vPLC: A Scalable PLC Testbed for IIoT Security Research

Syed Ali Qasim, Muhammad Taqi Raza, Irfan Ahmed
Grand Valley State University, University of Massachusetts Amherst, Virginia Commonwealth University
qasims@gvsu.edu, taqi@umass.edu, iahmed3@vcu.edu

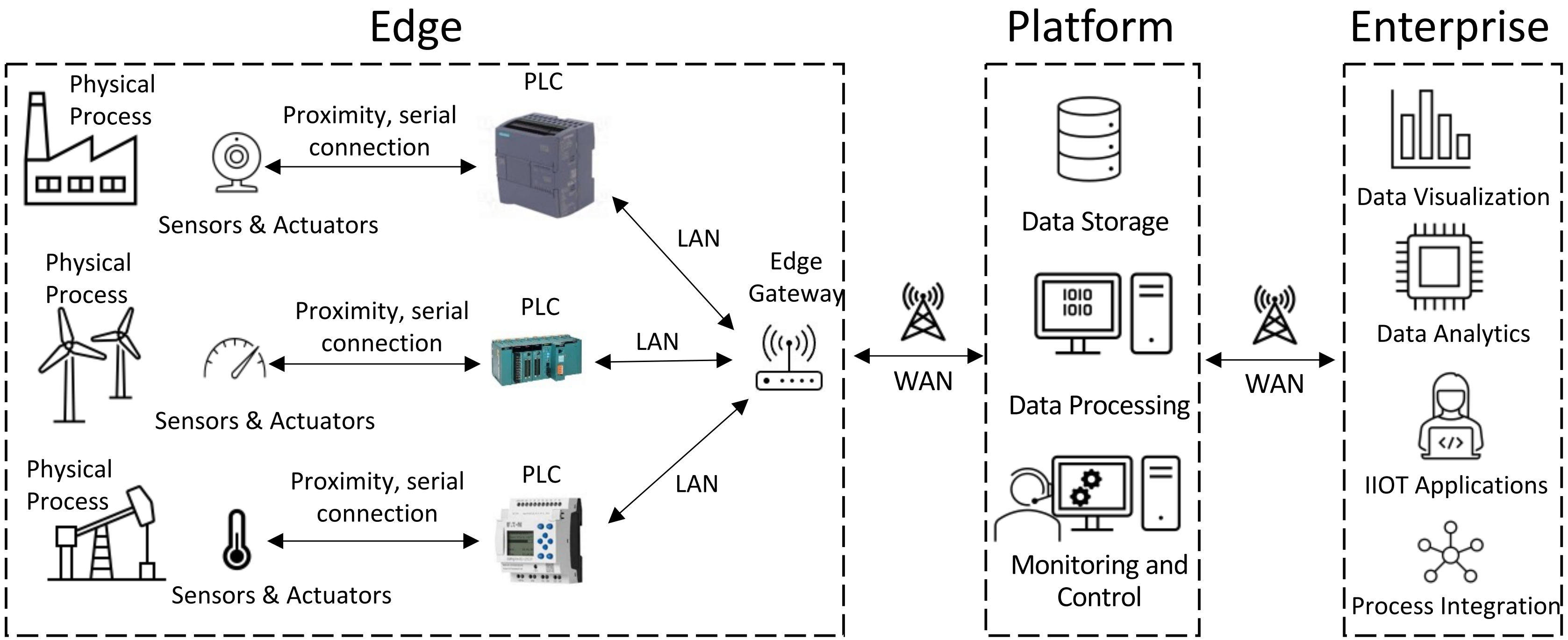
GRAND VALLEY STATE UNIVERSITY

SAFE Lab

Understanding IIoT and Cybersecurity

Brief Overview:

- Rising Importance of IIoT
- Challenges in Cybersecurity
- Need for Advanced Security Solutions



The Role of PLCs in Industrial IoT

Programmable Logic Controllers:

