



POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Informatica

Master Thesis

## Pin Control Defense

Protecting Linux Kernel Pin Control Subsystem from Pin Control Attack

**Supervisor**

prof. Antonio Lioy

**Candidate**

Andrea GENUISE

ACADEMIC YEAR 2016-2017



*f A nonno Carmelo*

# Summary

Recently embedded systems have become more and more integrated with all aspects of our lives, and their security concerns have risen as well. They spread in various fields such as automotive, electronic devices, home automation, manufacturing and mission critical applications. These systems, in particular PLCs deployed within the context of an Industrial Control System, use Input/Output interfaces to interact with the physical world by means of sensors and actuators. As demonstrated by a novel kind of attack called Pin Control Attack, one can tamper with the integrity or the availability of legitimate I/O operations, factually changing how a PLC interacts with the outside world and possibly causing physical damage to people and environment. In this thesis we design a possible countermeasure to the attack and implement it for Linux Kernel on an ARM-based Programmable Logic Controller, showing its effectiveness and impact on PLCs which usually have very limited resources and strict timing requirements.

# Acknowledgements

TODO Acknowledgements.

# Contents

<b>Summary</b>	IV
<b>Acknowledgements</b>	V
<b>1 Introduction</b>	1
1.1 Programmable Logic Controllers . . . . .	1
1.2 Problem statement . . . . .	2
1.3 Aim of the thesis . . . . .	3
1.4 Organisation . . . . .	4
<b>2 Related work</b>	5
2.1 Attacks . . . . .	5
2.1.1 Firmware modification attacks . . . . .	6
2.1.2 Logic modification attacks . . . . .	6
2.1.3 Control flow modification . . . . .	6
2.2 Defenses . . . . .	6
2.2.1 Firmware integrity . . . . .	7
2.2.2 Intrusion detection . . . . .	8
2.2.3 Control flow integrity . . . . .	8
2.3 Hardware-level attacks and defenses . . . . .	9
<b>3 Pin Control Attack</b>	11
3.1 Embedded architecture . . . . .	11
3.1.1 SoC pins . . . . .	12
3.1.2 PLC architecture . . . . .	14
3.2 Attack Design . . . . .	17
3.2.1 Defense analysis . . . . .	18
3.2.2 Threat model . . . . .	19
3.2.3 Pin Control Attack . . . . .	19
3.3 Attack Implementation . . . . .	21
3.3.1 Raspberry Pi . . . . .	21
3.3.2 PLC . . . . .	24

<b>4 Pin Control Defense</b>	30
<b>5 Experimental Results</b>	31
<b>6 Conclusions</b>	32
<b>Bibliography</b>	33

# Chapter 1

## Introduction

Embedded systems are widely used today in various applications, from cars, cell phones, home automation, to critical infrastructures like power plants and power grids, water, gas or electricity distribution systems and production systems for food and other products.

Since they were almost isolated from the network, embedded systems have not been designed and built with security concepts in mind. However, many recent cyber-attacks demonstrated that such an assumption is no more valid, and the security of embedded systems became an open question to deal with.

Unfortunately, this could be a more challenging problem with respect to security for desktop and enterprise computing, for the following reasons:

- the limited capabilities and the strict timing requirements these systems have;
- the physical side effects a security breach may lead to, e.g. property damage, personal injury, death and even environmental or nuclear disaster.

In the next sections we first describe a particular type of embedded systems, then present the problem on which the rest of the paper is focused and clarify the goal of this thesis.

### 1.1 Programmable Logic Controllers

Within the context of an Industrial Control System (ICS), embedded systems are better known as Programmable Logic Controllers (PLCs). PLCs are special-purpose embedded systems, usually deployed into harsh environments to control critical processes, e.g. automotive systems, assembly lines, robotic devices or any industrial machine that requires high control precision and reliability.

A simplified version of the environment in which a PLC may operate is outlined in Fig. 1.1.

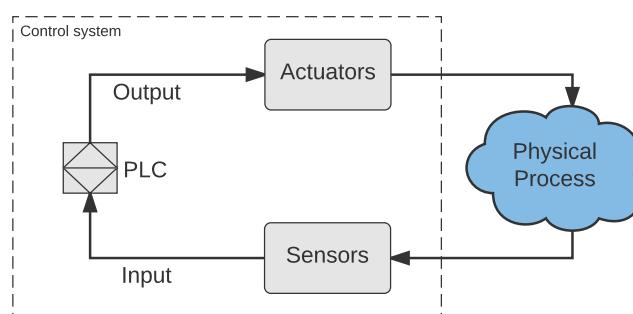


Figure 1.1: PLC environment

The PLC interacts with the physical world through external components called *sensors* and *actuators*. The sensors are responsible for reporting measurements about a set of properties of the physical process, while the actuators, as the name suggests, acts on the process modifying its current state.

The main task of the PLC is contained into the control program (the *logic*) which is programmed and loaded by the industrial operator or supervisor. The logic is executed repeatedly as long as the controlled system is running. Each single execution is known as *scan cycle*. For each scan cycle, the PLC reads the current state of the physical process measured by sensors. Internally, the logic takes these values as input and performs some calculations based on the loaded control algorithm. The output of the logic is then sent to the actuators, thus modifying the state of the controlled process.

The PLC main scan cycle is shown in Fig. 1.2.

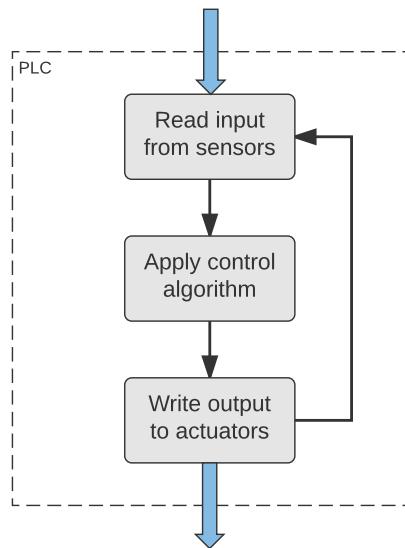


Figure 1.2: PLC logic main scan cycle

Based on the nature of the controlled process, the logic must satisfy different safety and timing properties. Furthermore, the majority of the PLCs are provided with a real-time operating system, in order to guarantee that the strict timing requirements are always respected. A violation of these requirements may lead to an unsafe behaviour of the physical process, and the consequences are heavily related to the nature of the process under control.

## 1.2 Problem statement

From a computer engineering perspective, PLCs control the outside world via their Input/Output (I/O) interfaces, also known as *pins*. Therefore, it is crucial that they are both reliable and secure. I/O pins are accessible through a specific memory region, called I/O memory. The I/O memory includes a set of registers through which the I/O can be configured. The I/O configuration (also called I/O initialisation) is typically performed at start-up time, according to the specific implementation. However, on almost every system it is possible to overwrite this configuration at run-time.

