RICSel21: A dataset with network attacks targeting IEC-60870-5-104 in SCADA systems*

Erik Westring[1], August Fundin[2], Chih-Yuan Lin[2], Tommy Gustafsson[1], and Simin Nadjm-Tehrani[2]

[1] FOI, Swedish Defense Research Agency, Sweden
[2] Linköping University, Sweden

Attacks against power grids and other critical infrastructure have been on the rise in recent years, with well-known examples like the attacks against the Ukraine power grid in 2015 and 2016. To battle these threats, security researchers need non-sensitive datasets collected in realistic environments to improve and benchmark defensive measures. RICSel21 is our contribution towards that goal: a dataset containing twelve network attacks targeting IEC-60870-5-104 (IEC-104) network traffic within an emulated supervisory and data acquisition (SCADA) network.

The dataset has been generated in the national Swedish testbed RICS-el that runs a commercial SCADA system and emulated remote terminal units [1]. RICS-el utilizes virtual machines and simulates a production environment of a company that generates and distributes electrical power. The testbed includes three automated bots that emulate operations, attacks and execute scenarios as shown in Fig. 1.

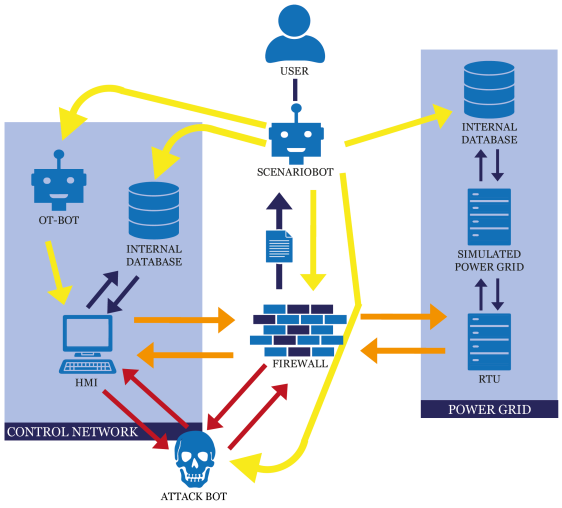

Fig. 1. The work flow of attack generation within RICS-el

* This work was supported by Swedish Civil Contingencies Agency (www.rics.se).

The ScenarioBOT is used for orchestrating repeatable and scripted experiments, as well as to collect the generated data after completion. When generating RICSel21, the ScenarioBOT started the power grid from a known state, used the OT-BOT to emulate an operator running the power grid and the Attack BOT to perform the attacks listed in Table 1.

Table 1. Overview of implemented attack scenarios

No	Attack description	Type
1	Scanning and ARP spoofing of identified targets	Scanning
2	Dropping all IEC-104 packets between two targets	DoS
3	SYN flooding of an RTU	DoS
4	Network traffic flooding, targeting the HMI and RTU	DoS
5	Intermittent dropping of IEC-104 packets	Sequence
6	Altering sequence numbers of IEC-104 packets	MitM
7	Altering sensor values in IEC-104 packets	MitM
8	Altering time tags of IEC-104 packets	MitM
9	Altering IOAs of IEC-104 packets	MitM
10	Replay of IEC-104 packets in control direction	Replay
11	Injection of setpoint commands	Injection
12	Masquerade as a second HMI	Injection

The attacks in the dataset include MiTM attacks targeting IEC-104 by altering sequence numbers, time tags, sensor values and register values. Packets are dropped intermittently and fully. There are also replay attacks, injections of setpoint commands, ARP spoofing and SYN flooding targeting a remote terminal unit. Fundin provides a more detailed description of the attacks [2].

The dataset generation followed this sequential workflow: Script preparation, system configuration, running attack scenario, data collection, data processing, data evaluation. During the experiments, the power grid values where sampled every five seconds. After each run, the ScenarioBOT collected the experiment data and related pcaps, which was then used to create RICSel21. The dataset is freely available at `https://gitlab.liu.se/ida-rtslab/public-code/2021_attack_rics`

References

1. Almgren, M., Andersson, P., Björkman, G., Ekstedt, M., Hallberg, J., Nadjm-Tehrani, S., Westring, E.: RICS-el : Building a National Testbed for Research and Training on SCADA Security (Short Paper). In: Critical Information Infrastructures Security (CRITIS). Springer International Publishing (2019)
2. Fundin, A.: Generating Datasets Through the Introduction of an Attack Agent in a SCADA Testbed. Master's thesis, Linköping University (2021), `https://liu.diva-portal.org/smash/get/diva2:1557696/FULLTEXT01.pdf`