Cybersecurity in Power Grids

Lloyd Wihl
Director, Application Engineering
Scalable Network Technologies
lwihl@scalable-networks.com
Challenges in Operating in the Cyber Domain

- Today energy is controlled by and through networks. The control systems include networked IP-addressable devices such as sensors, access control systems, and controllers.
- The energy sector has become a major focus for targeted attacks and is now among the top five most targeted sectors worldwide.
- All communication lines are attack surfaces, and adding connectivity and automation to power grid systems has increased vulnerability.
Cyber-Physical Vulnerabilities That Can be Exploited
Challenges

- Each attack vector’s modus operandi and impact can best be assessed in a lab-based simulation environment without imposing risk to the actual systems.

- Unfortunately, the testbed development process is not well established due to the complexity of:
  - Integrating cyber and physical resources
  - Incorporating realistic simulations of
    - physical systems
    - control systems
    - protocol vulnerabilities
    - cyber-attacks
    - data communication timing
    - network dynamics
Vision

- Scalable Network Technologies' EXata network emulation platform, along with its cyber library of simulated attacks and vulnerabilities, has been used effectively for many years by military organizations to analyze and test the resilience of mission-critical tactical battlefield networks.

- Scalable has partnered with OPAL-RT to apply this technology to critical infrastructure.
Software Virtual Network

- **Environment**
  Path loss, fading, interference, terrain, urban, ...

- **Emulated network**
  Devices, protocols, waveforms, ...

- **Live Interactions**
  Humans, devices, applications, ...

- **Cyber warfare**
  Vulnerabilities, attacks, defenses, ...

- **Accurate**
  Physical networks and models virtually indistinguishable

- **Scalable**
  Small live nets interoperate with large virtual nets

- **Real-Time**
  Response in same time as real network

- **Application-Centric**
  Unmodified apps work

Model execution on multi-core parallel architectures: maintain real-time speed and emulation fidelity as model complexity increases
Cyber Attack Framework (examples)

Attack models encompassing the protocol stack:

**Defensive Breach Framework**
- Firewall models
- Interface with attack generators & IDS

**Routing Misconfig Framework**

**Sniffing and Passive traffic analysis**

**Eavesdropping Framework**

**Signals Intelligence Framework**

**Physical Attack Framework**
- Barrage Noise Jamming
- “Silent” 802.11 MAC jammer
- Sweep jamming

**Denial of Service Framework**
- OS resource modeling
- Resource depletion modeling

**Jamming Framework**
- Wired & Wireless
Opal-RT/EXata Architecture

Real-Time Simulator
- Electromagnetic
- Electromechanical
- Mechanical

TCP/IP-based Protocols:
- TCP
- UDP
- Modbus
- DNP3
- C37.118

EXATA Server Communication Network Simulator

TCP/IP-based Protocols:
- TCP
- UDP
- Modbus
- DNP3
- C37.118

Intelligent Electronic Devices (IEDs) Controllers

Higher-Level System
- Controllers
- SCADA
- Real-Time Applications
- Servers
- Web
Network Defense Trainer

**Emulation Engine**
- Network Configuration Importer
- Cyber operations models
- Protocol models
- Host models
- Network and device performance
- Statistics

**HMI**
- HWIL, e.g. router, smart phone, IPS, switch, etc.

**Trainees**
- Player 1
- Player 2
- Player 3
- Player 4
- Player 5

**Exercise Control Utilities**
- Exercise Preparation
- Cyber Operating Picture
- Performance evaluation
- After Action Review

**Visualization**
- SWIL, e.g. SNMP mgr, SNORT, fuzzing, etc.

**Real Tools**
- GUI for Simulated Attacks

Underlined items = software provided by SCALABLE
EXata and OPAL-RT: Cyber Threat Assessment and Mitigation

**SCADA Defenses**
- Attack surface reduction
- Anomaly based IDS
- Connectivity adjustment
- Multiple viewpoint comparison
- Adaptation algorithms
- Time-varying reactions
- Isolation / shutdown strategies
- Control channel defense
- Dynamics modeling
- Code verification
- Reprogramming control devices
- ...

**SCADA Attacks**
- Reconnaissance, fingerprinting
- Authentication bypass, replay
- Bogus sensor inputs
- Modified controller outputs
- Time synchronization
- ...

**At-Scale SCADA System Model**
Connectivity, protocols, device models, access control, perimeter controls, firewalls, control & sensor data, physical process state

**Test Team**
Logging, attack progression, cyber and physical metrics

**Physical Controller mapped (HWIL)**

**Physical RTU mapped (HWIL)**

**Physical system dynamics**
SCALABLE and OPAL-RT Integrated Value

- Engineering-level network emulation to predict network behavior under attack.
- Ability to scale to represent the entire network.
- Integration of emulated network with equipment and power grid dynamics simulation.
- Run ‘what-if’ scenarios about critical infrastructure under cyber-attack without threatening operations.
- Assess effectiveness of tools, techniques and architectures to ensure system availability.
- Minimize vulnerabilities. Measure and improve system resiliency.
THANK YOU

SCALABLE Network Technologies
Los Angeles, CA
Miami, FL    Montreal, QC

lwihl@scalable-networks.com
scalable-networks.com