The problem here relies on the fact that there is neither any memory protection mechanism nor any hardware interrupt designed for restricting the access to I/O memory addresses. They can be easily written by a malicious application even while the system is running, thus over-writing the hardware configuration. As a consequence, the behaviour of the I/O interface, hence the interaction

with the physical process, may be altered in a dramatic way. In [1], Abbasi et al. showed how this feature is exploitable by attackers, who can tamper with the integrity or the availability of legitimate I/O operations, factually changing how a PLC interacts with sensors and actuators. Based on these observations, they introduced a novel attack technique against PLCs, which they call Pin Control Attack (also I/O attack [2]). The salient features of this new class of attacks are:

1. It is intrinsically stealth. The alteration of the pin configuration does not generate any interrupt, preventing the Operating System (OS) to react to it.
2. It is entirely different in execution from traditional techniques (e.g. manipulation of kernel structures or system call hooking) which are typically monitored by off-the-shelf protection systems.
3. It is viable. It is possible to build concrete attack using it.

To better understand a possible attack scenario, Fig. 1.3 shows a simplified control system.

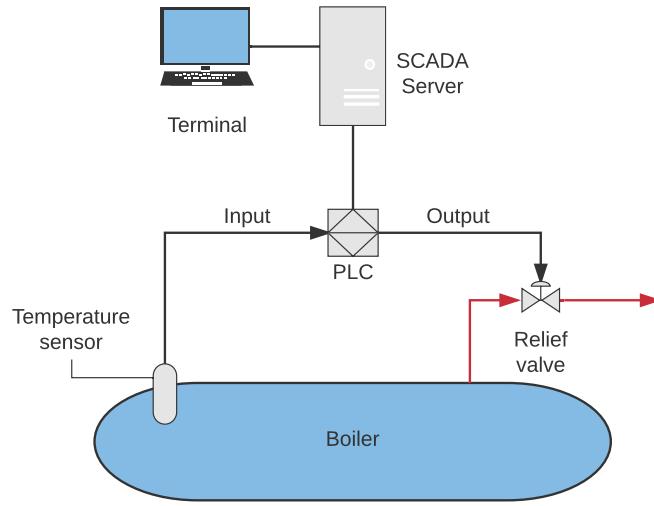


Figure 1.3: Simplified control system: a possible target of Pin Control Attack.

The system consists of a boiler equipped with a relief valve driven by the PLC according to the value provided by a temperature sensor. The PLC is connected to a SCADA server (Supervisory Control And Data Acquisition) to keep trace of its operation. The server is accessible from a terminal, through which an operator can load the logic into the PLC and monitor its current state.

Suppose that the PLC logic is programmed to read the values from the temperature sensor, and to open the relief valve if the temperature goes over  $80^{\circ}\text{C}$ . An attacker could tamper the temperature value read by the PLC, re-configuring the pin related to the sensor as output and writing its own desired value (e.g. always  $50^{\circ}\text{C}$ ) regardless of the actual temperature. Even simpler, one could reconfigure the pin connected to the valve (e.g. setting it as input) factually disabling any eventual command to the actuator.

Actually there is no detection mechanism able to react to these configuration changes, neither in the PLC firmware nor in the control system. Moreover, the operator of the control system will not be able to see the real temperature nor the actual valve state from the terminal, so it may likely not notice the intrusion at all. Such a condition may lead to an uncontrolled overheating, and if it is not detected in time it could even make the boiler to explode.

### 1.3 Aim of the thesis

The goal of this thesis is to design and develop a defensive mechanism against Pin Control Attack, extending the pin controller in order to be able to detect it. It is a challenging task for two reasons:

1. The pin control mechanism lacks hardware interrupts, so it is not possible to directly react to any configuration change. More complex detection mechanisms are needed in order to achieve the highest possible detection rate.
2. The resources available within an embedded system like a PLC are extremely limited. Therefore, our solution must be extremely agile and light since the smallest delay in the PLC I/O operation may have unintended consequences for the controlled process.

The work has been divided into three main steps. First, we discuss the idea behind Pin Control Attack, analyse its threat model and different implementations on an Embedded Linux ARM-based architecture. Second, based on the assumptions contained in the threat model, we describe and evaluate the design and the implementation of our defense. Finally, we validate the proposed architecture on the target system.

The target of our implementation is a real-time version of the Linux kernel running on an ARM-based SoC, as this is one of the solutions actually used for mid-range embedded systems, in particular PLCs. In the context of the Linux kernel, the pin controller is known as Pin Control Subsystem [3]. The implementation will be validated with respect to the following parameters: detection rate and performance overhead.

A brief organisation of the rest of the thesis follows in the next section.

## 1.4 Organisation

In Chapter 2 we list the known attacks to embedded systems existing in the literature, and then discuss the off-the-shelf protection mechanisms. To the best of our knowledge at the time of writing, as Pin Control Attack is a new kind of attack, none of the existing protections is able to prevent nor detect it. Chapter 3 contains, after a brief description of the embedded systems architecture, a detailed analysis of Pin Control Attack design and implementation. In Chapter 4 we present the architecture of our proposed Pin Control Defense, then we describe the implementation and provide developer and user manual for it. The Chapter 5 provides the results obtained during the experiments, showing the detection rate and the performance overhead on a PLC environment. Finally, in Chapter 6 we analyse the shortcomings of our defense and the possible future works and improvements.

# Chapter 2

## Related work

In this chapter we summarise the state of the art about security of embedded systems at the time of writing. First, we discuss about the attacks of the recent years, showing how the embedded systems security concerns are rising. Next, we analyse the defense mechanisms currently available in the literature, realising that they are still in a very early stage of their life. Finally, we consider the existing attacks and defenses targeting the hardware level, as Pin Control Attack does, showing that they are currently not applicable to embedded systems.

### 2.1 Attacks

In the past few years we have seen several attacks targeting embedded systems: most notably the infamous Stuxnet [4] targeting an Iranian nuclear facility in 2010. More recently Grandgenett et al. [5] analysed the authentication protocol between the RSLogix 5000 software and the PLC, based on a simple challenge-response mechanism. Since the protocol lacks freshness in its messages, is vulnerable to replay attacks, through which an attacker could repeat privileged commands to the PLC. Furthermore, they found that both the decoding of the challenge and the encoding of the response use an RSA-2048 key which is hard-coded in the RSLogix software, and it is actually valid for any Rockwell/Allen Bradley PLC. This indicates how the security mechanisms of these systems often have a really poor design, if any.

Papp et al. [6] analysed the existing attacks on embedded systems, relying on the proceedings of security conferences, with a focus on computer hacking, and on the Internet for media reports, blogs and mailing list. They built a taxonomy based on five dimensions: precondition, vulnerability, target, attack method and effect of the attack, showing that the threats to embedded systems are similar to the ones that affect traditional IT systems. However, embedded systems still lack solutions and tools to address these issues, and many ongoing research efforts are trying to deploy and adapt them to the needs of this field.

For our purpose, we may classify the attacks found in literature using a simpler criterion based on the attack method. We may distinguish three main categories:

1. **Firmware modification:** all the attacks aiming to upload a malicious firmware version (or part of it) in the device belong to this category.
2. **Logic modification:** this category consists of the attacks that modify the PLC logic in some way. In this case the integrity of the firmware is not violated, but a malicious program, or logic, is inserted into the PLC to make it misbehave during the control process.
3. **Control flow modification:** it includes the attacks that alter the normal control flow of a process by leveraging classic programming vulnerabilities such as buffer overflow or expired pointer dereference.

