Chuck McParland

& Sean Peisert

Lawrence Berkeley National Laboratory

Application of Computer Security Techniques in the Protection of Efficient Cyber-Physical Energy Generation Systems

Cybersecurity for Energy Delivery Systems Peer Review

July 24-26, 2012

Summary: Application of Computer Security Techniques in the Protection of Efficient Cyber-Physical Energy Generation Systems

- **Objective**
  - Develop the ability to prevent commands sequences from being issued to cyber-physical devices that would direct them to perform unexpectedly and/or exceed their physical limitations
- **Technical Approach**
  - Using real control system data, analyzing protocols used and devices controlled to determine initial specifications and monitor how commands adhere to these. Over time, expand this model to larger systems, using bounded device simulations

BERKELEY LAB

- **Schedule**
  - 1Q & 2Q FY12 met, Q3 on track
- **Performers:** LBNL
- **Partners:** Discussions with Energy Distribution Design (EDD Blacksburg, VA)

Technical Approach and Feasibility

- **Approach**
  - *Device* safety typically implemented at hardware level (SCADA PLC, etc.). *System* operations safety performed at control center level (GUI, operations policy). These layers/elements typically connected by vulnerable comm. layer (public/private IP networks).
  - Our approach seeks to secure this gap by combining low-level monitoring of command sequences with sufficient awareness of physical device limitations to ensure overall safe system operation.
  - This additional security layer will provide enhanced protection from *outsider* attacks and *insider* mistakes.

Technical Approach and Feasibility

- **Approach (cont.)**
  - Collect command and monitoring streams from facility-wide energy control system.
  - Create simplified computer models to help illuminate key physical constraints not derivable from traffic analysis.
  - Develop specifications of permissible device commands and combine with physical constraints (temp., RPM, etc.) – including system-level *inherited* constraints.
  - Apply above specifications to observed network command streams to study effectiveness in identifying intrusions or incorrect command sequences.

Technical Approach and Feasibility

- **Challenges to Success**
  - Acquiring Data at Site
    - Limited/fragmented knowledge of data semantics and collection paths and data access logistics
    - In absence of exceptions, only viewing *normal* operations
    - Exploring options for using simulations
  - Lack of System–level Architectural Knowledge
    - Lack of system documentation by vendors
    - Continuing IT/process control cultural differences at site
  - Lack of suitable hardware/software test beds
    - Risks of *in vivo* testing
    - Limited simulation framework alternatives

Progress to Date

- **Major Accomplishments**
  - Extensive Wireshark sniffing of control network.
  - Derived and verified network topology map through onsite inspection, Wireshark logs and interviews
  - Initial correlation analysis of observed measurement data performed
    - Can be used to define tests for anomaly detection
- **Actual Progress**
  - Delayed start due to change in collaboration partner
  - Map network and interactions between control systems, databases, PLCs, etc….*i.e. reverse engineering*

