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

August 5-6, 2014

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
- **Schedule**
  - Start: 1/1/12; End: 12/31/14
  - Key deliverables and dates expected/met
  - What capability will result from this effort that will be transitioned to the energy sector?

- **Total Value of Award:** $600,000 over 3 years
- **% Funds expended to date:** ~85%
- **Performer:** Lawrence Berkeley National Lab
- **Partners:** University of California, Davis, International Computer Science Institute (ICSI), OSIsoft

Advancing the State of the Art (SOA)

- **State of the Art:**
  - Device safety typically implemented at hardware level (PLC, DCS, SIS, RTU, IED, etc.).
  - System operations safety performed at control center level (GUI, operations policy).
  - Layers typically connected by vulnerable comm. layer (public/private IP networks).
- **Our approach:** secure this gap by combining low-level monitoring of command sequences with sufficient awareness of physical device limitations to ensure overall safe system operation.

Advancing the State of the Art (SOA)

- This additional security layer augments (but does not replace) existing firewall / IDS / etc... solutions
- It provides enhanced protection...
  - from *outsider* attacks and *insider* mistakes.
  - to both vulnerable legacy devices with little or no security *as well as* new devices with authentication/encryption
- Can also verify that physical infrastructure state is consistent with information and commands exchanged by controllers.

Challenges to Success

- **Acquiring Data at Sites**
  - Decided to create our own testbed as an initial step.
- **Lack of Suitable Hardware/Software Testbeds**
  - Bought several PLCs and built our own testbed.
  - Created several of our own scenarios: water heater & several electrical scenarios
  - After initial PLC-only evaluation, extended this by using combinations of Simulink-based simulations of physical systems and PLCs communicating via Modbus TCP.
- **Missing features in Modbus/DNP3 Parsers in Bro**
  - Worked with Bro development team to provide data (e.g., network traces) to help debug.

Progress to Date

- **Major Accomplishments**
  - Developed experimental testbed for several scenarios for cyber-physical energy distribution systems, e.g.:
    - Differential protection scheme for power transmission
    - Distribution fault location, isolation, and service restoration (FLISR) model
  - Implemented several sets of scenarios in ladder logic on network-connected Siemens PLCs and/or in Simulink programs that all communicate via Modbus TCP.
  - Developed specifications of physical device limitations and implemented them in Bro/Broccoli.
  - Ran live experiments of Bro/Broccoli flagging physical violations (as appropriate) from cyber commands sent to physical devices.

Collaboration/Technology Transfer

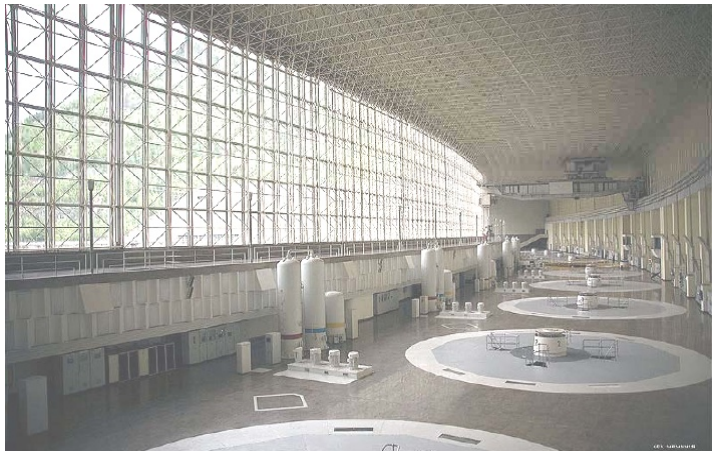
- **Plans to transfer technology/knowledge to end user**
  - Our work is potentially useful to asset owners, vendors, and OEMs.
  - Working closely with Bro development team at LBNL/ICSI.
  - Preparing release of example simulations and Bro specifications as open source code later this year.
  - OSIsoft has expressed interest in our work and hired one of our graduate students for the summer; we are currently working with them to adapt our technique to their software and protocols.
  - What are your plans to gain industry acceptance?
    - Will work with Bro development team to promote our scripts
    - OSIsoft collaboration adds considerable clout
    - Working with LBNL Environment Energy Technology Division to interact further with utilities, vendors, manufacturers, etc.. in related projects.

Next Steps for this Project

- **Approach for the next year or to the end of project**
  - Continue to integrate/formalize means for developing IDS specifications from mathematical models of device functionality
  - Finish implementing our technique on OSIsoft products.
  - Release live traffic captures, simulations, and and Bro-based examples (including documentation) as open source.
  - Complete reporting and authoring of peer-reviewed papers on the results of our work.

Motivating Examples

- ***Intentional*** SCADA attack on Maroochy Water Station in Australian (2000) by ex-employee, discharging 800K liters of raw sewage into nearby river.
- ***Accidental*** mis-configuration of marginal turbine for AGC load tracking at Sayano-Shushenskoe hydro plant (2009) contributed to failure of multiple turbines.



