Cyber Security is Easy. Except When it's not

Alfonso Valdes

Managing Director, Smart Grid @ Illinois

University of Illinois Urbana-Champaign

galvincenter for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

Provocative Questions

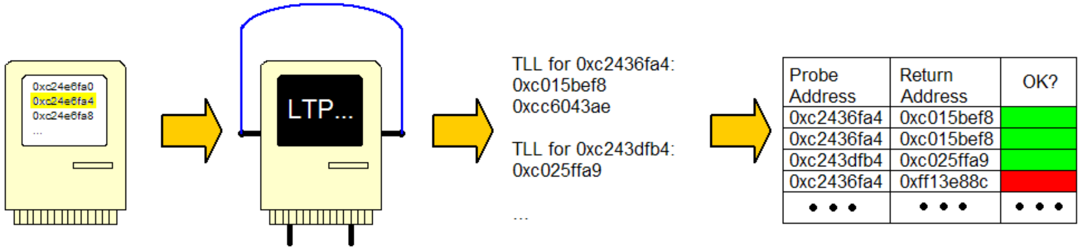
- What are key issues and differences in securing smart grid (and control systems in general) versus enterprise systems?
- Is the smart grid so complex that it is becoming brittle?
- Smart grid economics: can demand response potentially destabilize the grid?

Security Issues in Infrastructure Systems

Security Issue	Enterprise System	Infrastructure System
Attack Consequence	Financial, Inconvenience	Physical Consequence
Attack Surface	“Manageable”	Large number of nodes outside security perimeter
Communication Patterns	Complex	Predictable
Protocols	Complex	Spec based security possible?
Security measures	More mature	Unevenly applied, May upset process
Technology Lifecycle	Frequent refresh	Long device life

IDS for Embedded Systems, Protocols, and AMI

- Embedded Device IDS
- Specification-based AMI IDS
- Specification-based IDS for DNP3 protocol

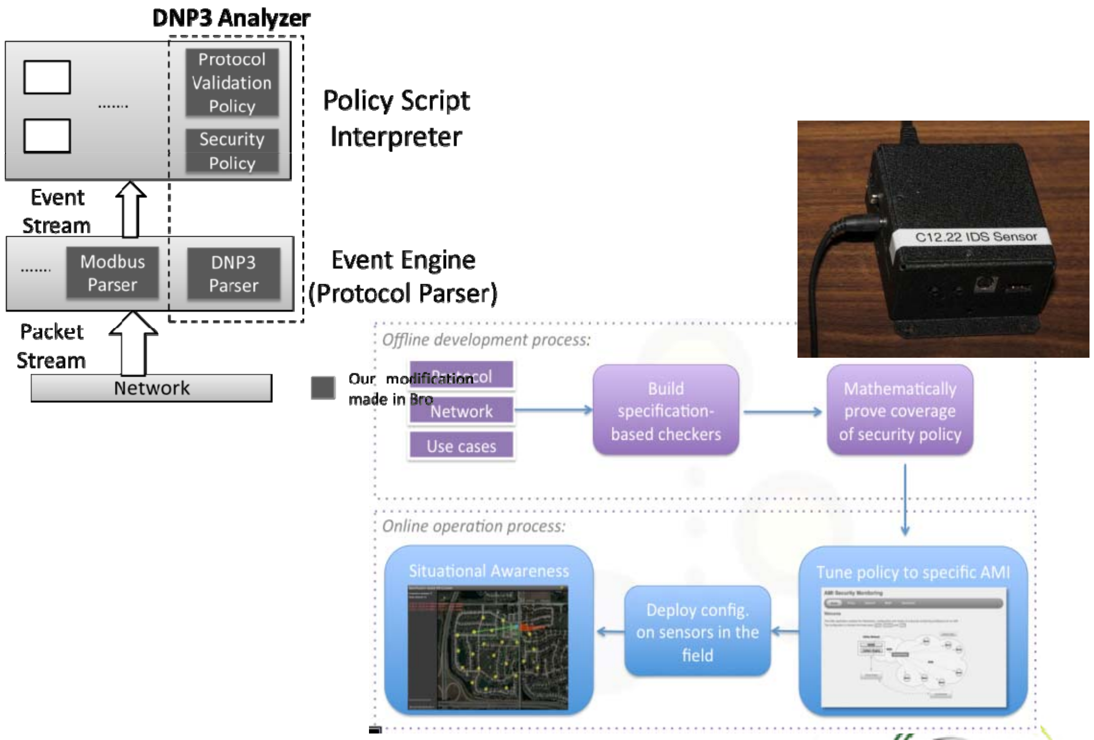


TLL for 0xc2436fa4:
0xc015bef8
0xcc6043ae

TLL for 0xc243dfb4:
0xc025ffa9

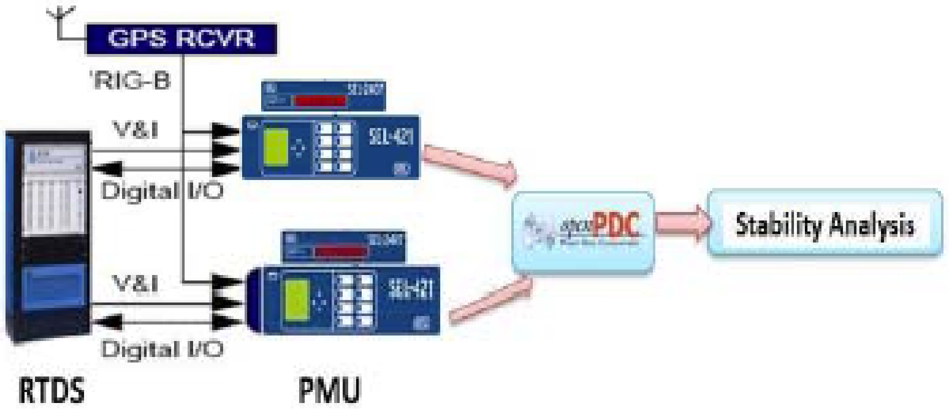
...