We briefly report about these different kind of attacks in the following sections.

### 2.1.1 Firmware modification attacks

Almost all modern embedded systems provide a way to update the firmware, and the attackers could exploit this feature to upload its own malicious firmware. Basnight et al. [7] reverse engineered an Allen-Bradley ControlLogix L61 PLC firmware showing how to bypass the firmware update validation method and successfully upload a counterfeit firmware. Peck et al. [8] demonstrate how using commonly available software an attacker can write and load his malicious firmware into Ethernet cards of devices used in control systems, potentially infecting the entire industrial control system. Cui et al. [9] discovered a vulnerability in the HP-RFU (Remote Firmware Update) feature of LaserJet printers, that allows remote attackers to make persistent modifications to the printer's firmware by simply printing to it.

### 2.1.2 Logic modification attacks

Stuxnet [4] belongs to this category. Along with its several components, mainly used to replicate and control the malware, its core is essentially an infected version of a SCADA software library used to program the PLC itself. By hooking some of the library functions it is able to load infected code and data blocks into the PLC and hide itself from the operator. McLaughlin et al. [10, 11] evaluated some techniques and implemented a tool (SABOT) to infer the structure of a physical plant and craft a dynamic payload, allowing an attacker to cause an unsafe behaviour without having a deep *a priori* knowledge of the target physical process. Similar techniques might mitigate the precondition needed by an attack, making it even more viable. Beresford [12] showed how the PLCs and the protocols used for communication in control systems were built without any security in mind, and demonstrated that they are affected by many vulnerabilities which may also enable the attacker to know the current configuration and rewrite the PLC logic. More recently, Klick et al. [13] used an internet-facing PLC as a network gateway by prepending a backdoor, made of a port scanner and a SOCKS proxy, to the existing logic code of the PLC. They developed a proof-of-concept tool called *PLCInject* to demonstrate their approach and measure the effects on the network.

### 2.1.3 Control flow modification

Many recent advisories [14–19] from ICS-CERT (Industrial Control System Cyber Emergency Response Team) report about various programming vulnerabilities affecting both PLC firmwares and control softwares. Most of them allow remote code execution and could be exploited without requiring particularly high skills. The vulnerabilities discovered by Beresford [12] also allow the attacker to insert a payload into the logic and subvert the control flow to execute malicious code. Nevertheless, the majority of the PLCs run the applications with root privileges, so it is quite simple for an attacker to get a root shell. One of the most dangerous kind of control flow attacks consists of ROP (Return-Oriented Programming) techniques, or similar variants [20, 21] which leverage different sequence of instructions equivalent to a return instruction. Since code vulnerabilities may affect embedded systems [12, 16–19], ROP techniques are applicable as well. Furthermore, due to the limitations imposed by these systems, is even more challenging to defend against them.

## 2.2 Defenses

Even though many incidents in SCADA systems occurred in the past decades [22, 23], the scientific community, together with PLC producers (Siemens, Hitachi etc.) and antivirus producers (Symantec, Kaspersky etc.), started to explore the security concerns of these systems only after the discovery of Stuxnet malware in 2010.

Since the communication protocols are the most vulnerable area in embedded systems, many efforts have been directed to *network-based* defenses [24]. In 2013, Clark et al. [25] designed a defense scheme against Stuxnet in which commands from the system operator to the PLC are

authenticated using a randomised set of cryptographic keys. Hadiosmanovi et al. [26] proposed a semantic-aware intrusion detection system, which is able to build a prediction model by observing the values of the process variables from the network communication, and then detect unauthorised changes with respect to the model.

In our work, however, we will focus on *host-based* defenses, in which the protection mechanism resides in the embedded system itself. Similarly to what we did for attacks, we can divide host-based defenses into the corresponding categories:

1. **Firmware integrity:** includes all the available techniques for preventing or detecting any malicious change in the PLC firmware.
2. **Intrusion detection:** host-based intrusion detection systems responsible for detecting rootkits or malicious software that could tamper with the normal process controlled by the PLC.
3. **Control flow integrity:** all the available mechanisms to defend against control flow attacks, like control flow integrity techniques or anti-ROP defenses, belong to this category.

### 2.2.1 Firmware integrity

In order to detect malicious modifications in the firmware of embedded systems, Wang et al. [27] proposed ConFirm, a low-cost technique, embeddable into the bootloader, based on measuring the number of low-level hardware events that occur during the execution of the firmware. To count these events, ConFirm leverages a set of special-purpose registers, the Hardware Performance Counters (HPCs), which readily exist in many embedded processors. The approach is divided into two phases: offline profiling and online checking. The offline profiling is executed before the system is deployed, and consists of registering the HPC signatures of code paths from a clean copy of the targeted firmware. The signature database is then embedded into the bootloader together with the ConFirm payload executed in the second phase. During the online checking, the same monitored paths are measured and compared to the golden references. Although this technique raises the bar for firmware modification attacks, if an attacker is able to reverse engineer and modify the bootloader, which usually has some update procedure as well, then the entire mechanism could be circumvented.

Other approaches that could defend against firmware modifications are based on a Trusted Execution Environment. While this kind of technology is commonly deployed in more capable systems, such as desktop or enterprise, the most of the embedded systems need a solution with lower resource requirements. The TrustZone Technology [28] enables trusted computing for ARM platforms by extending the hardware architecture, essentially the system bus, the processor core and the debug infrastructure, with security-aware components. Furthermore, Koeberl et al. [29] proposed a hardware-enforced security architecture named TrustLite, which is able to provide trusted computing capabilities on resource-constrained embedded devices without requiring CPU security extensions.

A trusted computing architecture can also enable attestation, through which a system, called verifier, can verify the integrity state of another system, called prover, which should provide a cryptographic proof of its integrity. Similar technologies could also be used to design a secure firmware upgrade mechanism. The PLC vendors need the possibility to provide firmware updates for their own devices, most likely when some vulnerabilities are discovered after release. Fuchs et al. [30] discussed the benefits of Trusted Computing Group’s Trusted Platform Module (TPM) 2.0 as a security-anchor for embedded systems, and proposed a proof-of-concept implementation of advanced remote firmware upgrade for embedded systems relying on the unique features of TPM 2.0.

A different approach is proposed by Lee, B. & Lee, J. [31], which leverages blockchain technology to securely check firmware versions, validate the correctness of firmware, and download the latest firmware for the embedded devices. Even though their work is focused on intensively interconnected embedded systems, such as in an IoT environment, the increasing number of internet-facing controllers let us suppose that may be worth investigating whether this technology could be applied to PLCs as well.

