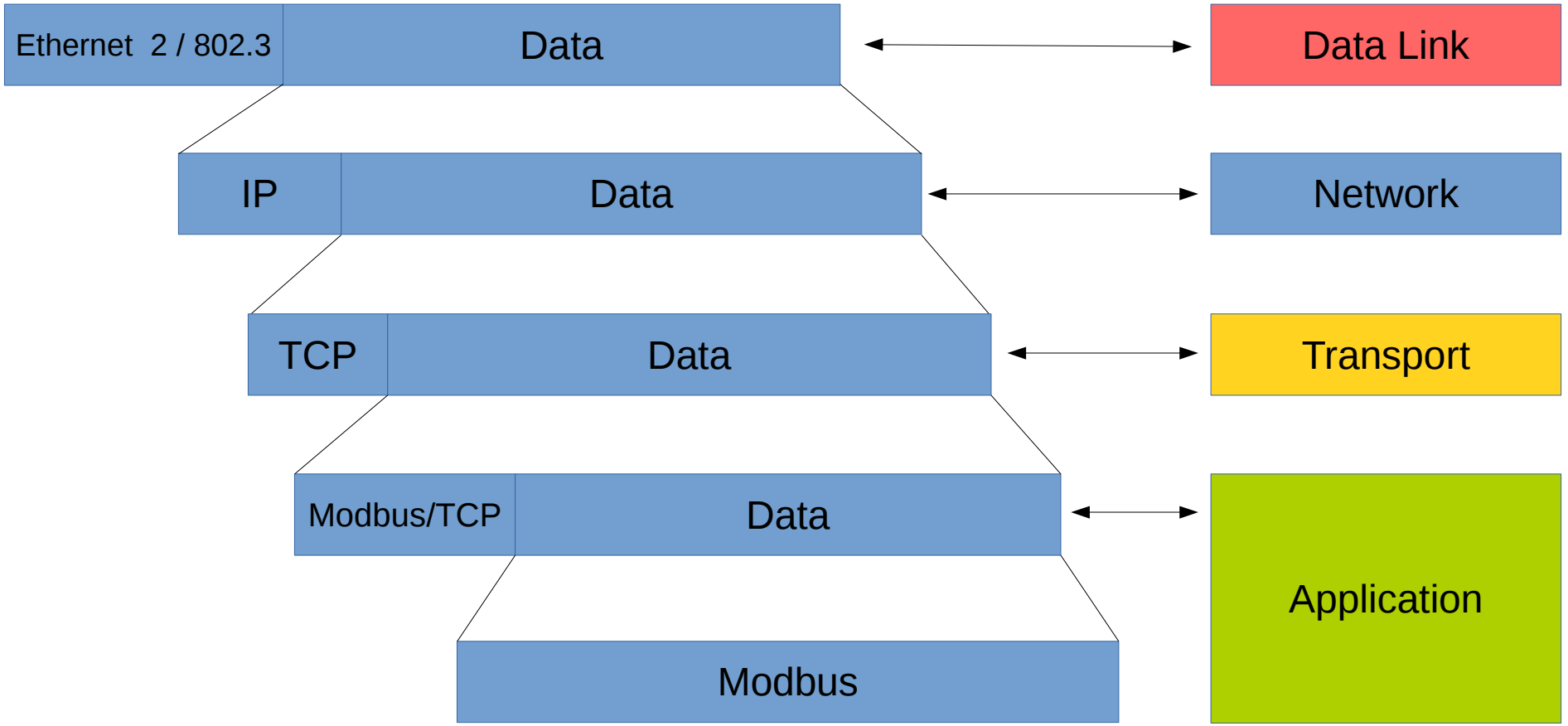
- Improve Operational Situational Awareness (OSA).
- Improve Security Situational Awareness (SSA).
- Integrate OSA and SSA into the Control Centers.

