PLCPrint: Attack Fingerprinting

- **PLC memory fingerprinting approach** – aims to detect and classify different types of attack
- **Vendor-independent** PLC fingerprinting algorithm that uses corelations in **PLC memory registers**
- **Low overheads** and **generalisable**

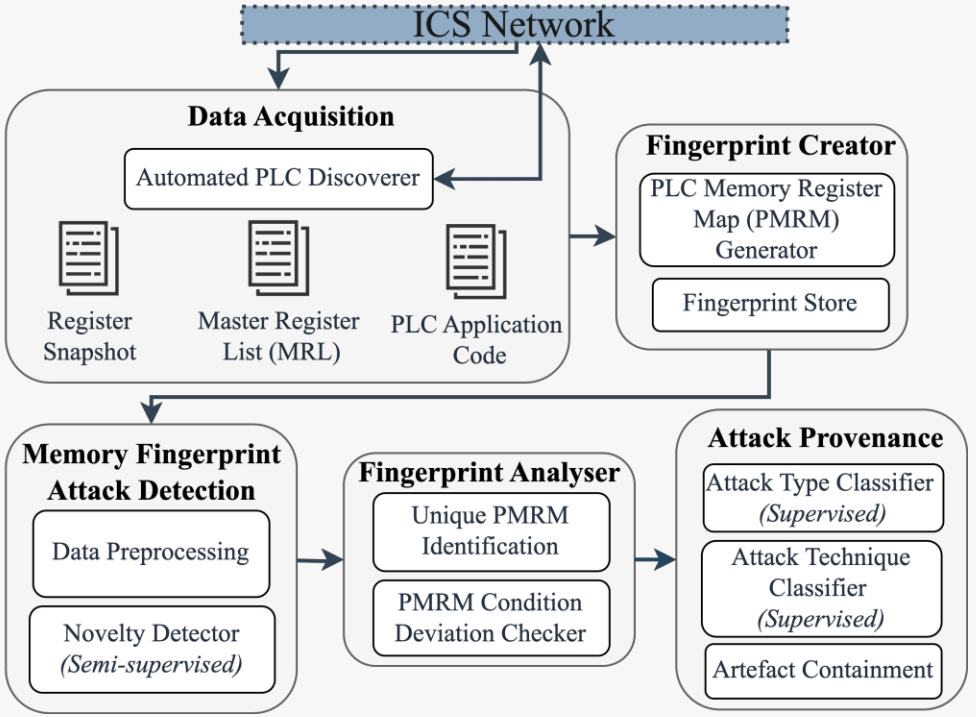


Fig 4. PLCPrint Architecture

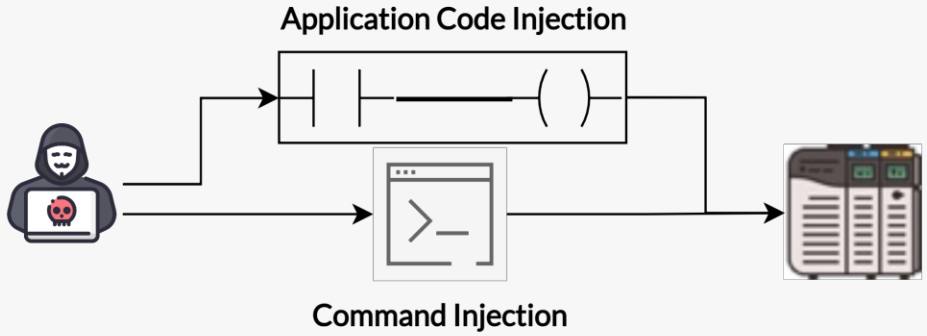
Attack Classification

- General threat model proposes **2 attack vectors**
  - Application code injection (static attacks)
  - Command injection (dynamic attacks)

- *Expectation:* **Behaviour** of PLC registers will **differ** between attack types and techniques

