SnapShotter: A lightweight Intrusion Detection for PLCs

Chenglu Jin, Saeed Valizadeh, Mason Ginter, and Marten van Dijk

University of Connecticut

{chenglu.jin, saeed.val, mason.ginter, marten.van dijk}@uconn.edu

1. Motivation

- Industrial control systems are connected to the network, and therefore they are venerable to cyber attacks. E.g. Stuxnet targets SCADA systems.
- Programmable logic controllers (PLCs) are one class of such devices mainly used for controlling the industrial processes.

2. Proposal

Attack Scenario:

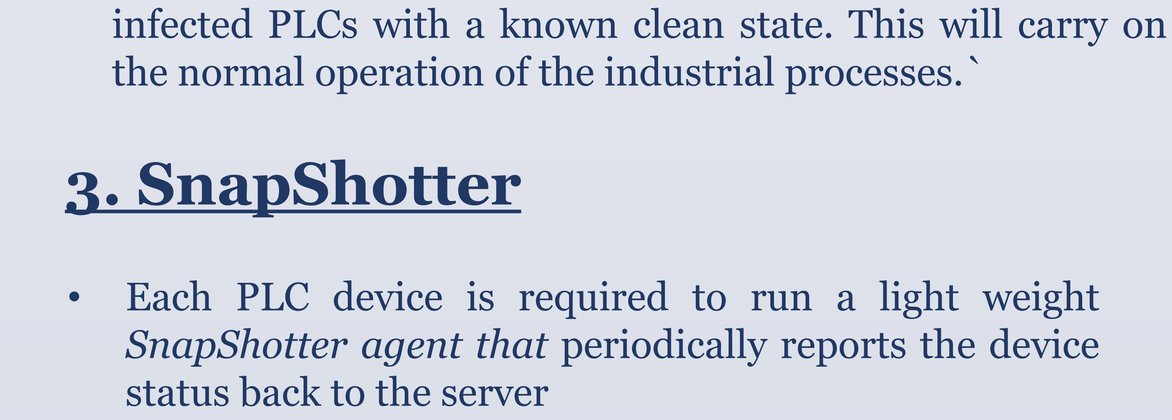
Malicious adversaries have gained access to PLCs, and submitted any malicious logic to the PLCs to generate arbitrary outputs from the PLCs to further hurt the industrial processes.

Our Solution:

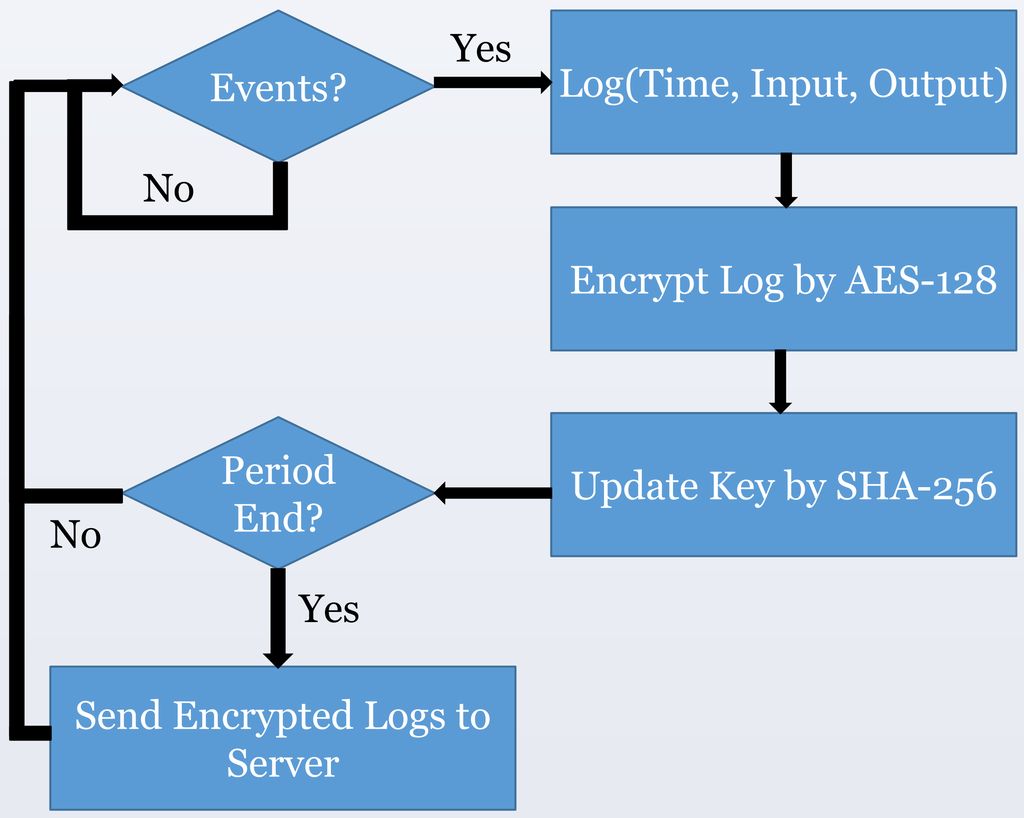
- Stealthy logging mechanism, called SnapShotter Agent.
- The status of each PLC is logged and sent to a central monitoring server in a **secure** and **stealthy** way **periodically**.
- The integrity of the logs can be verified by the server.
- The adversary is not able to infer whether he gets caught or not.
- If an intrusion is detected, the server will restart the infected PLCs with a known clean state. This will carry on the normal operation of the industrial processes.`