### 2.2.2 Intrusion detection

The PLC logic is usually executed in a scan cycle, in which the PLC reads the inputs from the sensors, executes the logic and writes the outputs to the actuators. Zonouz et al. [32] devised an approach capable of detecting whether a PLC logic could violate physical plant's safety requirements. Their technique is based on logic binary code analysis and model checking, and could be integrated in the PLC runtime itself, so that the check is made every time a new logic is uploaded to the system. Garcia et al. [33] leveraged the advanced computational power of embedded hypervisors, that could be coupled with modular embedded controllers, to provide both a memory verification solution and an intrusion detection system from within the PLC itself. The embedded hypervisor provides a library directly accessible from the PLC scan cycle either synchronously or asynchronously, and the hypervisor and the PLC can communicate through shared memory. Their approach may be extended to integrate any kind of security solutions inside the PLC. Cui et al. [34] proposed a host-based defense mechanism called Symbiotic Embedded Machines (SEM), designed for injecting intrusion detection functionalities into embedded system firmware code. The injected Symbiotes are basically code structures that will co-exist with the legacy firmware, sharing computational resources with it while protecting it against code modification. The SEM injection process is randomised, so that the firmware payload is divided into slices at random locations, called control-flow intercepts. Each code slice has its own Symbiote, which is basically a checksum of the corresponding section. When an intercept is reached by the firmware execution, the control goes to the Symbiote Manager which verifies the current portion of the code against the stored checksum. In this way SEM executes itself alongside the original OS while remaining stealthy and causing minimal overhead.

Moreover, Trusted Computing could also be used to enable malicious code detection capabilities at runtime. The main problem with this technology is to deploy it into embedded systems without impacting its limited resources and real-time constraints. Seshadri et al. [35] proposed a software-based attestation technique, named SWATT, to verify the memory contents of embedded devices and establish the absence of malicious code through a challenge-response protocol. SWATT is designed in a way that the minimum change to the code will result in a detectable delay. However, further research [36] has shown that this time-based approach is hard to design for embedded systems, and that some attacks are still possible.

Finally, another potential solution for intrusion detection in embedded controllers is based on power fingerprinting [37]. It consists of a physical sensor through which is possible to analyse and collect statistical data about power consumption and electromagnetic emissions, determining whether or not the process deviates from the expected operation model. Even though it is a powerful mechanism and does not interfere with critical operations, it provides limited support for forensic analysis once the attack has been detected, so this technique should be applied as a part of a security solution.

### 2.2.3 Control flow integrity

Control flow hijacking is one of the most used attacks to computer systems, because it usually leverages programming errors that are actually much more common than they should be. As more and more sophisticated control flow modification techniques were discovered, new defenses have been proposed, but only some of them are applicable to embedded systems. In 2012 Reeves et al. [38] proposed Autoscope Jr., an intrusion detection system designed for embedded systems, which is focused on detecting control flow alterations instead of malicious code insertions. Its approach consists of two phases: the learning phase and the detection phase. During the learning phase it collects control flow information from the function pointers used within the kernel, building a data structure, named Trusted Location List (TLL), which will be used in the second phase. The data structure basically maintains, for each monitored function pointer, a list of function addresses reachable from that pointer together with other control flow information (e.g. valid return addresses). During the detection phase it continues monitoring direct and indirect calls, and it generates an alert if an unknown function is reached from a monitored function pointer.

Habibi et al. [39] proposed a defensive technique for ARM architecture, named DisARM, effective against both code-injection and code-reuse attacks. Relying on the assumption that buffer overflow attacks lead the execution to a different return address than expected, they designed a mechanism for verifying the actual return address at runtime, thus protecting any potentially vulnerable program. First, they look for all the critical instructions contained into the program, defined as the ones that take input from the stack and affect the program counter directly or indirectly (e.g. through the link register). Second, they modify the binary code by putting a verification block before each critical instruction, so that the execution is stopped whenever a control flow manipulation is attempted through the stack.

Many other control flow integrity (CFI) solutions for embedded systems rely on hardware modifications in order to require smaller overheads. Francillon et al. [40] presented a technique to protect low-cost embedded systems against malicious manipulation of their control flow by using a simple hardware modification to divide the stack in a data and a control flow stack (or return stack). The access to the control flow stack is restricted only to return and call instructions, thus implementing an Instruction Based Memory Access Control (IBMAC) in hardware. Abad et al. [41] proposed a hardware-based security approach with predictable overhead for embedded real-time systems. They perform CFI checks on a real-time task by adding an On-chip Control Flow Monitoring Module (OCFMM) to the processor core with its own isolated memory unit. OCFMM monitors the run-time control flow and compares it to the stored Control Flow Graph determined in advance. Davi et al. [42] designed novel security hardware mechanisms to enable fine-grained CFI checks, based on three security policies. First, each function call enforces the processor to switch to a new state in which the only accepted instruction is a CFI instruction, thus restricting function calls to only target valid function entry points. Second, return instructions can only target a valid return of a function whose CFI instruction is active. The CFI instructions are identified by labels, managed through a CFI Label State Table embedded in the program data memory. Third, behavioural heuristics are used to cover typical patterns of ROP attacks. Afterwards, they provided an implementation for Intel Siskiyou Peak and SPARC, named HAFIX [43], demonstrating its security and efficiency in code-reuse protection while incurring only 2% performance overhead. Another hardware-based approach has been presented by Das et al. [44]: a fine-grained CFI at a basic block level, named basic block CFI (BB-CFI). A basic block is defined as a sequence of instructions, having a single entry and a single exit point. The policies used by BB-CFI are defined as follows: first, each function call can only target the first basic block of the function; second, each return can only target the basic block following the function call; third, indirect jumps must target a starting address of a basic block. Their approach is divided into two steps: 1) offline profiling of the program to collect control flow information data, and 2) runtime control flow checking. The control flow checker has been implemented on FPGA as a proof-of-concept, showing < 1% performance overhead, a small dynamic power consumption and a very small area footprint.

Finally, the attestation mechanism could be used to address control flow integrity as well. Abera et al. [45] presented the design and the implementation of Control-FLow ATtestation (C-FLAT), based on ARM TrustZone hardware security extensions. In their model, a verifier wants to attest runtime control flows of an application module on a remote embedded system, the prover. First, the verifier has to generate the Control Flow Graph from a clean binary of the application, storing the measurements of all the possible control-flow paths. Then, it sends a challenge to the prover, containing the name of the application and a nonce. The prover executes the application, computes a digital signature over the challenge and the executed path, and sends it back to the verifier for validation.

## 2.3 Hardware-level attacks and defenses

At the time of writing, we are not aware of any attack in literature which targets I/O of embedded systems. Neither any defense mechanism specific for embedded systems (or for PLCs) has been designed to protect I/O configuration. Although hardware level attacks are quite rare due to their complexity, they are very powerful and stealthy, because they are very close to the hardware. Here we provide an example of an existing hardware-level rootkit, and its corresponding defense. Even

though they are not applicable to embedded systems, they are still interesting for our purpose, due to their similarity with Pin Control Attack and Defense, respectively.

Embleton et al. [46] implemented a hardware-level rootkit which they call System management Mode Based Rootkit (SMBR). System Management Mode (SMM) is an isolated execution mode of the x86 architecture designed for low-level system control functions, such as power management. When the CPU is running in SMM mode, it uses a private memory space, it is completely non-preemptible, and it lacks any concept of privilege level and memory protection mechanisms. Thus, the code running in SMM mode is capable of directly accessing the underlying hardware. This could be very attractive for malicious users, as they demonstrated by implementing a chipset level keylogger and a network backdoor which interacts with the network card to send logged keystrokes to a remote machine via UDP stealthily. Their technique can be divided into two main steps. First, the rootkit needs to install its own SMM interrupt handler in place of the OS handler into a particular portion of memory called System Management RAM (SMRAM). Depending on the target system, this could require to modify and reflash the BIOS. Second, it reprograms the I/O APIC (Advanced Programmable Interrupt Controller) of the target peripherals in order to enable SMM mode on their interrupt signals. This is achieved without hooking the Interrupt Descriptor Table, making the rootkit undetectable. Once the target interrupt is routed, the rootkit SMM handler is called whenever the interrupt occurs (e.g. at each keyboard event). After its job is done, the rootkit may forward the interrupt back to the previously assigned handler, or may hide it, depending on its purpose.

