TCIPG

Specification-based IDS for the DNP3 Protocol

Adapting Bro into SCADA: Building a Specification-based IDS for DNP3

H. Lin, A. Slagell, C. Martino, Z. Kalbarczyk, R. K. Iyer

Goals

- Propose a specification-based intrusion detection system (IDS) that supports proprietary network protocols, such as DNP3, used in industry control environments.
- Evaluate the proposed IDS in a typical SCADA system operating electrical power grids:
  - Generate SCADA-specific network events for analysis.
  - Propose a security policy to detect a man-in-the-middle attack.

Fundamental Questions/Challenges

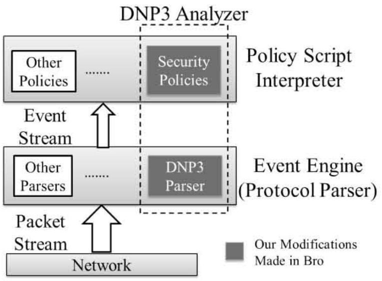
- Traditional signature-based IDS is not widely used.
  - Little analysis of real attacks is available to public.
- Traditional anomaly-based IDS lacks sufficient capabilities to investigate SCADA-specific network traffic.
  - Relies on information in TCP layer, e.g., host addresses, port numbers.
- Common proprietary protocols, e.g., DNP3, transmit information in plain text.
  - The network packets can be corrupted during transmission to modify control operations or measurement data.

Research Plan

- Develop a **DNP3 Analyzer** that is integrated with Bro-IDS.
  - **Bro**: a real-time network traffic analyzer widely used in forensic analysis, intrusion detection, etc.
- Separate event analysis from event generation.
  - SCADA events are analyzed by defined security policies.

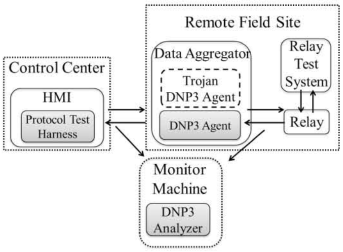
Implementation

- DNP3 analyzer components:
  - **DNP3 Parser.** A new parser integrated in Bro to generate SCADA system-specific events; the semantics related to each event are delivered to the corresponding event handler for analysis and processing.
  - **Security Policy.** A security policy implemented by selective definition of event handlers in terms of Bro scripts; the policy script interpreter executes the scripts to interpret the observed events and detect abnormal network activities.



Evaluation Results

- Experimental environment:
  - Real-world hardware devices and software to mimic operations in power grid substations.
  - Employ a Trojan software (Trojan DNP3 Agent) to mimic malicious activities by modifying measurement data sent to the Control Center (or SCADA Master).



- Security policy:
  - Compare payloads of network packets sent to the Data Aggregator from the Relay and data sent to the Control Center from the Data Aggregator; comparison results indicate whether the Data Aggregator is compromised.
- Initial findings:
  - Online monitoring does not interfere with runtime SCADA operations.
  - Off-line evaluation analyzes throughput of the DNP3 parser with and without the security policy in terms of two metrics: number of bits processed per second (bps) and number of packets processed per second (pps).

Evaluation Target	Throughput (Mbps)	Throughput (pps)
DNP3 Parser	39.87	10216
DNP3 Parser + Security Policy	31.39	8046

Broader Impact

- The testbed developed provides a platform to support a broad range of attack scenarios.
- The proposed DNP3 analyzer can be equipped with other scenario-specific policies in different operational contexts.

Interaction with Other Projects

- Collaborate with NCSA security operational team:
  - The Bro extensions made to support the DNP3 protocol will be included in Bro's next source code release (version 2.2).
  - Search for industry collaborations to deploy the DNP3 analyzer in real control environments.

Future Efforts

- Study how to use the DNP3 analyzer to decide whether or not a valid control operation is malicious.
  - Plan to correlate network semantics with domain-specific power flow analysis, i.e. ,contingency analysis.

Trustworthy Cyber Infrastructure for the Power Grid • www.tcipg.org
University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University