INTRUSION DETECTION IN INDUSTRIAL CONTROL SYSTEMS

ILLINOIS/EINDHOVEN COLLABORATION

ROBIN BERTHIER, HUI LIN, AL VALDES

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
JUNE 2014
OUTLINE

• TCIPG Summary
  – The challenge of trustworthy grid operation
  – TCIPG vision and research focus
  – Industry Interaction
  – Education, outreach, and training

• IDS in ICS

• Summary
THE CHALLENGE: PROVIDING TRUSTWORTHY SMART GRID OPERATION IN POSSIBLY HOSTILE ENVIRONMENTS

- **Trustworthy**
  - A system which does what is supposed to do, and nothing else
  - Availability, Security, Safety, …
- **Hostile Environment**
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- **Cyber Physical**
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction.
TCIPG VISION AND RESEARCH FOCUS

Vision: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for today’s and tomorrow’s power grid, so that it operates through attacks.

Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience
TCIPG STATISTICS

• Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
• $18.8M over 5 years, starting Oct 1, 2009 ($3.8M cost share)
• Funded by Department of Energy, Office of Electricity and Department of Homeland Security, Cybersecurity R&D Center, Office of Science and Technology
• 4 Universities
  – University of Illinois at Urbana-Champaign
  – Washington State University
  – University of California at Davis
  – Dartmouth College
• 23 Faculty, 17 Technical Staff, 38 Graduate Students, 9 Ugrad Students, 2 Admin Staff worked on the project in FY 2013
FY 13 TCIPG SCHOLARLY IMPACT
(OCTOBER 2012 – SEPTEMBER 2013)

• Degrees
  – 6 BS/BA, 4 MS, 9 Ph.D.
  – Numerous students at various stages of thesis preparation or defense
  – Graduates have started careers in academia, national labs, and industry

• Publications and Presentations
  – 52 Publications (40 refereed journal/conference, 12 thesis/tech rpt.)
  – 144 Presentations in conferences, symposia, industry group meetings, and individual industry partner interaction
TCIPG INDUSTRY INTERACTION

• Engage with Industry early and deeply
• Work on problems where fundamentals can make difference and whose solution will be high impact to industry
• Supplement grad student/faculty researchers with professional programmers, power engineers, security engineers to insure “industrial quality” of developed “product”
• Strategically decide the best method for transfer among: open source, incorporation in existing product, new product, start-up company
• Employ in-house “utility expert” to help focus research ideas and find appropriate tech transfer targets
• During testing, engage deeply with a small number of users first, and then expand the circle as concept/product develops
• Provide technology transfer support (through UI OTM, Office of Technology Management) to researchers
TCIPG AS CATALYST FOR ACCELERATING INDUSTRY INNOVATION

Utilities
- Sector Needs
- Pilot Deployment
- Data

Vendors/Tech Providers
- Access to Equipment, R&D Collaboration

TCIPG
- Validation and Assessment
- Solutions
COLLABORATION AND TRANSITION

• Utilities
  – AMI Security pilot with First Energy
  – Engagement with EPRI on various fronts
  – NetAPT as NERC CIPS pre-audit tool
  – SECURE, open communication gateway with Grid Protection Alliance (GPA)

• Industry
  – Schweitzer incorporating TCIPG embedded system security approach in their products
    • Schweitzer is a major donor of TCIPG testbed equipment
  – Honeywell collaboration on Role Based Access Control (RBAC) project in automation systems
  – New industry/academic initiatives with ABB, SEL, EPRI, Honeywell

• National Labs
  – Demonstrated Los Alamos NL quantum cryptography in our testbed, securing PMU communications using a hardware-in-the-loop experiment
  – NetAPT integrated with Idaho NL Sophia security visualization tool

• International
  – “In-Depth Defense of SCADA and Control Systems”, UI and University of Twente (NL), facilitated by DHS S&T and Netherlands Organization for Scientific Research (NWO). In pre-proposal process

• Transition
  – Startups Network Perception (more below) and River Loop Security
  – Open source transition of hardware IDS platform and tools for security assessment of wireless networks and SECURE open communication gateway
As a university consortium, education of professionals versed in cyber and power is the core mission
- Degree programs
- Internships
- TCIPG Reading Group

K-12 education and outreach
- TCIPG has developed interactive apps and educational kits
  - Over 5K downloads of TeslaTown, over 130K visits to app site
- Encouraging interest in STEM education and careers
- Teachers, parents learn too!