To overcome this SMM rootkit, a defense framework called IOCheck has been proposed in [47]. The IOCheck framework leverages System Management Mode as well. It checks the integrity of the I/O configuration and the firmware of I/O devices at runtime. It also locks the System Management RAM (SMRAM), which is the portion of memory where the SMM handler is stored. Once locked, SMRAM cannot be overwritten until a reset occurs. Furthermore, the BIOS firmware is securely stored in SMRAM at boot time, such that its integrity can be verified at runtime. In order to protect the BIOS against offline modifications as well, a Trusted Platform Module is needed.

Both SMBR and IOCheck leverage SMM, which is an execution mode existing on x86 architectures. Since x86 architecture is rarely used in embedded devices, we can state that those techniques are not applicable to PLCs. Furthermore, even if x86 is used, switching to SMM mode would take about 4 milliseconds, as reported in [47]. This might be a low performance overhead for many computer systems, but it is certainly not acceptable for real-time embedded systems like PLCs.

# Chapter 3

## Pin Control Attack

Before describing Pin Control Attack, a deeper analysis of the architecture of the target system is needed. Note that, although this paper is focused on PLCs, the architecture described in the next section is still valid for almost any embedded system. After having a proper knowledge of the underlying architecture, we can go deep into the description of the design of Pin Control Attack. We consider the idea behind the attack, showing how it is able to evade the currently available detection mechanisms. Next, we go further and describe some implementations of the attack, extending its applicability to a real Programmable Logic Controller. Based on our architecture analysis and our tests, we can finally demonstrate that the attack is actually viable on real PLCs, even on a higher abstraction level.

### 3.1 Embedded architecture

As briefly reported into Chapter 1, PLCs use I/O interfaces to communicate with sensors and actuators, and in general with any external device. Digging into their architecture, we know that PLCs are usually based on a so called System on Chip (SoC). A SoC is basically an integrated circuit made of a microprocessor, a memory block and a set of peripheral controllers all enclosed together in the same chip substrate. Thus, the SoC technology provides fully capable computers having both very small size and low power-consumption. A SoC usually comes with a set of connections, also known as *pins*, usually soldered to a printed circuit board to facilitate interconnection with external modules. Many types of pins may be included in a SoC, having different purposes (power, clock, I/O, etc.). An example of such a system is the Raspberry Pi board shown in Fig. 3.1, based on a Broadcom System on Chip. Actually almost all of the embedded systems use a SoC with similar boards, each one with its own size and configuration.

In order to accommodate many board implementations from different companies, each pin (or group of pins) of a SoC may have multiple configuration and operating modes. The configuration of the pins is managed by the pin controller, a particular subsystem of a SoC. Through a specific set of registers belonging to the pin controller, the system can configure the operating mode of the pins, such as their input or output mode. These registers are typically accessible through a particular memory region called I/O memory. Such a kind of I/O access is known as *Memory Mapped I/O*.

The features provided by a pin controller can be grouped into two main categories:

- **pin configuration:** allows the system to change some electrical properties of the pins, such as direction, event detect, interrupt, etc.;
- **pin multiplexing:** each pin of the SoC may have many usages, also known as *alternate functions*, depending on what is needed by the external board. The pin multiplexing feature enables the system to specify which type of function is needed on each pin.



Figure 3.1: Raspberry Pi [48] with Broadcom System on Chip

As the I/O attack is a very low-level attack, it is necessary to dig further into the electrical world to know how these I/O interfaces work.

### 3.1.1 SoC pins

I/O interfaces of a System on Chip provide a connection between internal modules and external electronic devices. As shown in Fig. 3.2, they are physically visible from the outside of the chip package, usually in the form of pins (a) or soldering balls (b).

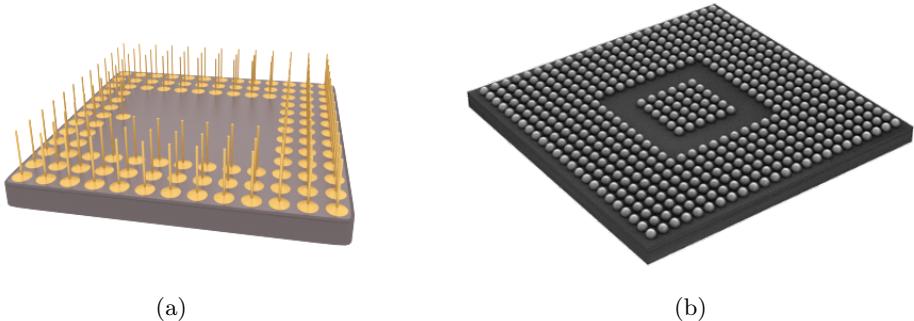


Figure 3.2: I/O connections packaged as (a) Pin Grid Array and (b) Ball Grid Array

Internally they are connected to the silicon die through bonding wires, and are managed by a specific I/O circuit which may vary according to the specific chip. Although there are many different implementations, almost all of the available SoCs have I/O ports with very similar functionalities. For our purpose, we can describe them in an implementation-independent manner by using simplified generic schematics.

#### Pin configuration

The schematic depicted in Fig. 3.3 helps us to discuss about the first set of features: pin configuration. The operation mode described in this section is also known as General Purpose I/O (GPIO).

Apart from the protection diodes that serve as shield against input currents lower than  $V_{SS}$  or higher than  $V_{DD}$ , the circuit is divided into two different parts: one for output and one for input.

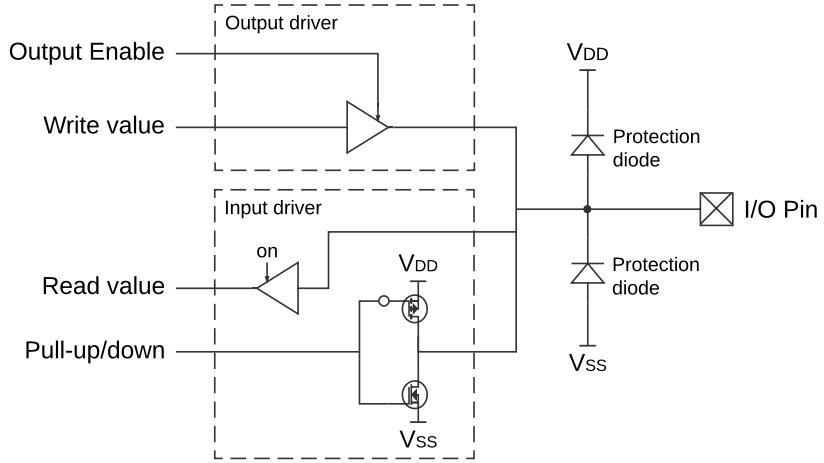


Figure 3.3: General Purpose I/O pin configuration circuit

- **Output driver:** The output module is basically a buffer controlled by an output enable signal. This signal controls the direction of the pin (input or output). If it is high, then the pin is in output mode and the value coming from a write operation goes through the buffer to the actual pin. If it is low, the pin is in input mode and the write signal is blocked, so it is not possible to change the external value of the pin from inside anymore.
- **Input driver:** The input driver has a similar buffer to read the value, usually having hysteresis capability which is useful for filtering unstable external values. Since the read buffer is always active, the input value is always available, even if the pin is currently working in output mode. The reason for this is merely physical: even if the external value was blocked by the buffer, one would always get a value by reading the input signal, because a value is nothing but an interpretation of the voltage level on a wire. When the pin is set as input, the pull-up/pull-down network enables the user to have a “default” value on the pin, namely a defined state maintained while the pin is not actively driven from outside. This feature is useful to avoid so called “floating” inputs.