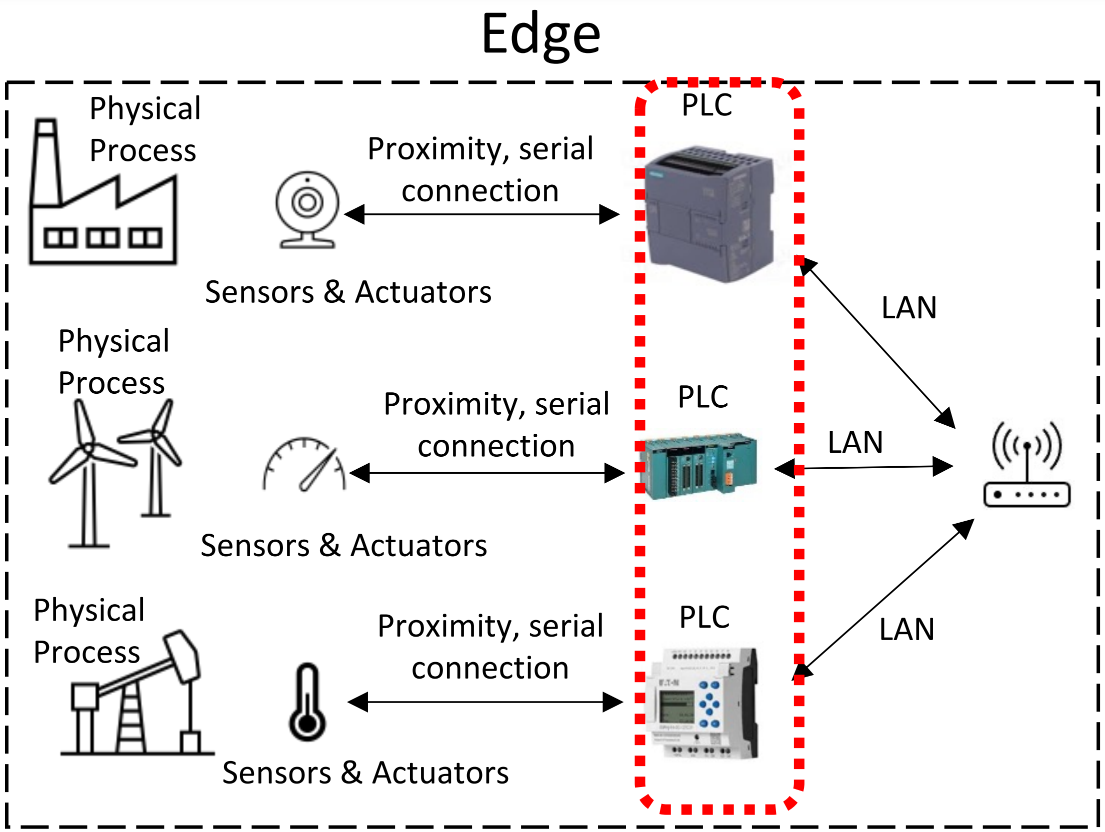
- Controls Machinery and Processes
- Real-time Monitoring and Decision-making

Integration of PLCs in IIoT Systems:

- Connects Physical Operations to Digital Networks
- Key in Smart Manufacturing and Industry 4.0

Importance of PLC Security:

- Critical for Industrial Safety and Reliability
- Target for Cybersecurity Threats in IIoT



The Need for Realistic IIoT Security Testbeds

Shortcomings of Existing Testbeds

- Industrial environments: Data acquisition challenges, not suitable for disruptive experiments
- Laboratory testbeds: Lack scale for comprehensive studies

Ideal Testbed Characteristics

- Scalability, configurability, and durability

Physical vs Virtual Testbed

- Challenges with physical testbeds: Limited scalability, restricted configurability, high repair costs

