PLCs Bewitched! Attacking the Control Logic through Design Flaws

Adeen Ayub, Wooyeon Jo, and Irfan Ahmed

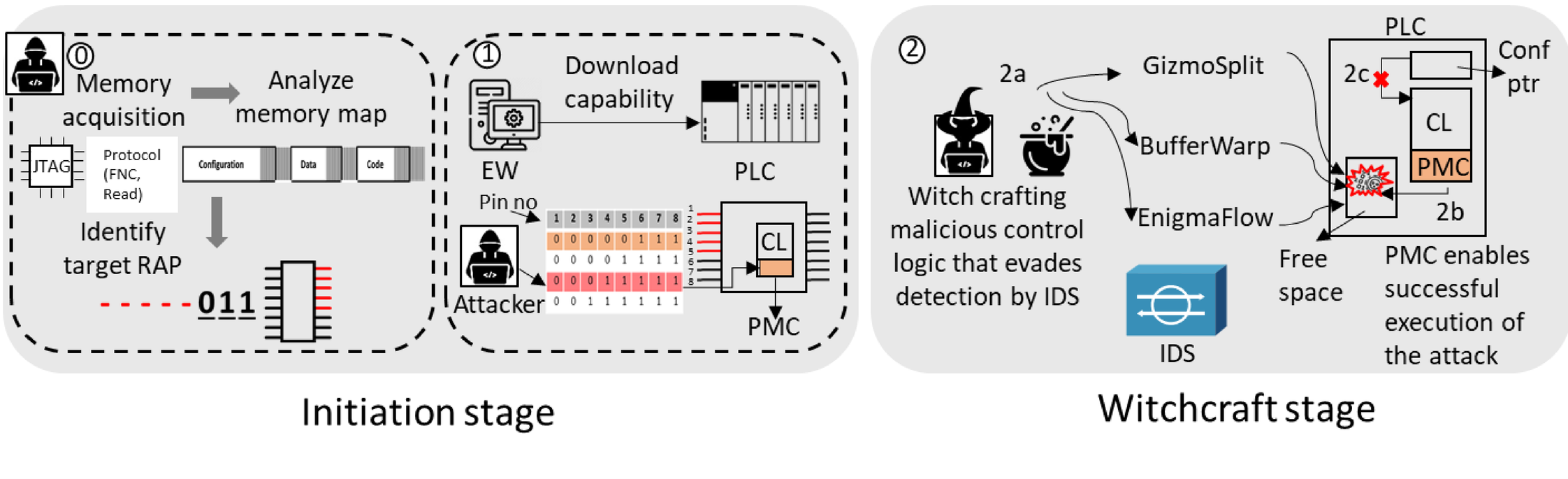
Motivation

- Programmable Logic Controllers (PLC) monitor and control critical infrastructures, including nuclear facilities and power grids
- They are targeted by malicious actors seeking to compromise control logic remotely
- Network intrusion detection systems (IDS) are deployed to detect malicious control logic
- Attackers' aim is to run a malicious control logic on a PLC without being detected by an IDS in place
- Standard IDS features such as entropy, n-gram, decompilation, are not resilient for detecting control logic binary programs

Introduction

- We identify a PLC design feature, redundant address pins (RAP), that enables attackers to inject a small piece of code known as programmable malicious code (PMC) to the control logic
- PMC acts as an initial vector and facilitates the seamless execution of malicious code with each scan cycle
- PMC is utilized for a discreet transfer of a complete malicious control logic over the network
- Three attack methods as PoC – GizmoSplit, BuffWarp, and EngimaFlow

Overview



Standard IDS features

- Protocol header
- Entropy
- N-gram
- Instructions
- Decompilation

GizmoSplit

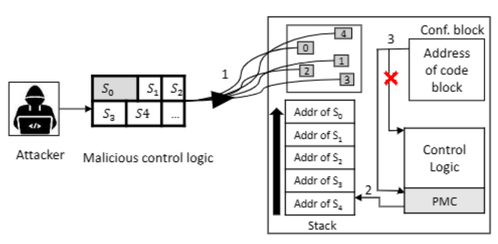


Fig. 3: GizmoSplit Attack

EngimaFlow

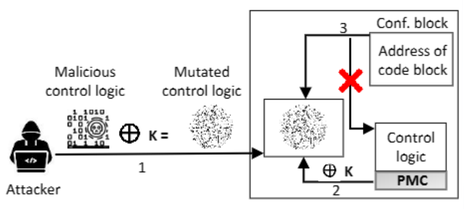


Fig. 5: EnigmaFlow attack

BuffWarp

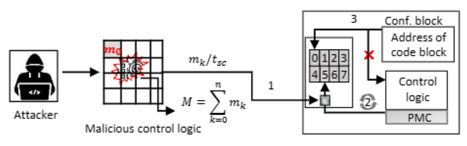


Fig. 4: BuffWarp Attack

Results

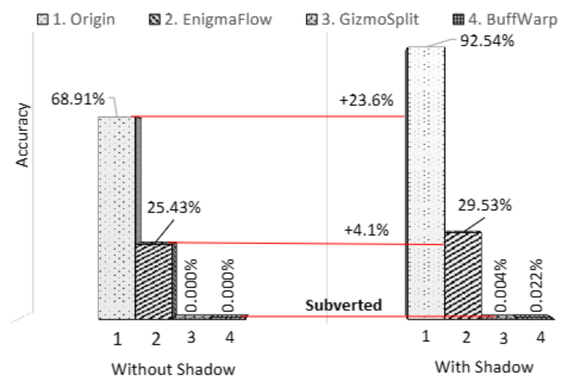


TABLE IV: Scaled Evaluation of Detected Semantic Features

Feature	Shadow Memory	Original	EnigmaFlow	GizmoSplit	BuffWarp
N-gram [27]	-	0.254	0.003	0.007	0.004
	✓	1.000	0.564	0.579	0.574
Decompilation [38]	-	0.688	0.291	0.027	0.017
	✓	1.000	0.505	0.418	0.039
Rung [19], [49]	-	0.805	0.733	0.001	0.000
	✓	1.000	0.809	0.003	0.001
Opcode [50]	-	0.634	0.702	0.023	0.023
	✓	0.884	1.000	0.023	0.023

High Medium Low