For Pin Control Attack, what is more interesting about the circuit in Fig. 3.3 are the following two properties:

- there is no checking about the input state, so it is possible to perform a read even when the pin is in output mode;
- vice versa, it is not possible to write to a pin which has been configured as output.

Furthermore, it is also possible to drive the pull-up/down network, factually disturbing the real value of the I/O pin in an unpredictable way. Virtually, it is even possible to interfere with the pin value by means of external electromagnetic fields. In these cases the effects strongly depends on the actual implementation of the printed circuit board as well as on the external components connected to the I/O pin.

### Pin multiplexing

Inside a chip, each I/O pin may be connected to more than one device, which can be selected depending on the application (i.e. the way of soldering or wiring the package into an electronic board). This SoC feature is known as pin multiplexing (also ball multiplexing, pad multiplexing, alternate functions). Even though pin multiplexing is designed for hardware configuration, in almost all modern chips it is possible to change the function at run-time.

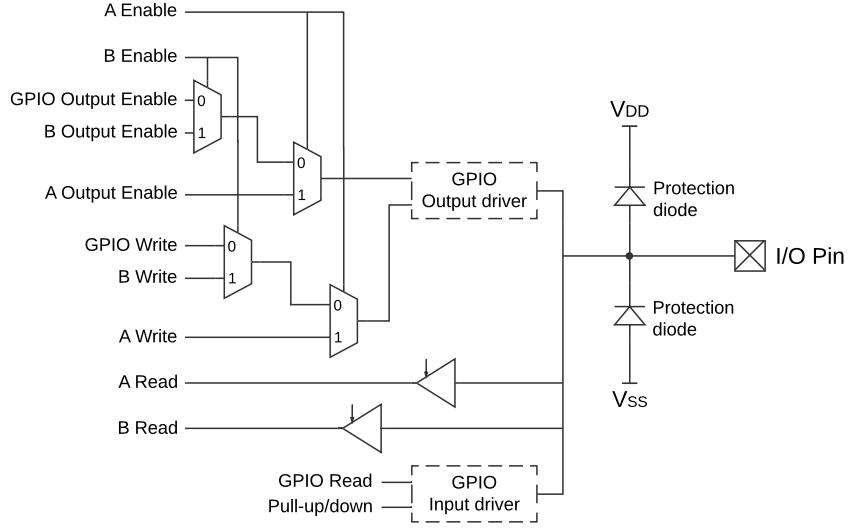


Figure 3.4: Generic I/O pin multiplexing circuit

Fig. 3.4 shows a possible hardware implementation of pin multiplexing. The I/O pin in the figure is connected to two different peripherals inside the chip, namely A and B, and it is also accessible through basic GPIO as described in Section 3.1.1 above. The access to the GPIO output driver is regulated by two in cascade multiplexers for each signal of the module. If the peripheral A is enabled, then the signals driven by A go through the multiplexers and can drive the actual value of the pin, while GPIO and peripheral B output signals are blocked. Instead, if only peripheral B is enabled then only its signals are able to reach the I/O pin. Note that in this last case the peripheral A should not be enabled, because A multiplexers have precedence against B ones. Thus, the cascading of multiplexers actually implements a priority mechanism between peripherals A and B. If neither A nor B are enabled, then no alternate function is active for the I/O pin and it could be driven by GPIO signals. Each peripheral may also have its own dedicated input line, to get values from the I/O port in the same way as GPIO does.

For our purpose, at least two interesting properties can be inferred from pin multiplexing schematic of Fig. 3.4:

- it is possible to block output signals from peripherals by simply changing the multiplexing configuration;
- the GPIO value can be read at any time, independently from the current multiplexing state of the output.

### 3.1.2 PLC architecture

As introduced in Chapter 1, Programmable Logic Controllers are a particular kind of embedded systems, designed to work into harsh environments and to control a physical process, typically an industrial or other critical processes. In this section we examine the hardware and the software architecture of a PLC. This analysis will be needed later to better explain the threat model and the implementation of Pin Control Attack.

#### Hardware architecture

Since it is built for working into a rough environment, the internal hardware of a PLC is shielded and not directly visible as the Raspberry Pi one. Fig. 3.5 shows an example of a basic PLC, provided by Wago. This model will be later used for our tests. Note that, although we provide

this specific example, the basic concepts described here are still valid for most of the PLC on the market, unless otherwise specified.



Figure 3.5: PFC200 Programmable Logic Controller from Wago

Internally, the PLC has a System on Chip whose architecture is substantially equivalent to the one discussed in the above sections. Therefore, the same concepts are applicable to PLCs as well. Anyway, from our analysis we found that their architecture could be a bit more complicated with respect to a plain SoC. Since the environment in which PLCs work may greatly differ case by case, they are designed to be as versatile as possible. Vendors know that their PLC could be deployed in many different physical processes, possibly having completely diverse sensors and actuators to interact with. Clearly, it is unreasonable to put every possible I/O interface on the same SoC. For this reason, most of the available PLCs comes with the possibility of connecting a certain number of external components called *I/O modules*. Each I/O module contains its own embedded SoC, responsible for a specific subset of I/O interfaces (e.g. digital input/output, analog input/output, pulse-width modulation, communication, etc.). This hardware architecture is summarised in Fig. 3.6.

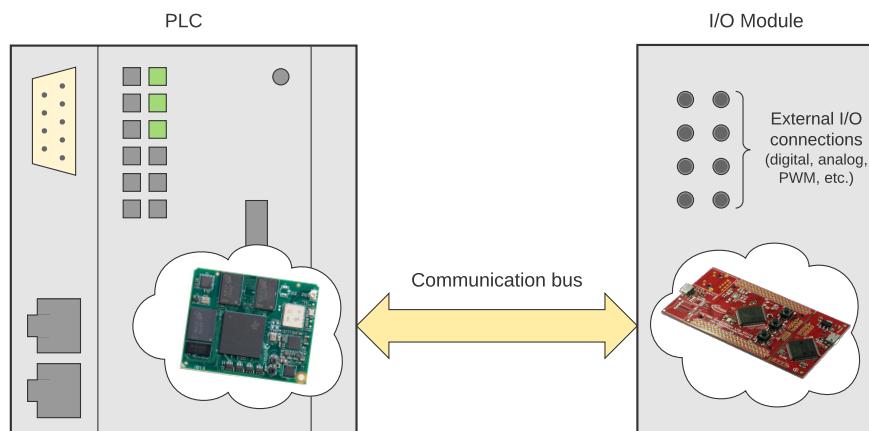


Figure 3.6: PLC hardware architecture

The main portion of the PLC communicates with the I/O modules via a system bus, which is, in turn, connected to the I/O interfaces of the PLC. This architecture with I/O modules adds one level of indirection between the targeted PLC and the external world, since there is another SoC in the middle. Anyway, the same concepts of Pin Control Attack can be applied to such an architecture as well. It is sufficient to consider that the I/O interface of the PLC, connected to the internal bus, is now the new direct target of our attack, while the final I/O becomes an indirect target. As we demonstrate in Section 3.3.2, by tampering with the I/O related to the communication bus it is possible to achieve equivalent results, proving that Pin Control Attack is still applicable on real PLCs.