Introducing vPLC - A Novel Solution

Concept of vPLC

- A virtual PLC testbed
- Simulates PLCs in a software environment

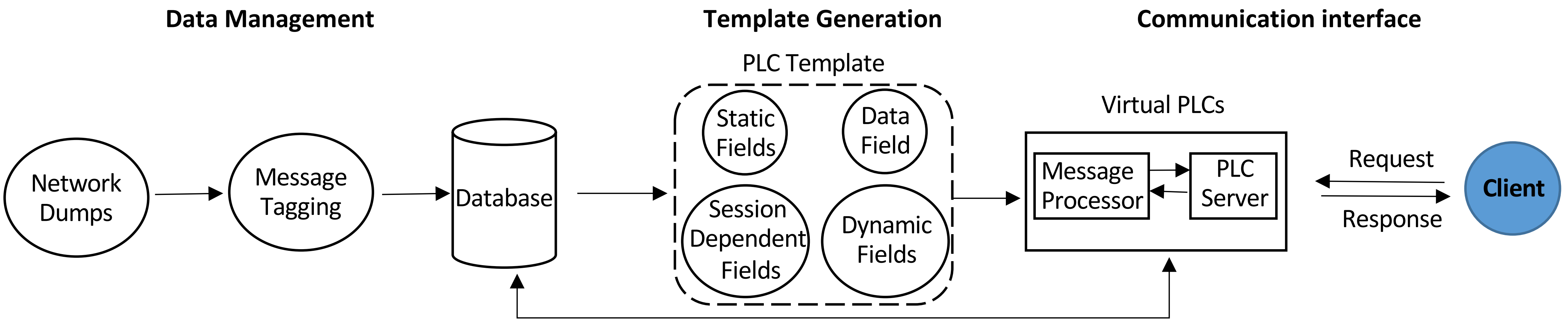
Innovative Approach

- Learn the protocol semantics and utilizes packet replay with real PLC network dumps
- Mimics actual PLC network behavior effectively

Advantages of vPLC

- Robust, scalable, and cost-efficient
- Ideal for extensive IIoT research

vPLC Architecture



- vPLC has three modules
  - Data Management
  - Template Generation
  - Communication Interface

vPLC Architecture

Data Management

- Take network dumps from a real PLC communication
- Extract application-level request-response message
- Creates a database of request response pairs

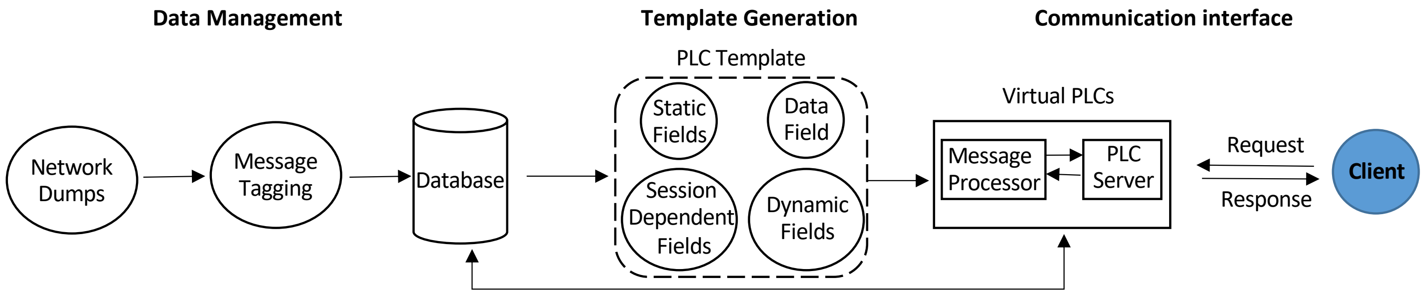
Template Generation

- User various heuristic based algorithms to identify various fields in the message
- Static fields
- Session-dependent fields
- Dynamic fields
- Control Logic fields