Assisting community colleges in smart grid curriculum development under IGEN Consortium

Short Courses
Hands-on security assessment
TCIPG Summer School
Annual Industry Workshop
TCIPG

INTRUSION DETECTION IN INDUSTRIAL CONTROL (INCLUDING ENERGY DELIVERY SYSTEMS)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Enterprise</th>
<th>ICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>System mission</td>
<td>Many</td>
<td>Single</td>
</tr>
<tr>
<td>Communications</td>
<td>Complex</td>
<td>Relatively static</td>
</tr>
<tr>
<td>Protocols</td>
<td>Many, complex</td>
<td>Few, relatively simple</td>
</tr>
<tr>
<td>Processors</td>
<td>Powerful, support</td>
<td>Embedded systems, limited</td>
</tr>
<tr>
<td></td>
<td>advanced security</td>
<td>compute, battery, comm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth</td>
</tr>
<tr>
<td>Life cycle</td>
<td>Frequent upgrade</td>
<td>Long deployment life</td>
</tr>
<tr>
<td>Security practices</td>
<td>Patched, OS current</td>
<td>Patches mat not be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>applied, legacy OS</td>
</tr>
<tr>
<td>IDS</td>
<td>Signature, whitelist</td>
<td>Learning-based, spec-based,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>whitelist</td>
</tr>
</tbody>
</table>
CONSIDERATIONS IN IDS FOR ICS

• Learning-based anomaly detection
  – Observe a system for some training time interval
  – Learn communication patterns, port mappings, function codes, etc.
  – Alert when a trained system observes anomalous traffic

• Specification-based detection
  – Formal analysis of the control protocol and security policy
  – Derive efficient on-line checker
  – Alert when traffic violates specification or policy

• Note that ICS include many validity and range checks for system operation and safety
SPECIFICATION-BASED IDS

• Security specifications:
  – Explicit declarations that define models of correct system behavior \[1\]
  – Security specifications are defined by using known system invariants, e.g., the definitions of the DNP3 protocol
    • other system invariants can be adopted to meet different scenarios

• We detect unexpected network activities based on predefined security specifications

• Adapt Bro to support proprietary SCADA protocols, e.g., DNP3
  – Define security policy targeting SCADA-specific attacks

DNP3 ANALYZER: ADAPT BRO TO SUPPORT DNP3

DNP3 Analyzer

- Protocol Validation Policy
- Security Policy

Extract 38 rules from the DNP3 protocol definition

Detect tampering of network packets

Event Stream

- Other Parsers
- DNP3 Parser

Device index
DNP3 response
Voltage magnitude

00 02 81 12 89 00 01 ...

Policy Script Interpreter

Network
PROTOCOL VALIDATION POLICY

- The policy detect communication patterns that violate security specifications
  - Violation may indicate attacks

<table>
<thead>
<tr>
<th>Violation</th>
<th>Possible Attack Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of range device index</td>
<td>An attacker is attempting to see how many devices are available in the reconnaissance phase of an attack.</td>
</tr>
<tr>
<td>Invalid operations on certain objects, i.e., relays</td>
<td>An attacker is attempting to change the original operation</td>
</tr>
<tr>
<td>Network packets fragmentation</td>
<td>An attacker is attempting to crash proprietary devices</td>
</tr>
</tbody>
</table>
SAMPLE SECURITY POLICY TO DETECT CONTROL-RELATED ATTACKS

- **Control-related attacks**: A sophisticated attacker can exploit system vulnerabilities and use a single maliciously crafted command to cause insecure system changes.

- Combine system knowledge on cyber and physical infrastructure in power grid to proactively estimate consequences of control commands and thus, to reveal attacker’s malicious intentions.