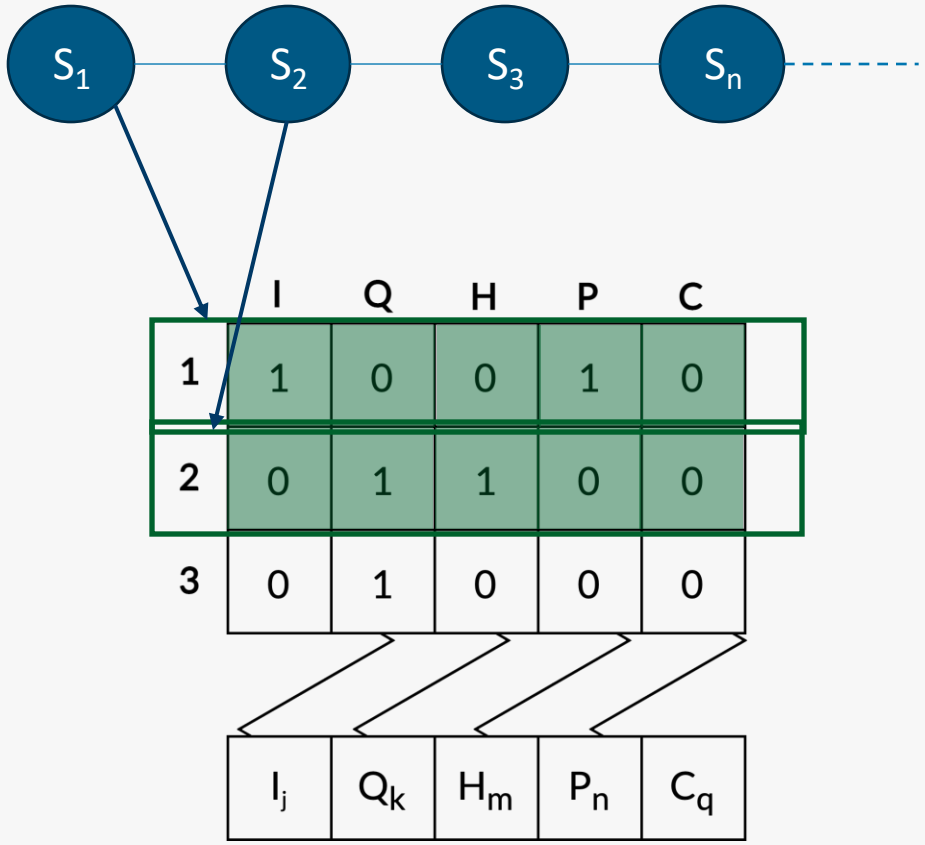
Attack Type	MITRE Technique	Observed In
Static	Program Download (T0843)	Stuxnet, IN-CONTROLLER (Pipedream)
	Modify Program (T0889) (StaticMP)	PLCBlaster, Stuxnet
	Modify Controller Tasking (StaticMCT) (T0821)	Triton
Dynamic	I/O Image (DynamicIO) (T0877)	Oldsmar Treatment Plant Intrusion
	Brute Force I/O (DynamicBF) (T0806)	Industroyer, Industroyer2

Table 1. PLC Memory Attacks and techniques



PLC Operation States

- Model PLC behaviour through set of finite states
  - State = Physical and Logical manifestations
- Represented by unique register combination
  - 5 register areas: Inputs (I), Outputs (Q), Holding bits (H), Timers (P), and Counters (C)
  - Number of registers per area is predefined
  - Registers are discrete (either 0 or 1 at point in time)



PLC Memory Register Mapping (PMRM)

- PLC application code – user-defined logic
- PLC registers provided with memory statuses – PMRM process
  - Dynamic Status – register active or inactive
  - Static Status – logically instantiated within application code function block (static instance)
- Mapping Conditions (MCs) – determined by combination of static and dynamic status (table 3)

MC	Dynamic	Static
MC1	0	0
MC2	0	1
MC3	1	0
MC4	1	1

Table 2. PMRM Mapping Conditions (MCs)

