Digital Forensic Readiness For Critical Infrastructure

University of BRISTOL
Bristol Cyber Security Group

Feras Ibrahim Shahbi
Supervisor: Prof. Awais Rashid

Bristol Cyber Security Group | Department of Computer Science | University of Bristol

Background

- Catastrophic cyberattacks could cripple critical national infrastructures (CNI) on which the core of everyday life in our modern societies heavily relies.
- Critical infrastructure sectors' assets, systems, and networks are vital that their incapacitation would have a debilitating effect on security, national economic, security, human lives or any combination thereof.
- Their physical processes are controlled and monitored by industrial control systems *ICS* also known as Supervisory Control and Data Acquisition *SCADA* systems.

Challenges of ICS Forensics

Limited Computing Resources

Vendor-Specific Proprietary Firmware

High Availability

Insufficient Logging Capabilities

Variety of Engineering Software

Lack of Memory Imaging Tools

Motivation

- The ascent of sophisticated and state-sponsored cyberattacks against ICS (colonial pipeline, triton, industroyer , blackenergy, stuxnet ...etc)
- The lack of forensically sound tools, techniques and approaches for forensic investigation in SCADA environment.

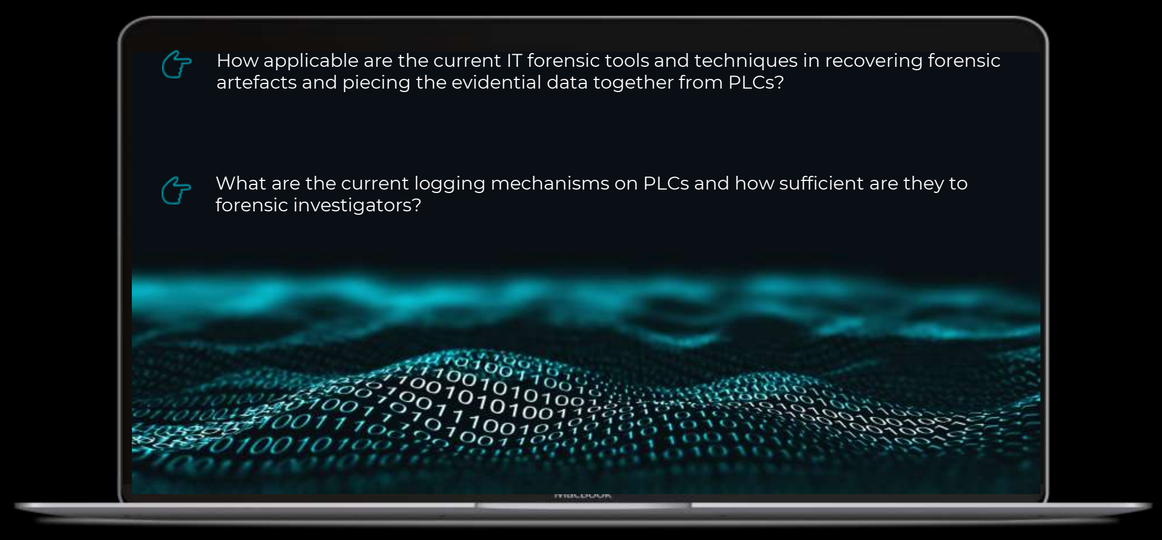
Main Objective

To derive an empirically-grounded host digital forensic framework tailored to PLCs in SCADA environment, and evaluate its effectiveness with regards to forensic soundness whilst maintaining the safety-critical properties.

Problem Statement

While there have traditionally been many applications of digital forensics and forensic readiness within the domain of personal and enterprise IT, much less attention has been directed at applying digital forensics to critical infrastructures. There is a lack of rigorous, evidenced-based host forensic techniques for analysing PLCs post-hoc a breach or even during an ongoing attack.

Year 1 Research Questions



Why host forensics (PLCs)

- Substantial Body of Work in IT Network Forensics May be Adopted.
- PLC Represents The Most Commonly Deployed Device across ICS.
- The Highest Level of Local Control Over a SCADA system.
- The Availability of a State-of-The-Art and Large Scale ICS Testbed in BCSG.

Industry Placement (Thales)

NDEC Site Visit → Lab Work → Structured Interviews