- **Master IDS** at the control center:
  - Identify control commands may change systems states
  - Trigger power flow analysis algorithm to estimate the execution consequence of the command

- **Slave IDS** at substations:
  - Obtain measurements directly from sensors (trusted in our threat model)
  - Validate measurements are not corrupted at other locations
SPECIFICATION BASED IDS FOR AMI

- Based on formal analysis of the C12.22 protocol
- Checker form factor can be a small Linux box
  - May eventually deploy an on-meter module
- Now in pilot deployment at a US utility
**AMILYZER**

- Technology developed in TCIPG
- Focus on network white-listing technology
- Collaboration with FirstEnergy
  - Deployment of *Amilyzer* at the head-end of a test AMI since December
**CASE STUDY**

**Failure Scenario:** AMI 1.7: Allow only scheduled remote disconnect during authorized time windows

**Security Policy:** Remote disconnects detected outside of authorized time window shall trigger a high-level alert

**[Developer]** Define specifications to identify “Remote Disconnect Operation”

**[Operator]** Define parameter “Authorized time window”

Monitor systems and networks and raise alerts on policy violation

Review alerts and escalate

AMI network

Amalyzer

Logs & Alerts
DETECTION OPERATIONS

AMI network

Amilyzer

Logs & Alerts

Packet stream
1011000010011010100
01010110111000011
11000101010101100
01101011101010100
01010101011010101
01010101010011011
01010101101000101
01011011101010101
0

Dissection
1,src1,dst1,Logon
2,dst1,src1,Ack
3,src1,dst1,Secur
4,dst1,src1,Ack
5,src1,dst1,Write
6,dst1,src1,Ack
7,src1,dst1,Logof
8,dst1,src1,Ack

Flow reassembly
Flow id: 1
Source: src1
Target: dst1
Timestamp: 3:31
Operation: Remote Disconnect

Intrusion Detection
Pattern: Remote Disconnect
Parameter: Authorized time window
Trigger: MATCH
Alert level: HIGH

Monitor systems and networks and raise alerts on policy violation

Review alerts and escalate
SECURITY POLICY

- 16 categories, 36 rules

<table>
<thead>
<tr>
<th>Violation</th>
<th>Low, Moderate, High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention</td>
<td>Authentication, Traffic Control…</td>
</tr>
<tr>
<td>Response</td>
<td>Revert config, terminate access…</td>
</tr>
<tr>
<td>Monitoring Location</td>
<td>Head end, Field-area network…</td>
</tr>
<tr>
<td>Response Location</td>
<td>Head end, Meter…</td>
</tr>
<tr>
<td>Information Required</td>
<td>Network traffic, user privileges…</td>
</tr>
</tbody>
</table>
CONTINUOUS DEPLOYMENT AT FIRSTENERGY

- Sample data volumes:
  - 28 days
  - 11,672 nodes
  - 158,690 flows (average 5,667 flows/day)
  - 10,724,780 packets (average 383,027 packets/day, 67 packets/flow)
  - 2,320,767,015 bytes (average 79 MB/day, 14 KB/flow)

Timeline of the number of flows per hour over 28 days
TRAINING: 1.5-DAY SHORT COURSE

• Prepared at the request of our funding agencies (DOE and DHS)
• Geared to program managers
• Topics:
  – Power Grid Equipment
  – Communications and Networking for Utility Computing and Control
  – Basics of Cybersecurity
  – Power Grid Infrastructure Basics
  – Trustworthy Wide Area Monitoring and Situational Awareness
  – Trustworthy Technologies for AMI
  – Cybersecurity Maturity Model
TRAINING: TCIPG SUMMER SCHOOL

- Offered on alternate years; Last session was June 2013
- Weeklong event, 173 participants
- Geared to graduate students, utility practitioners, and consultants
- 20 Technical sessions, presented by leading subject matter experts
- “Deep Dive” on selected topics
- Hands-on SCADA security assessment training (see next)
TRAINING: HANDS-ON SCADA SECURITY ASSESSMENT

- Six-hour vulnerability assessment exercise of a utility-like system
- Runs on self-contained network
- Established a simplified, “utility-like” virtual environment
  - Included typical security flaws
  - No real systems or actual vulnerabilities
- Students received instruction on
  - Security assessment tools
  - Tricks to analyze public-facing information for security flaws
  - Techniques for mapping networks, exfiltration, and data manipulation
- Very popular at the summer school: Added a session by popular demand
INDUSTRY WORKSHOP

• We present TCIPG research clusters and activities
• Four industry panels. This year the topics are:
  – Challenges of Cybersecurity Economics in Distribution Systems
  – Security of Cloud Computing for the Power Grid
  – Case Studies of Cybersecurity for Smart Grid Deployments
  – Cybersecurity for Smart Buildings and Microgrids
• Poster session
  – Opportunity for industry to directly engage researchers
• Limited to industry invitees (utility, system vendors, consultants), government, and National Labs