A Novel Framework for OT Protocol Vulnerability Discovery: Leveraging Insights from Formal Modeling, Network Simulation and On-Device Testing

Matthew Boeding, Michael Hempel and Hamid Sharif

Department of Electrical and Computer Engineering, College of Engineering

Motivation

Operational Technology (OT) systems are becoming more **interconnected** and are **converging with IT** systems.

Cybersecurity priorities traditionally were different between OT and IT systems:

- Availability is paramount in OT systems
- Confidentiality is a higher priority in IT systems

Different protocol implementations can create vastly different behaviors to cyber attacks.

Protocol specifications must be manually evaluated by each vendor to create their own protocol implementation.

Challenges

Protocol Specifications are limited in scope:

- Reliant on industry experts to create robust device implementations
- Devices can have large discrepancies in handling a large amount of traffic
- May assume a "Defense in Depth" strategy, that leave devices vulnerable to protocol specific attacks

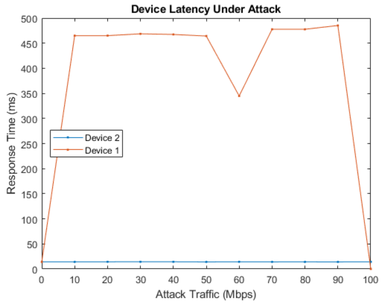


Figure 1. Effect of Cyber Attack on Device Response Time [2]

- A formalized method for identifying and verifying vulnerabilities would facilitate more robust devices

Contribution

Formal Verification Models of Protocol Specifications:

- Created using Construction and Analysis of Distributed Processes (CADP) [1]
- Identify risks within specification and implementation cybersecurity, solely from protocol specifications

Simulation of OT Networks:

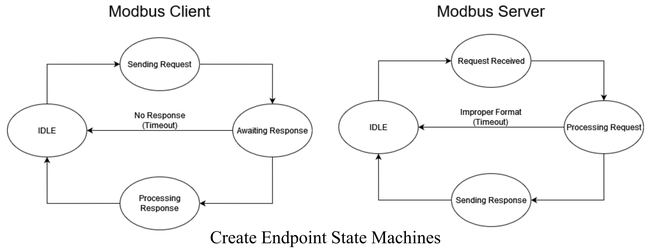
- Utilize OMNET++ package with INET framework
- Build OT specific protocols on top of existing network simulations

Testbed with Hardware:

- Creation of individual protocol libraries using C
- Tested Compliance against production Intelligent Electronic Devices (IEDs)

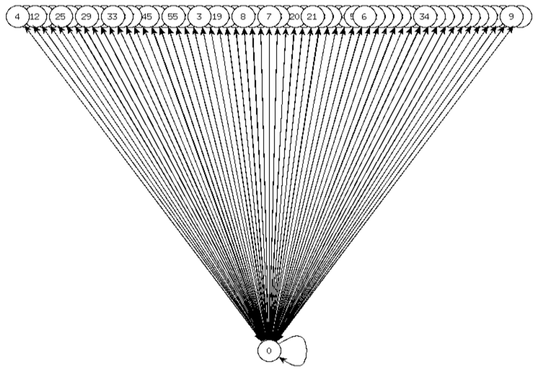
Methodology

1. Manually Evaluate Protocol for Expected Behavior



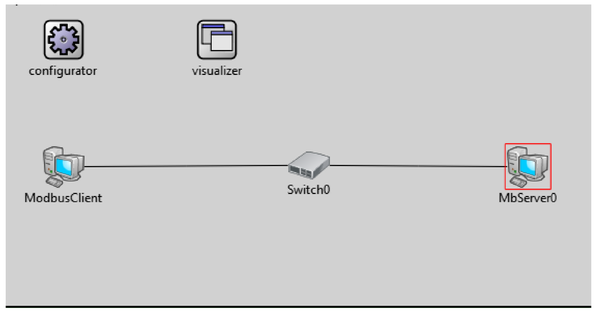
Create Endpoint State Machines

2. Identify Vulnerable States Through Formal Verification



Create Formal Model through CADP [3]