### Software architecture

The PLC typically comes with a real-time operating system (e.g. Linux with RT-preempt patch, VxWorks etc.), because of the time requirements imposed by its main task. Above the operating system, a software called *PLC runtime* is responsible for managing the execution state of the control process and regulating the access to the PLC. Through the runtime, the industrial operator can connect its terminal to the PLC and upload the desired control program, the *logic*. The PLC logic is the application code responsible for the control of the physical process, dealing with input and output interfaces. As shown in Fig. 3.7, this architecture can be divided into three layers, laying one above the other.

- **Firmware:** the lowest layer, which basically corresponds to the operating system kernel. Although they are typically two distinct parts, here we consider the bootloader also as “part” of the firmware, because in this context their separation is irrelevant.
- **Runtime:** a software which is part of the application layer above the firmware, and it is started by the operating system itself.
- **Logic:** the control program running within the runtime environment. Its execution is started and stopped by the runtime, and its code is dynamic: it may change whenever the industrial operator decides to upload a new control program to the PLC.

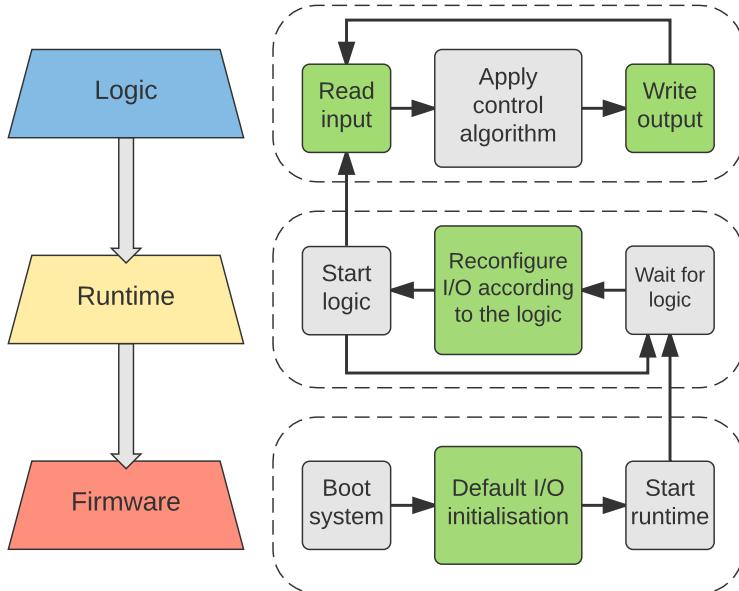


Figure 3.7: PLC software architecture

Fig. 3.7 also summarises the execution flow of each layer, from bottom to top, highlighting (in green) the tasks directly related with the I/O.

When the firmware is loaded into memory and the system is booting, one of the early operation performed is known as I/O initialisation sequence. In this phase, the drivers within the kernel configure their own I/O registers with their default values. I/O initialisation includes both pin configuration and pin multiplexing. Normally, pin multiplexing is only performed at boot time, and, even though it is not forbidden, pin multiplexing is never modified at run-time. Conversely, pin configuration may be changed later at run-time. Thus, depending on the implementation, the configuration written during I/O initialisation may correspond or not to the one desired by the final application.

After the I/O has been initialised, the firmware loads the main application needed by the controller: the runtime. The PLC runtime waits for a logic to be uploaded into the PLC from a terminal connected via the network interface. The execution flow reported in Fig. 3.7 for the runtime layer is a general process, including the case when a PLC is started for the first time. If a PLC is already in production, it is rarely restarted. However, when a reboot is needed (e.g. for firmware update), it may be configured to persistently save the current logic into a non-volatile memory and restore it after reboot. In this case the “Wait for logic” step in Fig. 3.7 can be simply skipped, because a logic may be already available from disk.

When a logic is available, from network or from disk, the PLC runtime analyses its content. The I/O configuration expected by a specific logic is bundled with the logic itself, because it is decided by the operator who has knowledge of the physical process and knows how sensors and actuators are connected to the PLC I/O ports. With respect to the hardware architecture shown in Fig. 3.6, a change in the input/output required by the operator is actually reflected into a configuration change of the external I/O modules. Whether this process involves a change in the I/O configuration of the PLC itself depends on the implementation and on the modification extend (e.g. if a new I/O module has been attached, this will probably require a change in the communication protocol and so on the I/O interface of the PLC). After the new I/O configuration has been applied, the logic can be executed. From an operating system point of view, the logic is running in the same context of the PLC runtime.

As briefly discussed in Chapter 1, the PLC logic executes the main *scan cycle*. For each iteration, it reads from inputs, executes the control algorithm, and writes to outputs. The control algorithm has been programmed by the industrial operator, and loaded through the interface provided by the PLC runtime. When the logic is running, input and output pins have already been configured by the runtime, and the logic assumes that the I/O configuration does not change during its execution. Both the logic and the runtime interacts with the I/O, but in different ways. The runtime deals with I/O configuration registers, while the logic performs read/write operations related to I/O values. Both kind of interactions, anyway, require the same privileges, which will be later leveraged by Pin Control Attack.

## 3.2 Attack Design

Given the properties discussed in Section 3.1, it is possible to misuse the registers used to configure I/O peripherals, and that is what Pin Control Attack does. This can happen at run-time, during the execution of the controller on a real process, without any reaction from the PLC runtime or the operating system, thus remaining completely stealth.

We can argue that Pin Control Attack is actually applicable on any System on Chip having the architecture described in Section 3.1. However, PLCs represent a particularly interesting target among all the embedded systems based on SoC. PLCs leverage the interfaces of a SoC to interact with sensors and actuators, having direct effects on our physical world. Therefore, if the I/O of a PLC is compromised, this constitutes a much more significant security and safety risk with respect to other non-critical embedded system. For this reason, PLCs represent one of the most attractive targets for Pin Control Attack.

In this section we focus on the design of I/O attack. First, we summarise the host-based detection mechanisms taken into account during the attack design and the techniques used to evade them. Second, we analyse the attack itself in more detail. The goal of this chapter is to help

us having a better understanding of the attack, and to provide a detailed threat model on which our defense design will be based on.