Integration OSA and SSA in ICS



Traffic Analysis

Dissecting Modbus Packets



Modbus/TCP

```
###[ Ethernet ]###
  dst= 00:0d:8d:00:91:0f
  src= 84:2b:2b:65:96:47
  type= 0x800
###[ IP ]###
     version= 4L
     ihl= 5L
     tos= 0x0
     len= 52
     id= 58399
     flags= DF
     frag= 0L
     ttl= 128
     proto= tcp
     chksum= 0xb8ba
     src= 172.16.2.34
     dst= 172.16.3.167
     \options\
###[ TCP ]###
        sport= 64248
        dport= 502
        seq= 2535847098
        ack= 331910864
        dataofs= 5L
        reserved= 0L
        flags= PA
        window= 64400
        chksum= 0xeed
        urgptr= 0
        options= []
###[ MODBUS/TCP ]###
           trans_id= 0x190f
           proto_id= 0x0
           len= 0x6
           unit_id= 0x0
###[ Modbus Request ]###
              fcode= Read Holding Registers
              start_addr= 0x2d7
              nreg= 0x2
```

```
###[ Ethernet ]###
  dst= 84:2b:2b:65:96:47
  src= 00:0d:8d:00:91:0f
  type= 0x800
###[ IP ]###
     version= 4L
     ihl= 5L
     tos= 0x0
     len= 53
     id= 33703
     flags=
     frag= 0L
     ttl= 254
     proto= tcp
     chksum= 0xdb31
     src= 172.16.3.167
     dst= 172.16.2.34
     \options\
###[ TCP ]###
        sport= 502
        dport= 64248
        seq= 331910864
        ack= 2535847110
        dataofs= 5L
        reserved= 0L
        flags= PA
        window= 2048
        chksum= 0x8108
        urgptr= 0
        options= []
###[ MODBUS/TCP ]###
           trans_id= 0x190f
           proto_id= 0x0
           len= 0x7
           unit_id= 0x0
###[ Modbus Response ]###
              fcode= Read Holding Registers
              nbyte= 4
              rvals= [16512, 0]
```

Intrusion Detection

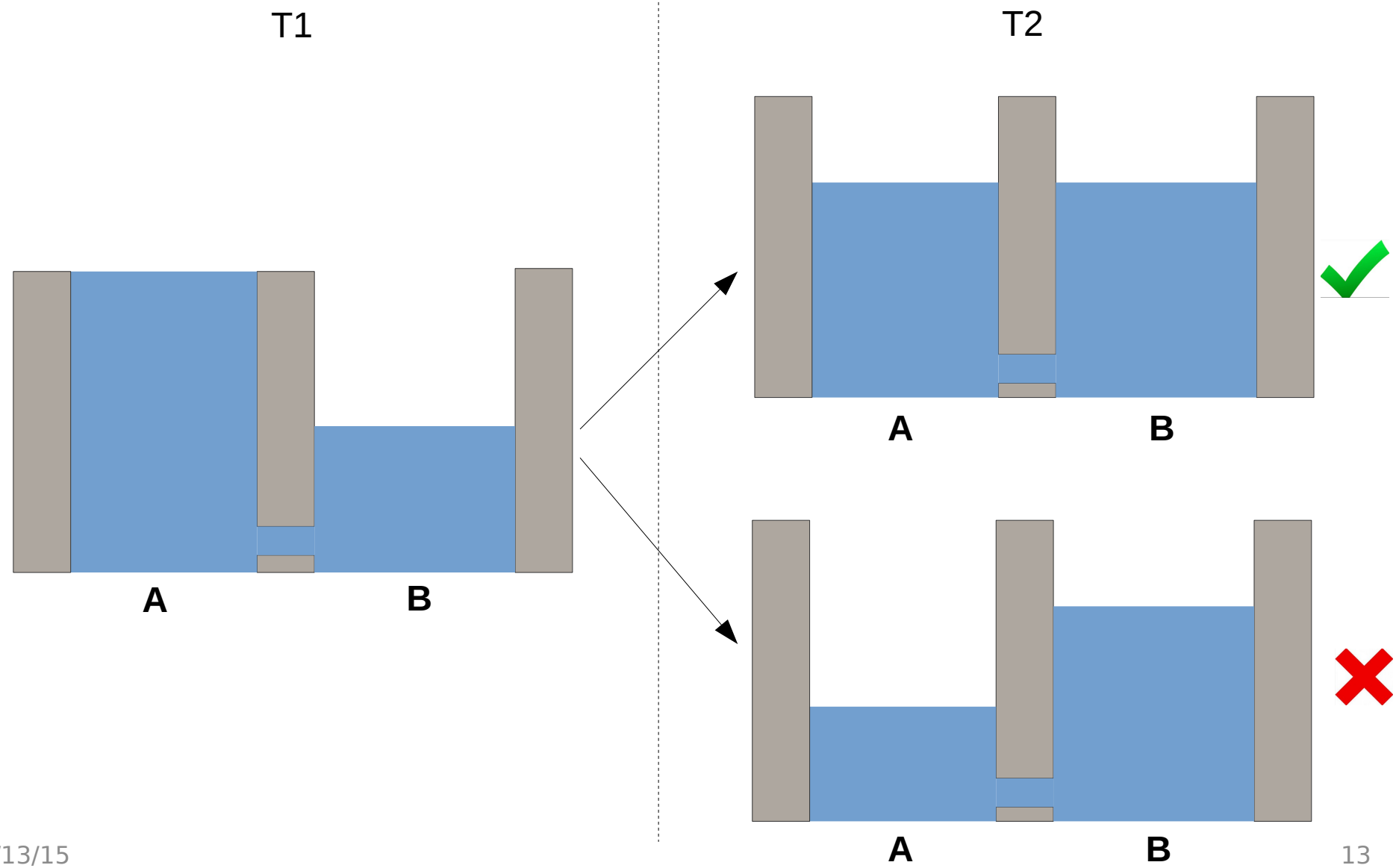
Detection methods:

- *Knowledge-based intrusion-detection* techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. **(IT)**
- *Behavior-based intrusion-detection* techniques assume that an intrusion can be detected by observing a deviation from the normal or expected behavior of the system or the users. **(ICS)**

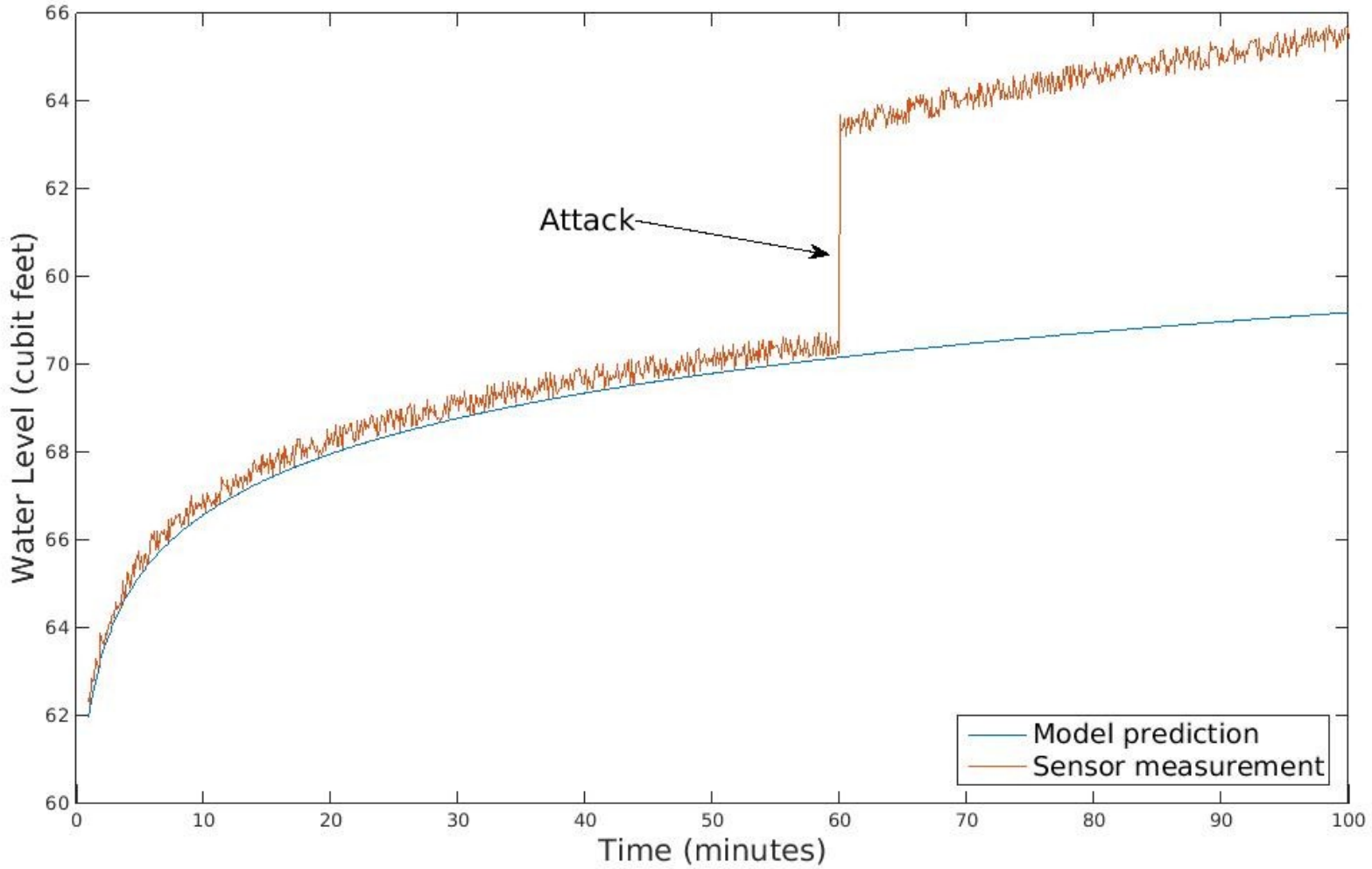
Detection methods:

- *Knowledge-based intrusion-detection* techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. **(IT)**
- *Behavior-based intrusion-detection* techniques assume that an intrusion can be detected by observing a deviation from the normal or expected behavior of the system or the users. **(ICS)**

Law Abiding "Behavior"



Using models to detect deviations



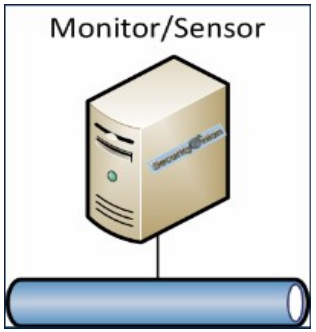
Which tools do we use?

- Ubuntu-based Linux distribution for NSM.
- Free and open source *GNU GPL v2*

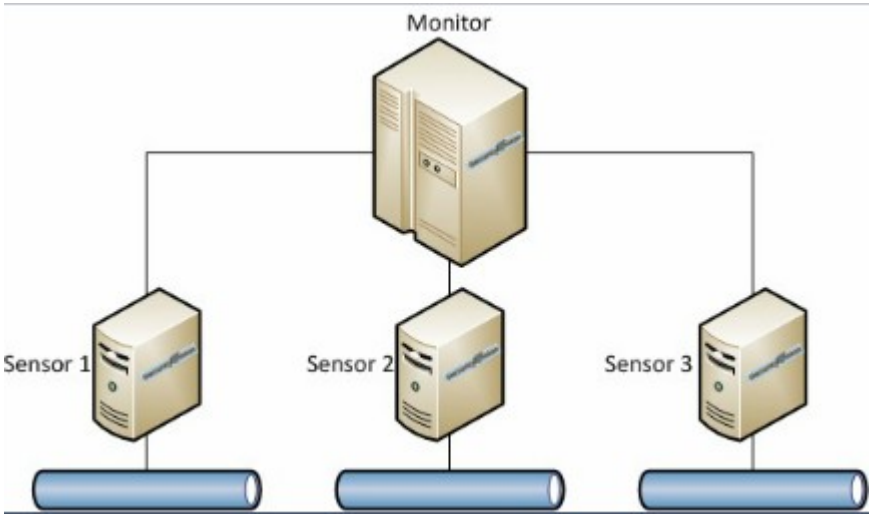
- Helps on:
  - Deep Packet Inspection
  - Protocol Analysis
  - Traffic Analysis
  - Intrusion Detection and Prevention

Deployment scenarios

- Standalone



- Server-sensor



- Core functions
  - Full packet capture → netsniff-ng (http://netsniff-ng.com)
  - Network-based IDS
    - Snort (http://snort.org)
    - Suricata (http://suricata-ids.org)
    - Bro (http://bro-ids.org)
  - Host-based IDS
    - OSSEC (http://www.ossec.net)
  - Analysis Tools
    - Sguil (http://sguild.sourceforge.net)
    - Squert (http://www.squertproject.org/)
    - Snorby (https://snorby.org/)
    - ELSA (https://code.google.com/p/enterprise-log-search-and-archive/)

Bro

Extensible network analysis framework not restricted to any particular detection approach.