Other Examples

- Cyber attacks on cyber-physical systems can have physical consequences
  - Stuxnet is an example involving industrial control systems
  - Other examples could relate to electrical load, etc..
- PLCs are vulnerable — in many installations, any networked device can change set points.
  - In some cases, can cause devices to exceed their physical limitations.
  - Can drive overall system to unanticipated states.

Approach Details

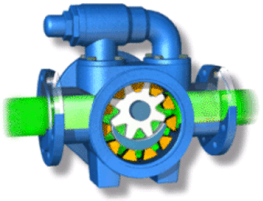
1. Collect command and monitoring streams from
   - conversations between PLCs (Siemens S7-1200) and HMIs
   - simulated Modbus TCP conversations
2. Create simplified computer models that include key physical constraints not derivable from traffic analysis.
3. Develop specifications of permissible device commands and combine with physical constraints (temp., RPM, etc.) – including system-level inherited constraints.
4. Apply these specifications to observed network command streams
5. Study effectiveness in identifying intrusions or incorrect command sequences.

Bro/SCADA Architecture

SCADA/HMI

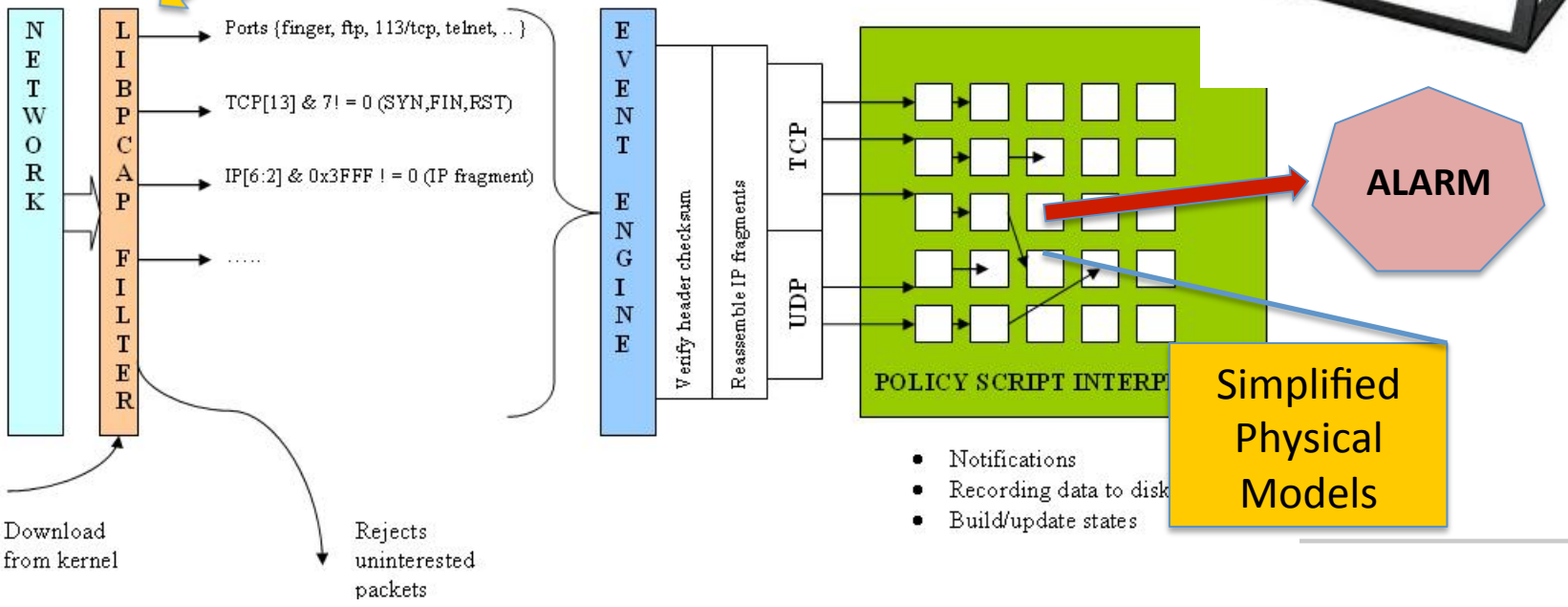
Modbus

PLC



PLC

BRO-IDS System Structure



Integration with Production IDSs

- Currently using Bro Network Monitoring Framework
  - Well known network security/intrusion detection package.
  - Modbus TCP and DNP3 parsers built-in
  - Runs on Raspberry PI at low end to 40 GB/sec + at high end
  - Supports highly "stateful" view of application layer behavior.
  - Integrated post hoc security analysis and comprehensive network archiving.
  - Real-time, open interfaces to cooperating applications.
  - Readily adaptable – new protocols and analyzers.
  - Open source promotes collaboration and code sharing.
  - Local expertise and developers (LBNL and ICSI).
- Modularity of specifications demonstrates the adaptability of hybrid solutions —
  - Bro as network-facing
  - Broccoli-based client talking to a "physics module" to look at device physics
- OSIsoft funding and involvement demonstrates serious vendor interest.