3. Create Simulation Models for Critical State Evaluation



Network Model in OMNET++

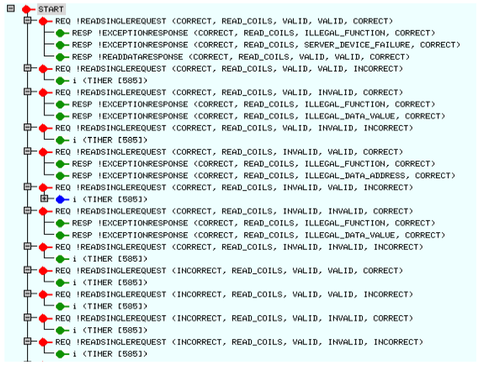
4. Test Simulation Results Against Production IEDs

Hardware Testbed

Results

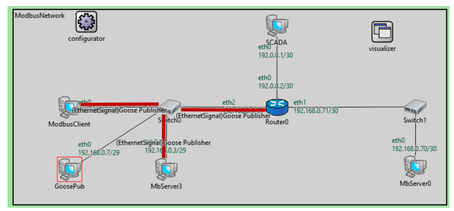
Formal Verification Results:

Found vulnerabilities, labelled with hidden label ("i" in the image below)

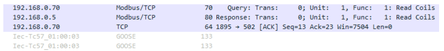


Simulation Results:

- Creation of simple Peer to peer and more complex simulations

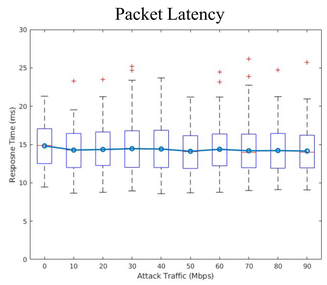


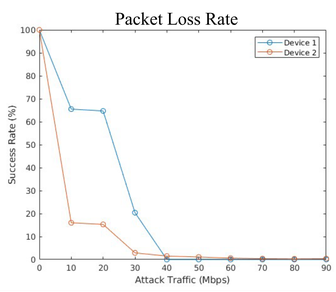
- Output packet traces of both session based (Modbus) and Time Sensitive (GOOSE) Protocols



Hardware Testbed Results

Ability to identify latency and packet loss for individual devices, which can be leveraged for matching simulation results to hardware behavior.





Conclusion and Future Work

Future Work:

- Validate simulation results against physical IEDs
- Expand Simulation to representative case study
  - Using UNMC network as reference
- Create dynamic tests to match simulation parameters to physical device behavior
- Match emulated IED behavior to physical devices
- Identify weak points in reference network through simulation

Conclusions:

- Introduced End-to-End evaluation framework for OT protocols
- Identified protocol vulnerabilities through Formal Modelling
- Created representative simulation for OT network
- Created physical testbed for production hardware
- Can be expanded to identify weak points in existing networks

Project Collaborators

This work was supported by the Nebraska Public Power District through the Nebraska Center for Energy Sciences Research at the University of Nebraska-Lincoln.

NEBRASKA CENTER FOR ENERGY SCIENCES RESEARCH

[1] Garavel, H., Lang, F., Mateescu, R. et al. "CADP 2011: a toolbox for the construction and analysis of distributed processes", Intl. Journal on Software Tools for Technology Transfer, vol. 15, 2013. DOI: 10.1007/s10009-012-0244-z
[2] Boeding, M., Hempel, M., Sharif, H., Lopez Jr., J., Perumalla, K., "A Flexible OT Testbed for Evaluating On-Device Implementations of IEC-61850 GOOSE", Intl. Journal on Critical Infrastructure Protection, 2023
[3] Boeding, M., Hempel, M., & Sharif, H. "Vulnerability Identification of Operational Technology Protocol Specifications Through Formal Modeling." ICSPCS. IEEE. 2023