

Forensic Readiness for Critical National Infrastructure During Cyberwarfare Evaluating Logging and Evidence Collection Gaps

Presented by: Khadija Banu (2527944)

Background & Context

- Critical National Infrastructure is increasingly targeted by cyberattacks
- Cyberwarfare can target physical infrastructure
- IT networks are increasingly connected with OT/ICS
- This creates new attack paths into industrial environments
- Traditional digital forensics is mainly reactive
- Forensic readiness enables evidence collection before an incident

Research Problem

The Forensic Visibility Gap

- OT systems prioritise:
 - Availability
 - Safety
- Security logging is often limited
- Evidence can disappear very quickly

Research Aim

- Assess logging and forensic collection deficiencies in CNI
- Focus on simulated cyber warfare scenarios
- Investigate OT/ICS forensic limitations
- Develop an implementable forensic readiness framework
- Framework should be:
 - Tool-agnostic
 - Passive
 - Suitable for OT/ICS
 - Designed to preserve system availability

Research Objectives

1. Assess Evidence Gaps (Measure log lifetime, Identify at least three artifact collection limitations)
2. Compare IR Methodologies (Compare at least three DFIR methodologies, Focus on hybrid IT/OT/ICS environments)
3. Measure Technology Limitations (Measure CPU usage, Measure network latency, Evaluate traditional forensic tools)
4. Develop a Solution (Passive data collection, Out-of-band network tapping)

Literature Review: Key Themes

Cyberwarfare & CNI

- Increasing state-sponsored threats
- Attacks can target industrial protocols

Forensic Readiness

- Evidence must be collected and preserved proactively
- OT environments have major evidence gaps

OT/ICS Limitations

- PLC memory is highly volatile
- Traditional IT tools may not be suitable

Identified Research Gap

- PLCs operate using continuous scan cycles
- Malicious logic may be overwritten rapidly
- Evidence may disappear before acquisition
- Traditional IT forensic methods are difficult to apply safely
- Existing research identifies the problem
- Limited practical solutions exist

Proposed Research Approach

Traditional Approach

Incident > Active Extraction > System

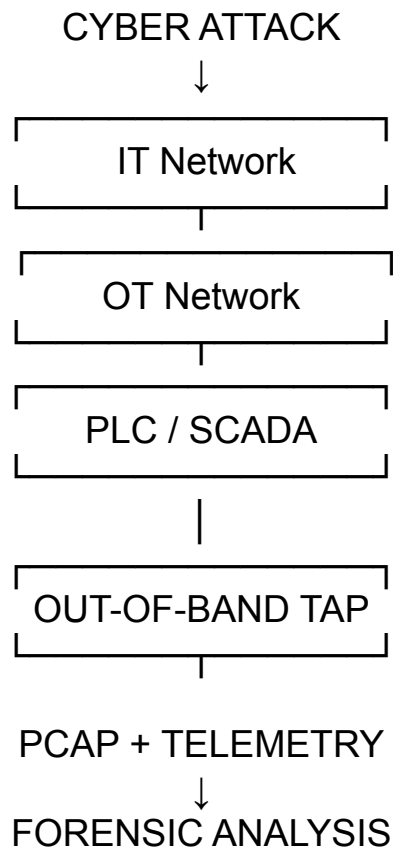
Impact > Evidence

Proposed Approach

Incident > Passive Network Capture >

Telemetry Collection > Evidence

Preservation



Research Design & Methodology

Design Science Research (DSR)

- Develop forensic readiness framework
- Address a real-world problem

Quantitative Experimental Simulation

- Controlled IT/OT/ICS laboratory
- Hardware-in-the-Loop (HITL)
- Simulated cyberwarfare scenarios

Experimental Method

Phase 1 — Attack Simulation

- Simulate IT - OT intrusion
- Measure evidence volatility

Phase 2 — Forensic Extraction

- Apply traditional IT-based techniques
- Measure operational impact

Phase 3 — Analysis & Validation

- Analyse PCAP and memory data
- Compare active vs passive collection

Research Metrics & Tools

- **Evidence Acquisition**
 - Quantity of recoverable forensic evidence
- **Network Latency**
 - Delay in milliseconds
- **Controller Availability**
 - Operational availability of controllers

Main Tools & Equipment

- KAPE
- Wireshark
- Python
- PLC
- HMI server
- Network taps
- Managed switches

Data Collection & Ethics

Data Collection

- Controlled IT/OT/ICS testbed
- Out-of-band network taps
- Raw PCAP files
- PLC volatile memory dumps

Ethical & Safety Controls

- Physically isolated laboratory
- No Internet connection
- No real CNI infrastructure
- Controlled cyber warfare simulation
- No exposure to public networks

Expected Outcomes, Limitations & Timeline

Expected Outcomes

- Improved evidence preservation
- Reduced impact on OT availability
- Better reconstruction of cyberattacks
- Reduced accountability gap

Key Limitations

- Lab testbed cannot fully represent national-scale CNI
- Limited access to classified threat intelligence

Timeline

- **Weeks 1–2:** Literature review & ethics
- **Weeks 3–4:** HITL testbed setup
- **Weeks 5–6:** Attack simulation & forensic extraction
- **Weeks 7–8:** Data analysis & validation
- **Weeks 9–10:** Final manuscript

Conclusion

- CNI faces increasing cyber warfare risks
- OT/ICS creates unique forensic challenges
- Traditional IT forensic approaches may be unsuitable
- Evidence can disappear rapidly
- Passive collection provides a safer alternative
- Research aims to improve forensic readiness and accountability

References

- [1] R. A. Awad, M. H. Rais, M. Rogers, I. Ahmed, and V. Paquit, "Towards generic memory forensic framework for programmable logic controllers,"
- [2] S. Ali Qasim, A. Ayub, and J. Johnson, "Attacking the IEC-61131 Logic Engine in Programmable Logic Controllers in Industrial Control Systems,"
- [3] R. M. Thompson, "Evaluating the Efficacy of KAPE and IT-Centric Triage Tools in Hybrid Environments,"
- [4] Federal Bureau of Investigation (FBI) and CISA, "Secure Connectivity Principles for Operational Technology (OT),"

Any Questions