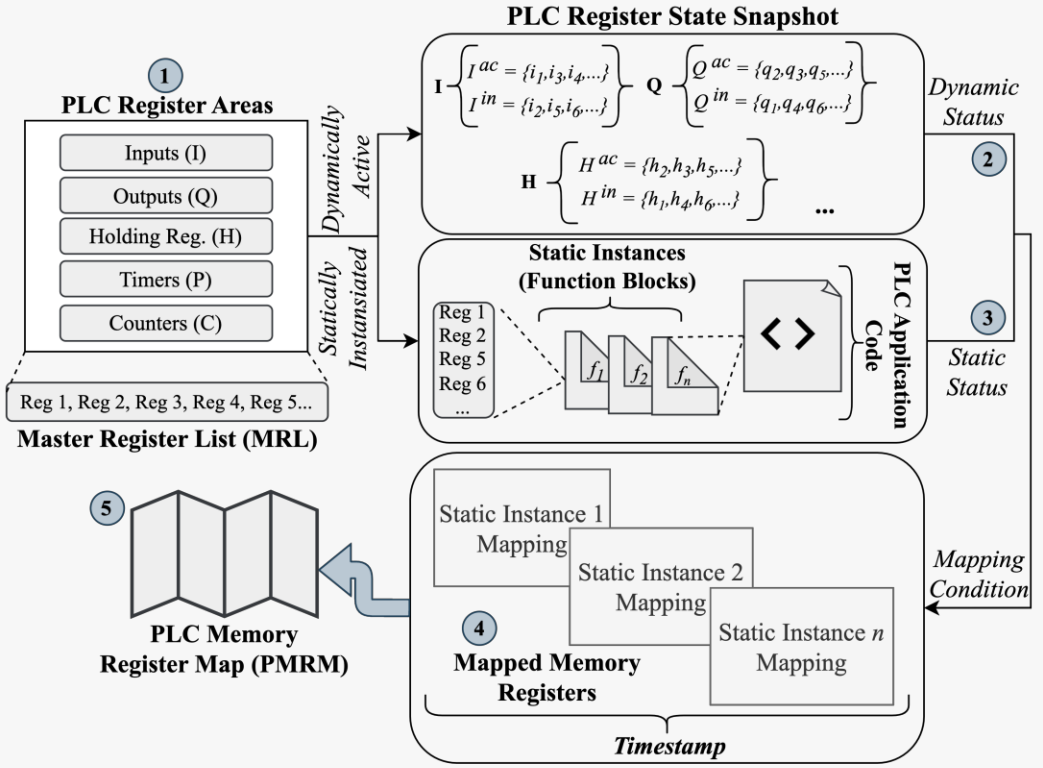


Fig 5. PLC Memory Register Mapping (PMRM) Approach

Evaluation and Results

- Some mapping condition (MC) correlations demonstrate better **differentiation** of attack types (Fig. 7)
- Combination of **MC2 and MC3** present **clearer separation** of clustering
- Attack techniques provide **denser clusters** (Fig. 8)
  - Greater similarities between **techniques from same attack type**

