Specification-based IDS for the DNP3 Protocol

Overview and Problem Statement

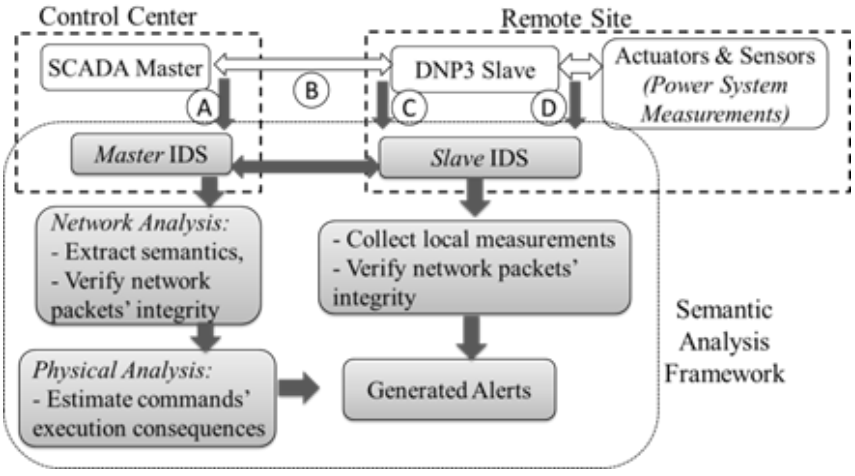
Modern SCADA systems are increasingly adopting Internet technology to control industrial processes. Because of security vulnerabilities and potential exposure (intended or unintended) to public networks, attackers can penetrate control systems to issue malicious control commands that drive remote facilities into an unsafe state, without exhibiting any obvious protocol-level red flags. While a few Intrusion Detection Systems (IDSes) are becoming available to investigate network traffic based on unique proprietary protocols, it is challenging to detect such attacks based solely on network activity. To overcome that challenge, we introduce a semantic analysis framework based on collaborating network IDSes. The framework exploits a power flow analysis algorithm adapted to accurately estimate the execution consequences of control commands with short latency, thus revealing a potential attacker's malicious intentions.

Research Objectives

- Provide theory base to analyze the impact of the attacks that exploit control commands.
- Augment Bro IDS with power flow assessment tools to perform run-time power flow analysis to predict the consequences of executing a (potentially maliciously crafted) control command that is transmitted by run-time network packets.
- Design and implement an adapted power flow analysis algorithm that significantly reduces the detection latency.
- Experiment to evaluate the attack scenario and establish the feasibility of the proposed semantic framework.

Technical Description and Solution Approach

- Master IDS at the control center:
  - Distinguish critical commands from noncritical ones.
  - Collect measurements from multiple substations.
  - Include adapted power flow analysis algorithm to estimate consequences of executing a given command.
- Slave 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 for the attacker.



Results and Benefits

- Through integration of power flow analysis modules, the deployed Bro IDS is able to detect malicious commands transmitted in network packets that are syntactically correct within the protocol.
- Experiments estimate the physical consequences of malicious control commands for power systems.
  - E.g., increase generation, increase load demands, or open transmission lines.
- Experiments demonstrate the good performance of the adapted power flow analysis algorithm.
  - Significantly reduces the detection latency.
  - Introduces very few false detections.

Researchers

- Hui Lin, hlin33@illinois.edu
- Adam Slagell, slagell@illinois.edu
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar K. Iyer, rkiyer@illinois.edu

Industry Collaborators

- Donald Borries, Ameren TAC

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security