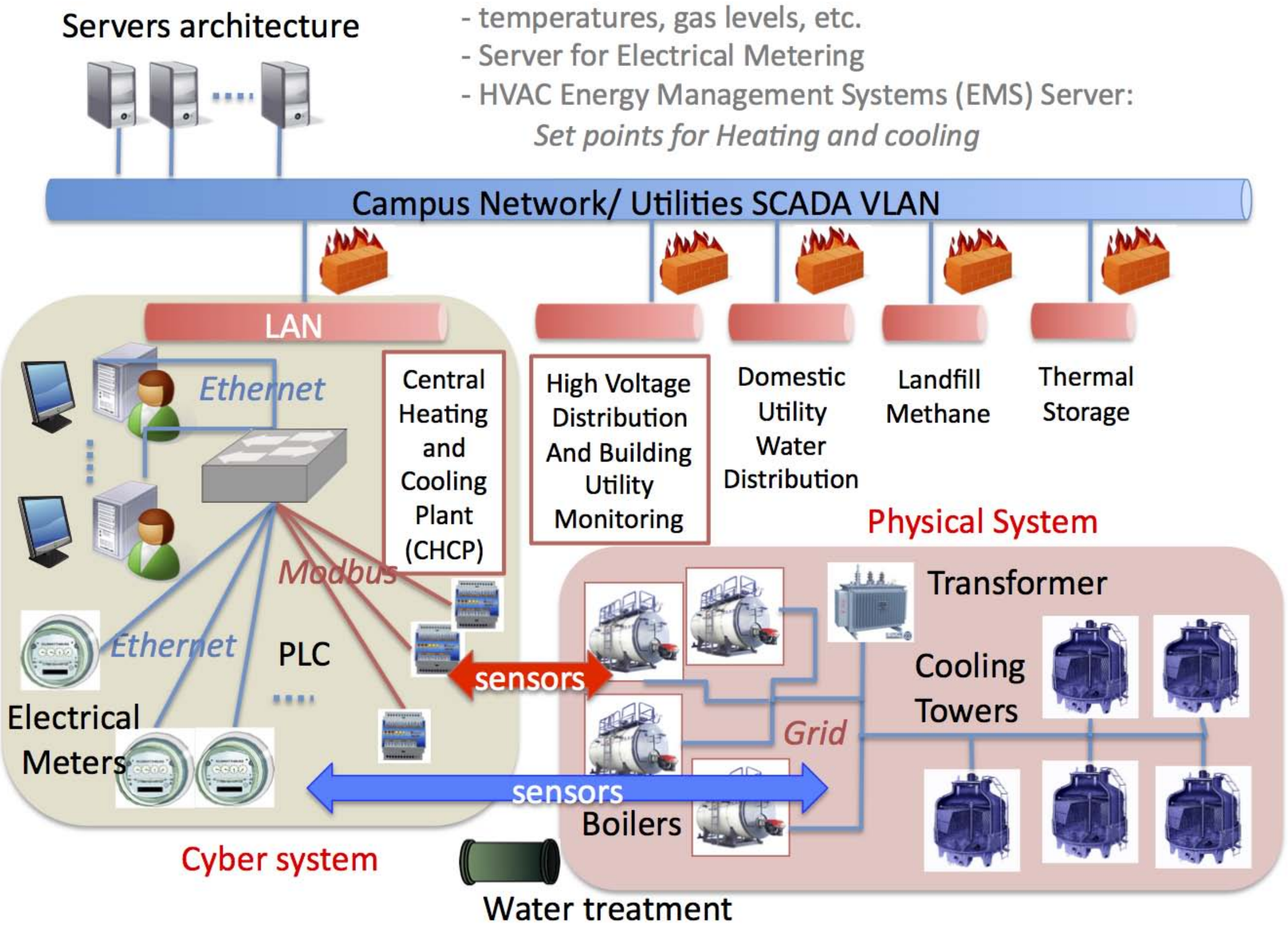
Collaboration/Technology Transfer

- Problem: mid-size, non-regulated infrastructures will remain in *legacy* state for up to a decade
  - Cost, lack of engineering expertise, perceived obscurity, etc.
- Solution: incorporate intrusion detection and physical constraint violation algorithms into passive network monitoring framework:
  - Network protocol and traffic pattern profiling and monitoring
  - For major components, continuous validation of system operation against simplified physical behavioral model.
- Once demonstrated, collaborate with control system vendors to incorporate above toolkit into products and services.....possibly dual track Open Source distribution