3. SnapShotter

- Each PLC device is required to run a light weight *SnapShotter agent that* periodically reports the device status back to the server
- The server verifies the received log and the operation integrity
- If the received log is tampered or the operation is not valid, the server raises an alarm
- In case of an intrusion, the PLC device will be reset to a safe/clean state by the server

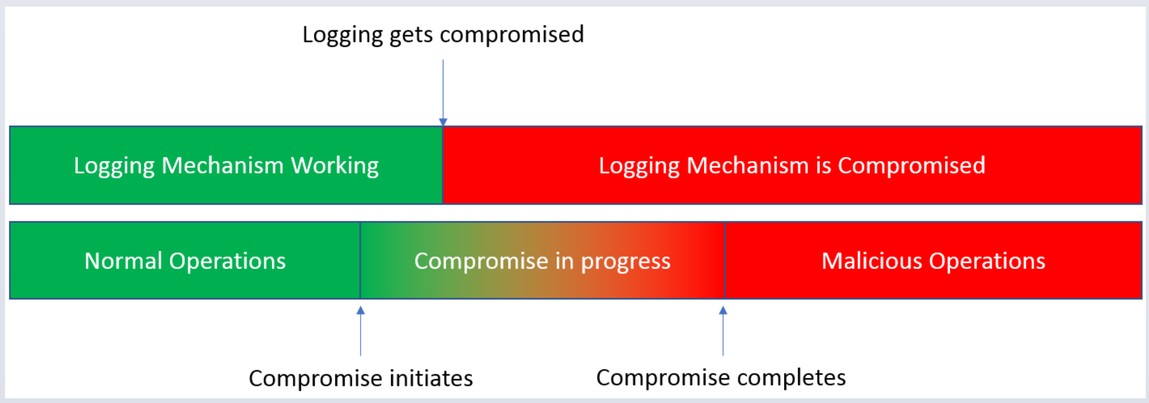


4. Agents and logging mechanism



5. Security Guarantees

Assumption: there exists a time window between the starting point of compromise and the moment that the logging mechanism gets compromised.



- Obfuscated log of all events (normal or malicious) with forward secure key generation
- Integrity of the logs can be verified
- Hiding from an attacker with access to the device whether the log reports detection of malicious behavior.
- The communication cannot be blocked, since the log is reported back at pre-defined time intervals.

6. Performance Overhead

- The measurement is done when the PLC is running simple HelloWorld logic.
- The average execution time of one scan cycle increases by 21.6%, comparing with the original OpenPLC design.

7. CONCLUSION

We have implemented a lightweight intrusion detection system to secure PLC systems by using simple and practical techniques such as PillarBox [1] .

REFERENCES

[1] Bowers, Kevin D., et al. "Pillarbox: Combating next-generation malware with fast forward-secure logging." *International Workshop on Recent Advances in Intrusion Detection*. Springer, Cham, 2014.