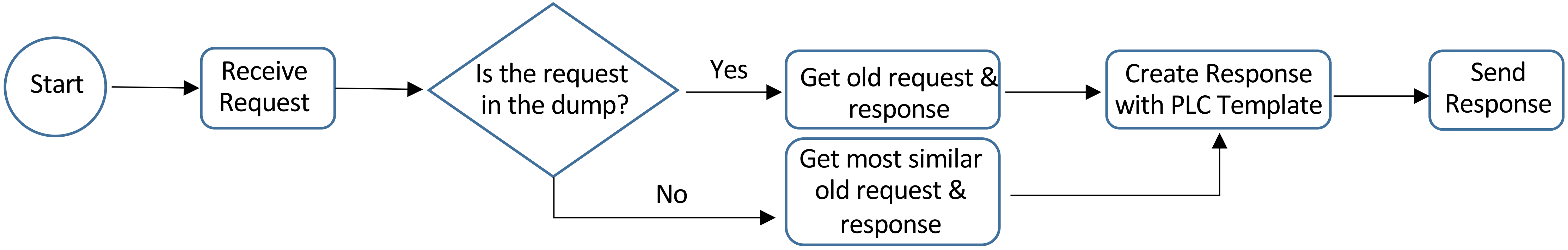
vPLC Architecture

Communication Interface- Virtual PLCs

- PLC server
- Message Processor



Flowchart of vPLC communication



vPLC Evaluation

Impersonation of a real PLC

- Network Discovery
- Connection Setup
- PLC operations

Ability to replay network dumps

- Database lookup
- Response message generation

Processing Time

- Processing time vs real PLC

vPLC Evaluation

Experimental Setup

- PLCs: Allen-Bradley MicroLogix 1400 and 1100, and Schneider Electric Modicon M221
- Engineering Softwares: SoMacineBasic, RsLogix

Experimental Methodology

- Capture the network communication of a real PLC
- Fed captured data into vPLC to instantiate virtual PLCs
- Impersonate the real PLC

vPLC Results

Impersonation of a real PLC

- 20 different control logic programs
- 100% Transfer accuracy

Control Logic Upload Accuracy of vPLC

PLC	# of control logic files uploaded	Original Program (Rungs)	vPLC Program (Rungs)	Upload Accuracy %
MicroLogix 1400	20	109	109	100%
MicroLogix 1100	20	235	235	100%
Modicon M221	20	211	211	100%