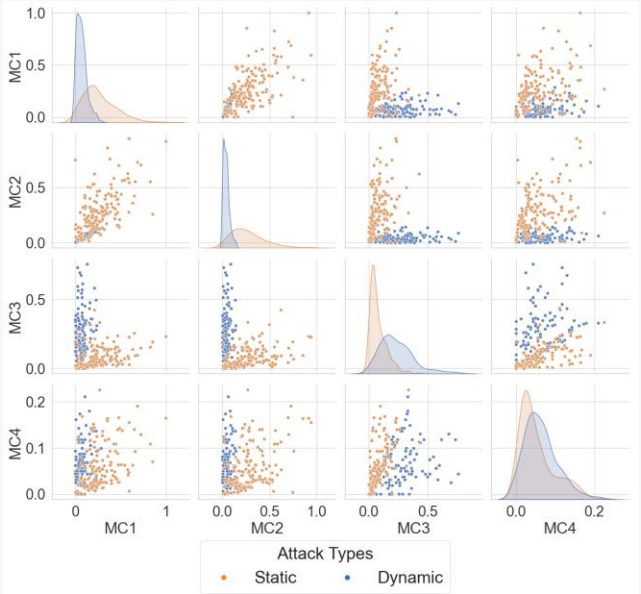


*Fig 7. MC distribution of attack **types***

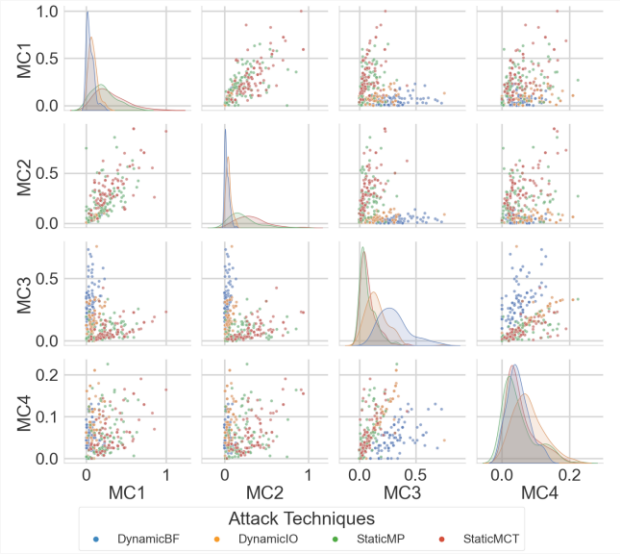


*Fig 8. MC distribution of attack **techniques***

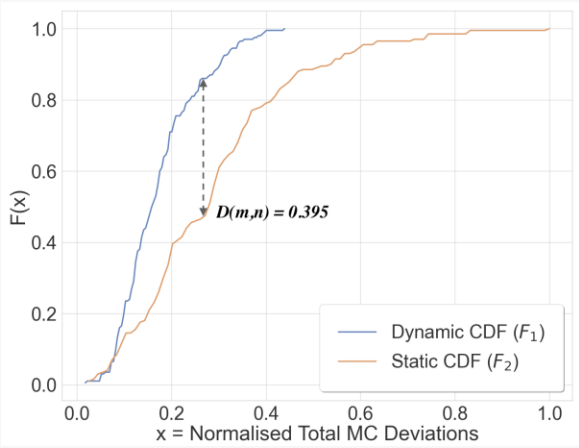


Fig 9. Statistical inference of attack types

Evaluation and Results

- **High accuracy** for detecting (95%) and correctly classifying (98%) attacks – optimal MC feature usage

- Generalisable performance:
  - Different PLC models
  - Multiple machine learning algorithms (e.g., K-Nearest Neighbour, Logistic Regression)

- Low overheads
  - Attack detection in < 500ms
  - Attack classification in < 1s (most cases)

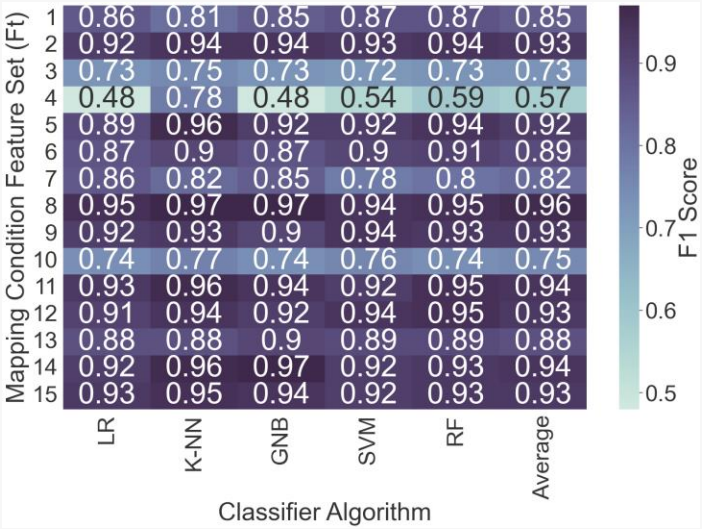


Fig 10. Attack classification

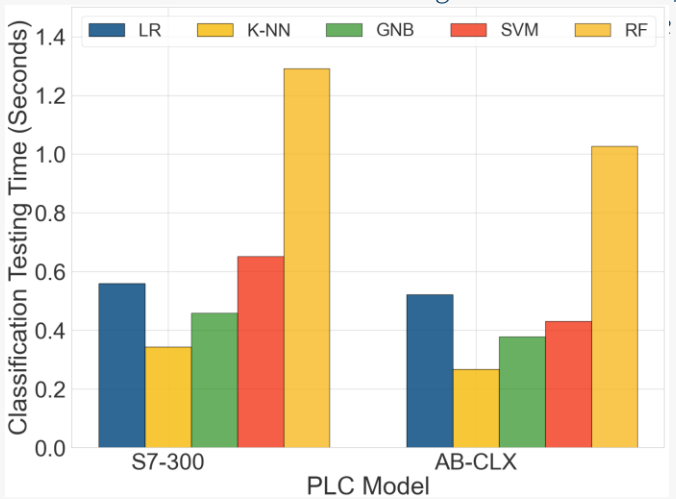


Fig 11. Computational performance – time taken to perform attack classification

Cook, Marco M., Angelos K. Marnerides, and Dimitrios Pezaros. "PLCPrint: Fingerprinting Memory Attacks in Programmable Logic Controllers." *IEEE Transactions on Information Forensics and Security* (2023). (doi: 10.1109/TIFS.2023.3277688)