Probe Address	Return Address	OK?
0xc2436fa4	0xc015bef8	🟩
0xc2436fa4	0xc015bef8	🟩
0xc243dfb4	0xc025ffa9	🟩
0xc2436fa4	0xff13e88c	🟥
• • •	• • •	• • •



DNP3 Analyzer
....
Protocol Validation Policy
Security Policy
Policy Script Interpreter
Event Stream
....
Modbus Parser
DNP3 Parser
Event Engine (Protocol Parser)
Packet Stream
Network
Our modification made in Bro
C12.22 IDS Sensor
Offline development process:
Protocol
Network
Use cases
Build specification-based checkers
Mathematically prove coverage of security policy
Online operation process:
Situational Awareness
Deploy config. on sensors in the field
Tune policy to specific AMI

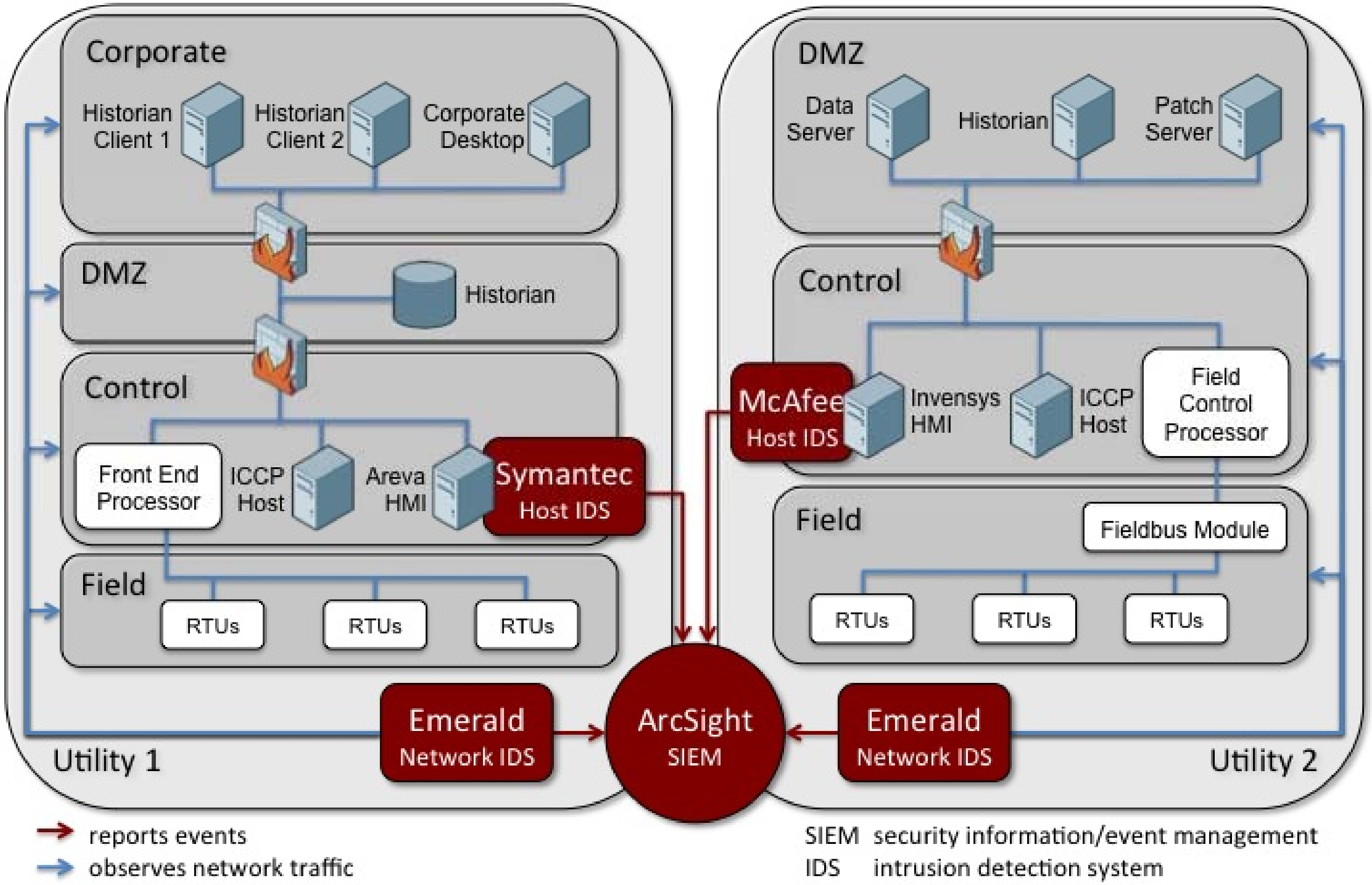
PMU and Wide Area Measurements



(a) RTDS/PMU/PDC testbed configuration.

- False data injection analysis and countermeasures
- GPS Spoofing and SCADA-based countermeasures
- Security of measurement devices

Cross-Site Detection and Correlation



Summary

- Smart Grid security is easier than enterprise system security
  - Simpler protocols
  - Easier to define correct behavior (anomaly and model-based security mechanisms more effective)
- Smart grid security is harder
  - Situation awareness must comprehend cyber and power
  - Security mechanisms stress limited bandwidth networks, embedded processors, and legacy devices
  - Millions of new nodes: Much larger attack surface
    - Most outside of secure perimeter and not under professional system administration
  - Market mechanisms require trust between multiple stakeholder communities and reliable autonomic response