vPLC Results

Ability to Replay Network Traffic

- 60 experiments
- 7000 request messages received
- 100% lookup and response

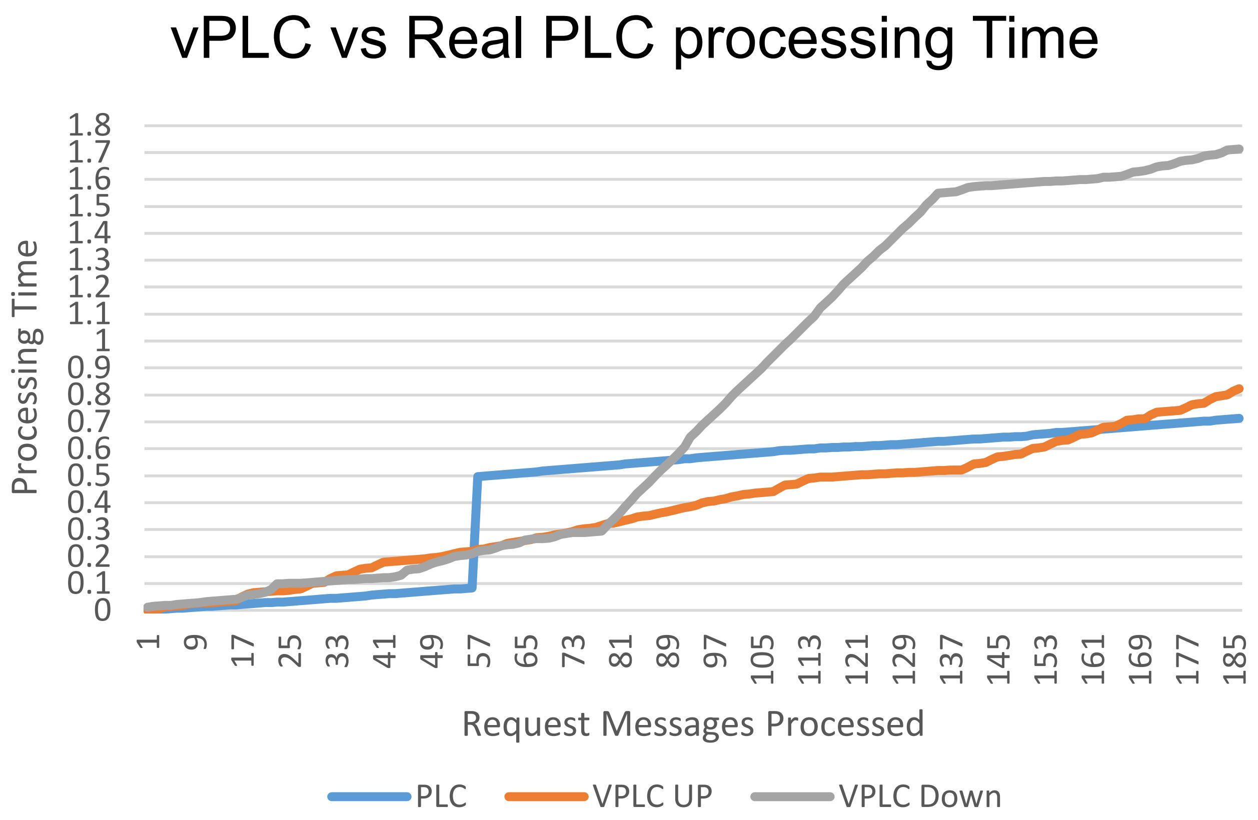
Request messages received by the virtual PLC & Database Lookup

PLC	# of Experiments	# of Request Messages Received	# of Request Messages Found in DB	Lookup Success %
MicroLogix 1400	20	2060	2060	100%
MicroLogix 1100	20	1440	1440	100%
Modicon M221	20	3500	3500	100%

vPLC Results

Message Processing Efficiency

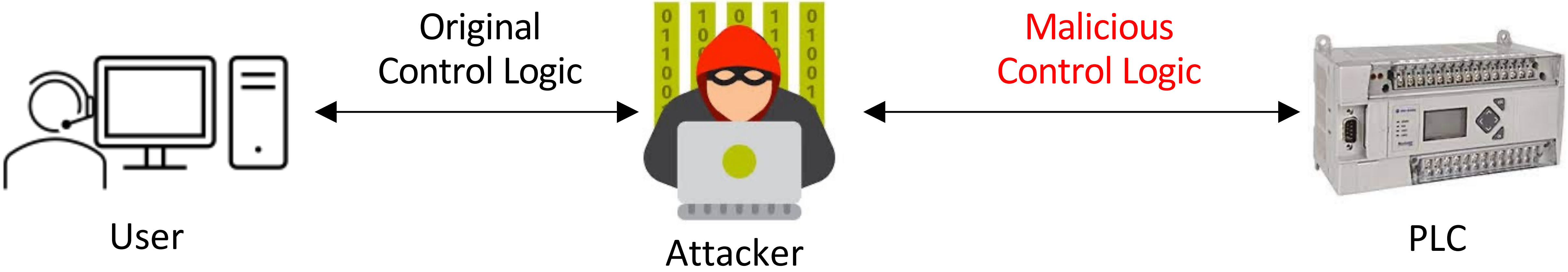
- M221 average time 0.0038
- vPLC impersonating M221 average time 0.0044
- vPLC processes requests faster when the network dump's operation matches the current operation
- No connection timeout/disruption



CASE STUDY: INVESTIGATING IIOT ATTACKS USING VPLC

Denial of Engineering Operations Attack (DEO I):