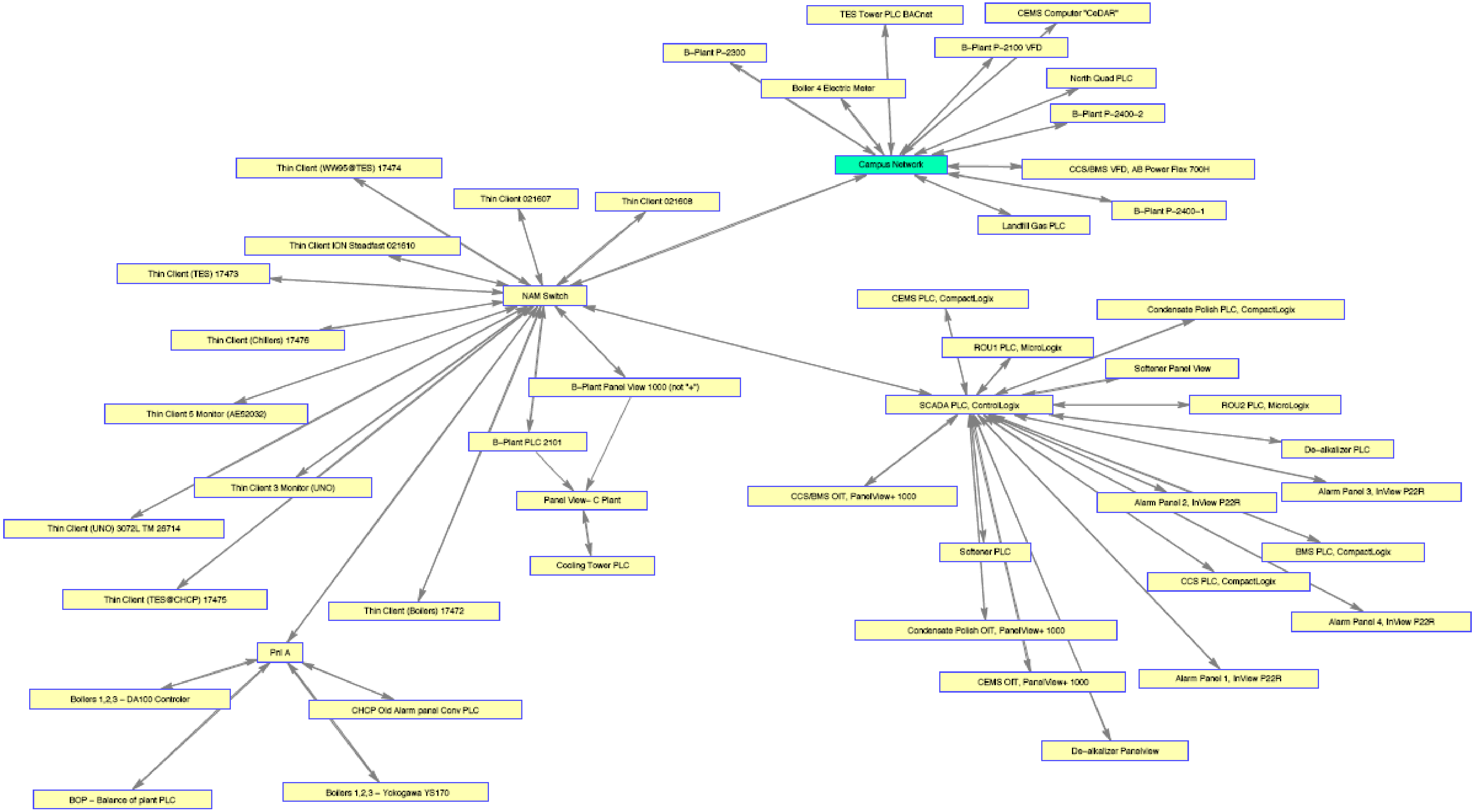
Next Steps

- Devise physical constraint algorithms for devices.
- Develop specification and model of command stream
- Analyze/inventory degree to which above physical and heuristic operational constraints can be mapped onto operational control network ("How many components can be protected...against what form of threats?").
- Verify patterns and their interpretation with operators and system experts to determine success.
- Penetration Testing (may require initial simulation)
  - Design test suite using the Flaw Hypothesis Methodology (FHM)
  - Implement and run tests

Additional Slides: Overview of SCADA Network Ecosphere


Servers architecture
- temperatures, gas levels, etc.
- Server for Electrical Metering
- HVAC Energy Management Systems (EMS) Server:
Set points for Heating and cooling
Campus Network/ Utilities SCADA VLAN
LAN
Ethernet
Central Heating and Cooling Plant (CHCP)
High Voltage Distribution And Building Utility Monitoring
Domestic Utility Water Distribution
Landfill Methane
Thermal Storage
Physical System
Modbus
Transformer
Ethernet
PLC
sensors
Cooling Towers
Electrical Meters
Grid
sensors
Boilers
Cyber system
Water treatment

Additional Slides: SCADA Network Map



TES Tower PLC BACnet

CEMS Computer "CeDAR"

B–Plant P–2300

B–Plant P–2100 VFD

Boiler 4 Electric Meter

North Quad PLC

B–Plant P–2400–2

Thin Client (WW95@TES) 17474

Campus Network

CCS/BMS VFD, AB Power Flex 700H

Thin Client 021607

Thin Client 021608

B–Plant P–2400–1

Landfill Gas PLC

Thin Client ION Steadfast 021610

Thin Client (TES) 17473

NAM Switch

CEMS PLC, CompactLogix

Condensate Polish PLC, CompactLogix

Thin Client (Chillers) 17476

ROU1 PLC, MicroLogix

Softener Panel View

B–Plant Panel View 1000 (not "+")

SCADA PLC, ControlLogix

ROU2 PLC, MicroLogix

Thin Client 5 Monitor (AE52032)

B–Plant PLC 2101

De–alkalizer PLC

Thin Client 3 Monitor (UNO)