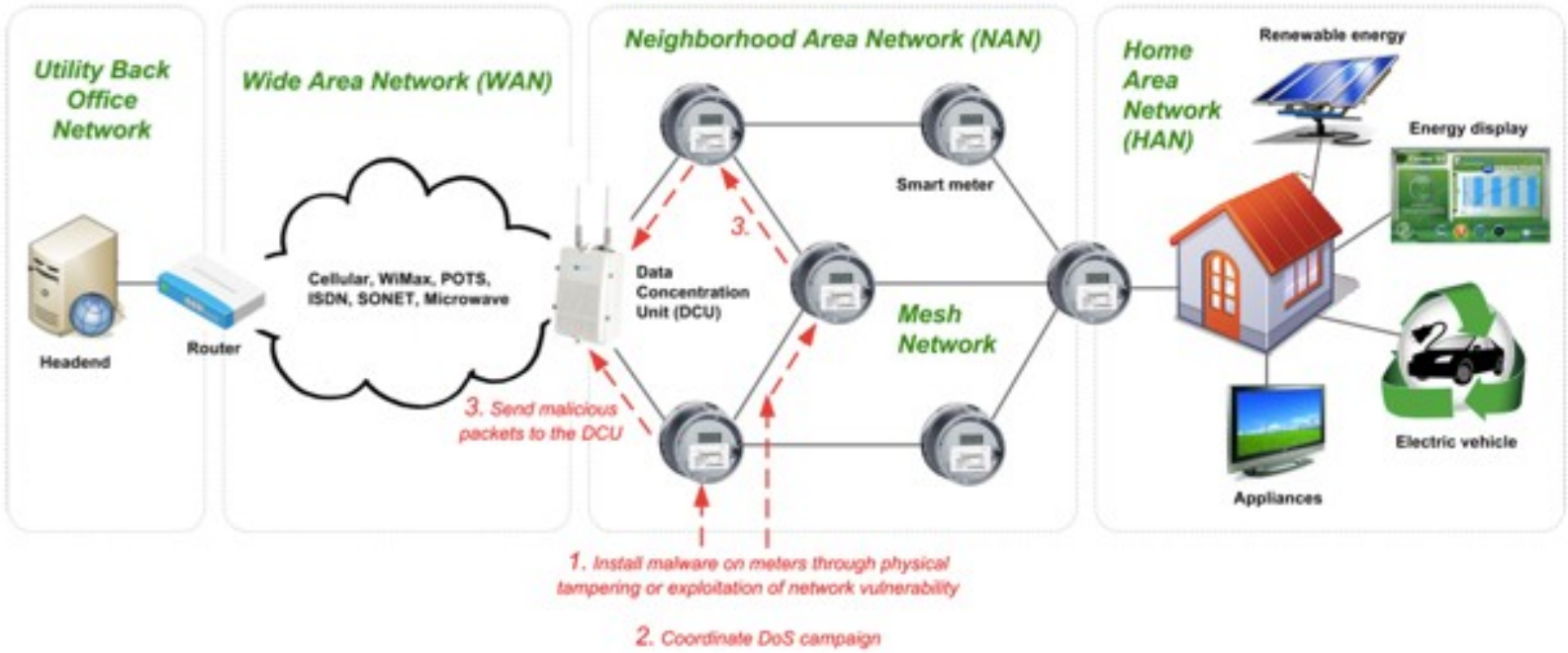
- Free and Open Source

Bro features

- Logging framework
- Multiple Traffic Analyzers for IT and ICS protocols
- Extensible Analysis Architecture
- Domain-specific, Turing complete Scripting language

Previous related research

- Analysis of Encrypted Traffic
  - Best Paper Award, "On the Practicality of Detecting Anomalies with Encrypted Traffic in AMI", IEEE SmartGridComm, 2014.



Thanks!