- Attacker performs MITM between the PLC and Control center
- Downloads a malicious control logic on the PLC
- Conceals compromised control logic from the engineering software



CASE STUDY: INVESTIGATING IIOT ATTACKS USING VPLC

Forensic Investigation of DEO I:

- Network Traffic if captured has evidence of manipulation of control logic

Challenges in Forensics Investigation:

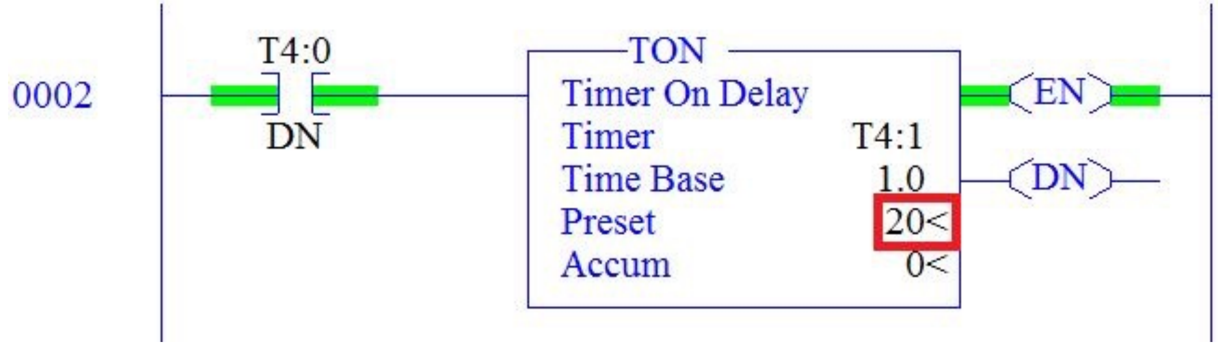
- Proprietary protocols (ENIP,PCCC)
- Binary control logic decompilation

Using vPLC for Investigation

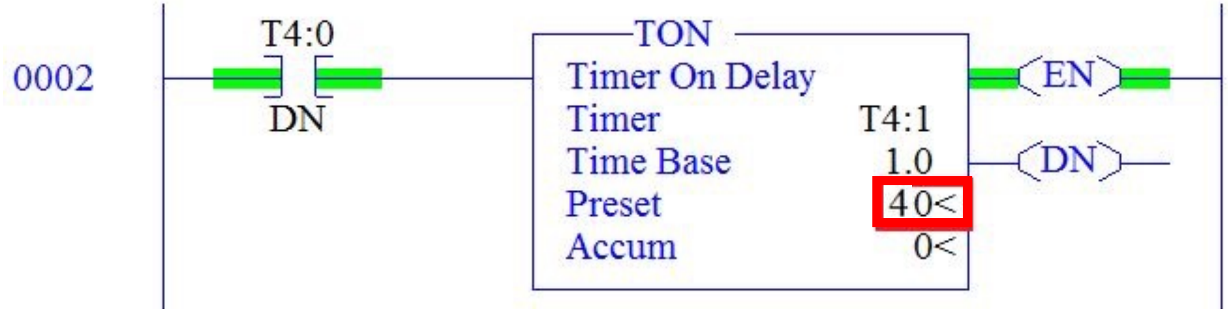
- Separate two network streams using MAC
- Use vPLC to replay both network dumps to engineering software

CASE STUDY: INVESTIGATING IIOT ATTACKS USING VPLC

Control Logic Retrieved Using vPLC:



Original Control Logic



Malicious Control Logic

Conclusion & Future Work

- Developed vPLC: A Scalable, Configurable, and Durable Testbed
- Evaluated vPLC Capabilities in Impersonating the Operation of Real PLCs
- Tested vPLC on Three Real-World PLCs
- Presented a Case Study on the Forensic Investigation of a Real Attack Using vPLC
- We are working on enhancing the capability and functionality of vPLC to develop PLC honeypots and gather threat intelligence

Thank You

Questions?