CCS/BMS OIT, PanelView+ 1000

Alarm Panel 3, InView P22R

Panel View– C Plant

Alarm Panel 2, InView P22R

Thin Client (UNO) 3072L TM 28714

Softener PLC

BMS PLC, CompactLogix

Cooling Tower PLC

CCS PLC, CompactLogix

Thin Client (TES@CHCP) 17475

Thin Client (Boilers) 17472

Alarm Panel 4, InView P22R

Condensate Polish OIT, PanelView+ 1000

Pnl A

Alarm Panel 1, InView P22R

CEMS OIT, PanelView+ 1000

Boilers 1,2,3 – DA100 Controler

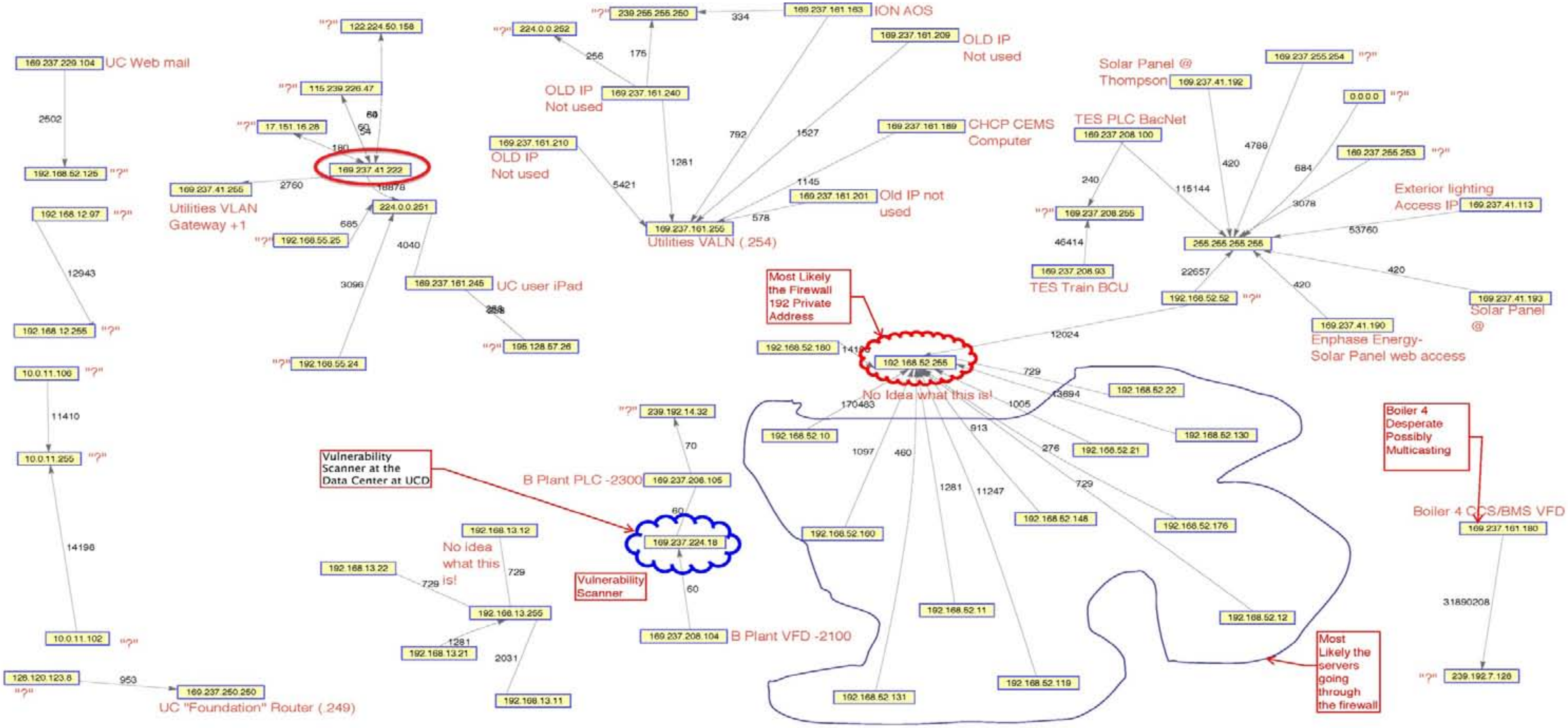
CHCP Old Alarm panel Conv PLC

De–alkalizer Panelview

Boilers 1,2,3 – Yokogawa YS170

BOP – Balance of plant PLC

