Study of Real-World OPC-UA Implementation using State Machine Inference

Olivier Levillain

We have been studying various protocols using state machine inference techniques in the departement for several years now. The studied protocols have mainly been TLS (presented at ESORICS22[1]), SSH and OPC-UA (with a recent publication at ARES24[2]). Our work has mainly been focused on open source implementation we could set up in containers and interact with easily.

In this project, we would like to extend our work on OPC-UA with a real-world implementation provided by an industrial control system (ICS). This would present several challenges since the interaction will truly be a black-box interface, with no easy way to reset the system under test.

Since this setup might be hard to control and master, we can also imagine another extension to our work on OPC-UA, which consists in expanding the vocabulary of our tools (more specifically the OPC-UA mapper), by adding new messages regarding recent evolutions of the standard with Diffie-Hellman key exchange.
The project would probably consist of the following tasks:

- get acquainted with OPC-UA and the state machine inference techinques (the paper to read for the first seminar will probably be our article at ARES24);
- replay some of our experiments on open source OPC-UA implementation, using the different tools we published as open source;
- configure our industrial platform to expose a working OPC-UA interface;
- run experiments to infer the state machine of the OPC-UA implementation from the platform;
- (optionnaly) expand the vocabulary of our tools to include DH messages.

Practical Information

Regular meetings will be scheduled with the advisor, either via visioconference or in Palaiseau. If you are interested, send an email to the advisor.

[1] Aina Toky Rasoamanana, Olivier Levillain, Hervé Debar. Towards a Systematic and Automatic Use of State Machine Inference to Uncover Security Flaws and Fingerprint TLS Stacks. ESORICS 2022

[2] Arthur Tran Van, Olivier Levillain, Hervé Debar: Mealy Verifier: An Automated, Exhaustive, and Explainable Methodology for Analyzing State Machines in Protocol Implementations. ARES 2024