Specification-based IDS for the DNP3 Protocol

Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, and Ravi K. Iyer

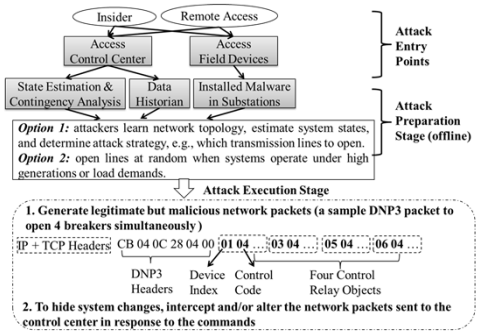
GOALS

- Overall:
  - Detect sophisticated semantic attacks that drive a power grid into an unsafe state without exhibiting any obvious protocol-level red flags.
  - Combine system knowledge of both cyber and physical infrastructure in power grids to estimate the execution consequences of maliciously crafted control commands.
- Specifically:
  - Augment Bro IDS with:
    - DNP3 network packet analyzer to monitor control commands and data exchanged between the SCADA master and substations.
    - Power flow assessment tools to perform run-time state estimation to predict consequences of executing (potentially maliciously crafted) control commands.

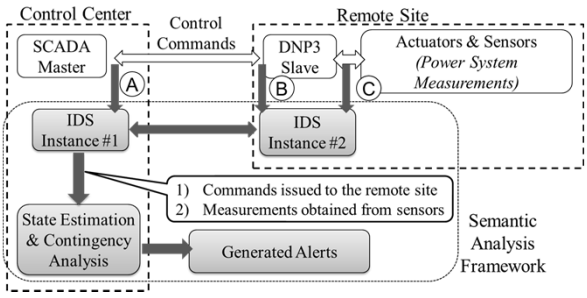
FUNDAMENTAL QUESTIONS/CHALLENGES

- A sophisticated attacker can exploit system vulnerabilities and use legitimate commands to cause a wide range of system changes.
- Hard to detect such control-related attacks with network IDS exclusively.
  - Maliciously crafted control commands can be encoded in legitimate format.
  - Few anomalies are found in SCADA networks.
  - Few attack signatures are publicly available.
  - Can avoid traditional contingency analysis, which usually targets low-order (N-1) contingencies.
  - Measurements obtained through SCADA networks may be corrupted.

Attack Example



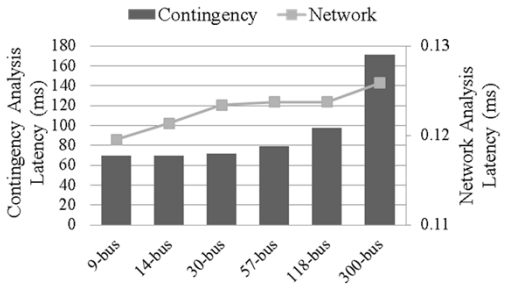
RESEARCH PLAN



- IDS at the control center:
  - Distinguish critical commands from noncritical ones.
  - Collect measurements from multiple substations.
  - Include state estimation & contingency analysis components to estimate consequences of executing a given command.
- IDS at the remote site:
  - Use local IDS to obtain trusted measurements directly from sensors.
    - Assume that concurrent physical tampering with a large number of distributed sensors is not practical.
  - Confirm that measurements are not corrupted at other locations.

RESEARCH RESULTS

- Execution time of analyzing critical commands.
  - Network monitoring ("Network Analysis").
    - Filtering out noncritical commands and extracting parameters of critical ones.
  - Triggered power flow analysis ("Contingency Analysis").
    - Analyze the execution consequences of network commands.
- The time to estimate the execution consequence of a command is almost three orders of magnitude higher than the time for the network monitoring.
- Even though analyzing control commands takes time, the proposed semantic analysis can work reliably in real setup as:
  - Network throughput in SCADA networks is still low.
  - Types of critical commands are limited.



BROADER IMPACT

- The semantic analysis requires a small amount of time, which can provide manual operations (i.e., control commands issued by operators) with another layer of protection.
  - The distributed IDS with semantic analysis does not affect the normal operation of the power grid.
  - The method and implementation of semantic analysis can be extended to other industrial control environments.
- The implemented network IDS can be equipped with other scenario-specific policies in different operational contexts.

INTERACTION WITH OTHER PROJECTS

- Collaborate with International Computer Science Institute (ICSI) and the University of Illinois' National Center for Supercomputing Applications (NCSA).
  - The extension made on Bro to support the DNP3 protocol is included in Bro's current source code release (version 2.2).
  - Searching for industry collaborations to deploy the DNP3 analyzer in real control environments.
  - New NSF award is being used to support further work.

FUTURE EFFORTS

- Study possible response mechanisms to attacks.
  - Preemptive responses may be needed to prevent physical damage.
  - But how to prevent the preemptive responses from becoming new system vulnerabilities?
- Include in IDS high-order contingency analysis algorithms to estimate the effect of control commands before they are issued.

SELECTED PUBLICATIONS

1. Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter Sauer, and Ravishankar Iyer. "Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids." In *Proceedings of Smart Energy Grid Security Workshop, SEGS 2013.*
2. Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer. "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol." In *Proceedings of 8th Annual Cyber Security and Information Intelligence Research Workshop, CSIIRW 2012*. Top Three Paper Award.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T