Additional Slides: SCADA Traffic Mapping and Analysis



Most Likely the Firewall 192 Private Address

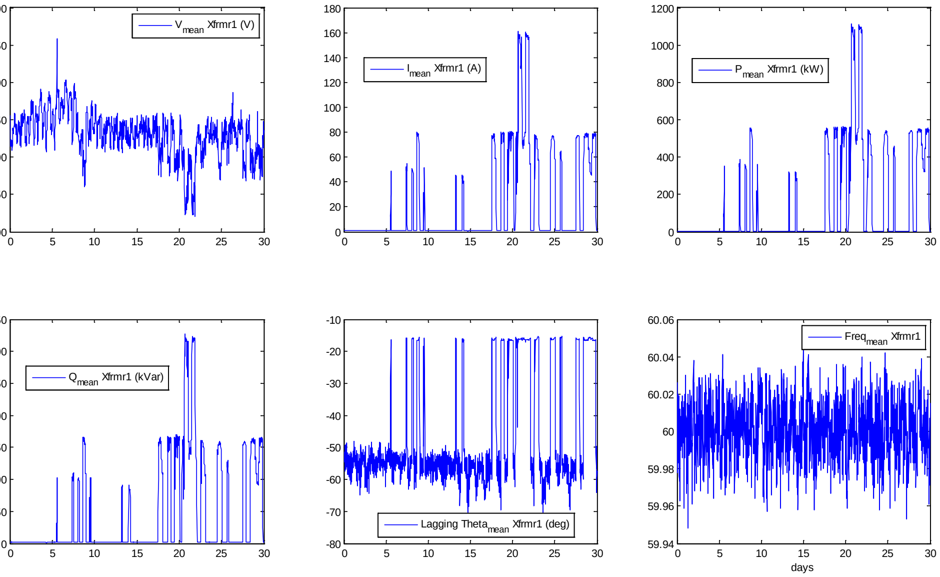
Vulnerability Scanner at the Data Center at UCD

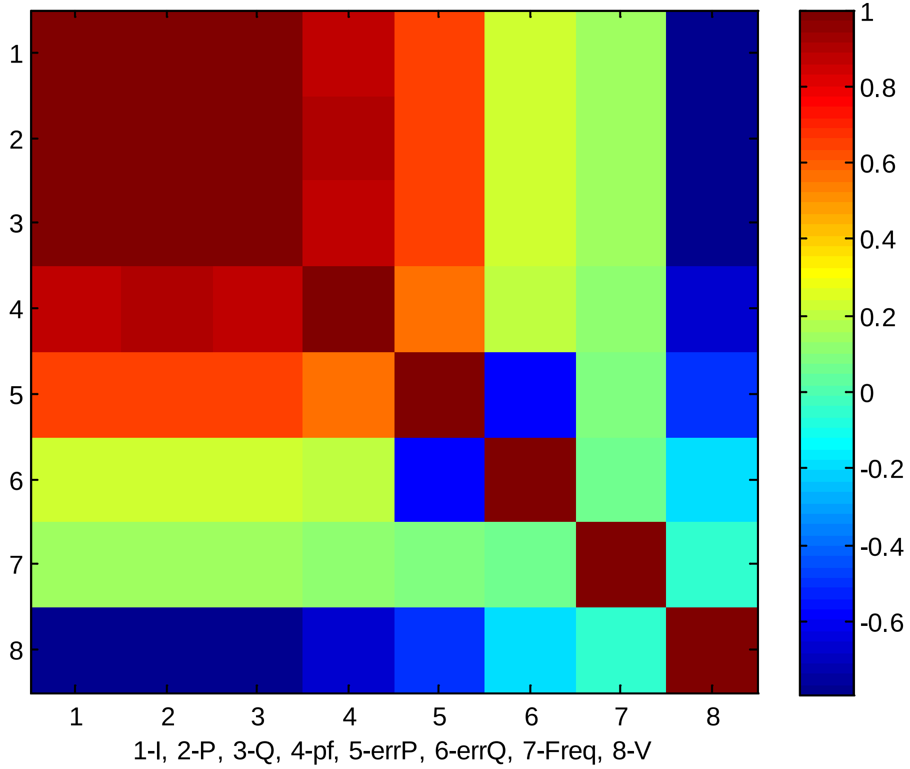
Vulnerability Scanner

Boiler 4 Desperate Possibly Multicasting

Most Likely the servers going through the firewall

Additional Slides: Initial Analysis of Measurement Correlations Based on Physical Systems


V mean Xfrmr1 (V)
I mean Xfrmr1 (A)
P mean Xfrmr1 (kW)
Q mean Xfrmr1 (kVar)
Lagging Theta mean Xfrmr1 (deg)
Freq mean Xfrmr1
days


1-I, 2-P, 3-Q, 4-pf, 5-errP, 6-errQ, 7-Freq, 8-V