Pin Control Attack has been designed to be different from previous attack techniques, and to circumvent the off-the-shelf host-based detection systems. The authors of I/O attack have identified two main defensive mechanisms whose properties makes them more easily applicable to PLCs. Here we want to generalise and consider them in our threat model, clarifying how and when Pin Control Attack becomes applicable and interesting for attackers. We also show how these defenses are circumvented by Pin Control Attack, and describe the available attack techniques. We do not repeat here the detailed description made in [1]. We only want to have basic concepts definition, in order to be able to focus on our further analysis and implementation of the attack.

### 3.2.1 Defense analysis

At this point, one could ask why descending to the lowest level possible to conduct an attack, when a lot of easier techniques (e.g. function hooking) may achieve equivalent results. The point here is that many producers of embedded systems and PLCs already started to move towards a more security-aware production. As considered in [1], in order to be applicable to PLCs, a defensive mechanism should have at least the following properties:

- low CPU overhead: CPU resources are limited in embedded systems such as PLCs, which typically have hard real-time constraints;
- designed to run on an operating system: almost all of the modern PLCs have a real-time OS running on it;
- no hardware modification required: many solutions are hardware-based [29,40–42,44], making them not easily applicable;
- no virtualisation required: the majority of embedded systems, like PLCs, does not support virtualisation; thus solutions like [33] are less attractive.

Given these considerations, we can list some of the applicable defenses:

- **SEM:** the Symbiote detection system described in [34], which protects the kernel from code modification attacks;
- **Autoscopy Jr.:** the lightweight intrusion detection system proposed in [38], effective against control flow manipulation inside the kernel.

The above detection systems still have some shortcomings, leveraged by Pin Control Attack. First, they are based on a comparison with golden references (the symbiotes and the TLL, respectively) taken from a subset of the entire kernel space. If the attacker is able to find a portion of the kernel space which has not been considered by the detection system, then it can be circumvented. For example, Autoscopy Jr. can be bypassed if the attacker is able to craft a duplicate of the kernel functions it needs. If a duplicate function is used instead of the original version, Autoscopy Jr. does not throw an alert, because this function is not listed in the TLL at all. Second, the references used by both defenses are *static*, which means that they are based on previous analysis of the immutable (static) portion of the system. Thus, an attacker could still use dynamic memory, whose content changes during run-time, to conduct its own attack. In the case of SEM, only static code regions (which are immutable) are taken into account, so any malware placed in dynamic memory will not be detected. Autoscopy Jr., instead, considers the function pointers used inside the kernel, including the ones inside the System Call Table and other similar tables. Therefore, it is able to detect only *data hooks* but not *code hooks*; in other words, any direct code modification (e.g. of the kernel text) is still possible.

Anyway, these two defenses may be used in combination, thus providing a host-based IDS able to detect both code and data hooks. Even if they are deployed together, however, attacks

through dynamic memory and without function hooking are still possible, since monitoring dynamic memory is a far more complex issue. One of the implementations of Pin Control Attack (see Section 3.3) leverages exactly the kernel dynamic memory to reach its purpose.

Host-based detection mechanisms like the ones discussed above will likely be deployed into many commercial products within the next years [49, 50], raising the bar for attackers. Therefore, Pin Control Attack will become more and more interesting as long as classical techniques (e.g. function hooking) are overcome.

### 3.2.2 Threat model

In our work, we assume that the system is protected at least by the HIDSs described in Section 3.2.1, or equivalent. Hence, we assume that the attacker cannot tamper with operating system (kernel) functions and data structures, but it can still use dynamic memory to insert its malicious code and tamper with the I/O configuration. The attacker can also write its own version of kernel functions if needed, and call them separately in order to avoid HIDSs. This approach, anyway, requires very high effort and would really be the last option for an attacker.

The attacker, depending on the attack implementation, may need different running privileges on the target system to execute Pin Control Attack. Generally speaking, the minimum privilege required is the privilege level of the PLC runtime, which has access to the I/O configuration registers. As already discussed in [1], many ICS-CERT advisories have shown that PLCs have vulnerabilities that could lead to malicious code execution [13–18], and they may affect PLC runtime software as well. Thus, obtaining the same PLC runtime privilege level is feasible on real systems.

As in [1], we assume that the attacker knows both the physical process controlled by the target system and the mapping between I/O configuration and external sensors and actuators. The former is typically known by the attacker, which has reasonably studied its target before conducting the attack. This is confirmed by Stuxnet [4], where attackers had very deep knowledge of target system and physical process. The latter is given by a knowledge of the PLC logic, which, as said, already comes with the mapping between I/O interfaces and control variables used by the logic. Furthermore, the research presented in [10, 11] shows that it is possible to infer the structure of the devices connected to the PLC and used by the logic, factually lowering the bar for attackers which do not need an a priori knowledge of the I/O mapping anymore.

### 3.2.3 Pin Control Attack

Based on the previous assumptions, Abbasi et al. [1] crafted Pin Control Attack, which is capable of manipulating the physical process controlled by a PLC without requiring any firmware or logic modification. The idea of Pin Control Attack is that the attacker operates at the lowest level possible, targeting the interaction between the firmware and the I/O, as shown in Fig. 3.8. For this reason, the attack is also known as I/O attack. Despite its crucial function in embedded systems, I/O hardware architecture and I/O drivers are currently designed without taking into account any concept of security, assuming that I/O is reliable. Unfortunately, given the properties inferred in Section 3.1 from a generic hardware architecture, this is often not the case.

As described in [1], Pin Control Attack is designed to evade off-the-shelf HIDSs presented in Section 3.2.1. In particular, it leverages kernel dynamic memory (in one implementation variant) or it uses a simple user code (in a second variant). Both variants are able to circumvent the above detection mechanisms.

The authors of [1] have found at least two different attack vectors for Pin Control Attack: *Pin Configuration* and *Pin Multiplexing*. Both kind of attacks leverage the SoC properties described in Section 3.1. The attack is performed by misusing the control registers used to program the I/O peripherals, writing malicious values into them. If the attack targets I/O configuration registers, it is a Pin Configuration Attack, otherwise, if the targeted registers are related to the multiplexing state of the pins, then it is a Pin Multiplexing attack. In some architectures, I/O configuration and

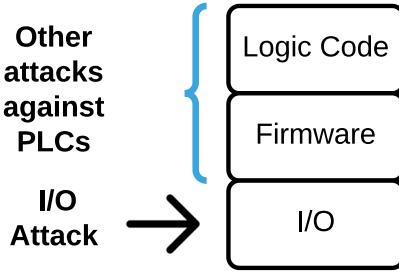


Figure 3.8: Pin Control Attack target, from [1]

multiplexing is achieved by using the same set of registers (e.g. different bits of the same register may have different purposes).

In both cases, the main principle behind the attack is something that they called *memory illusion*, which is represented in Fig. 3.9. In a system equipped with a Memory Management Unit (MMU), that is the most common scenario for PLCs, each process cannot directly access to physical address space. Every memory access is mediated by the MMU, which creates an abstraction called *virtual address space*, or *virtual memory*. When a process wants to access physical memory, it has to request a mapping to the system between physical address space and virtual address space. In this way, every process has its own “virtual view” of the physical memory. This is valid also for I/O memory, which is part of the physical memory. Once a mapping has been established, the I/O can be managed by accessing the mapped virtual memory. Thus, as Fig. 3.9 outlines, an attacker

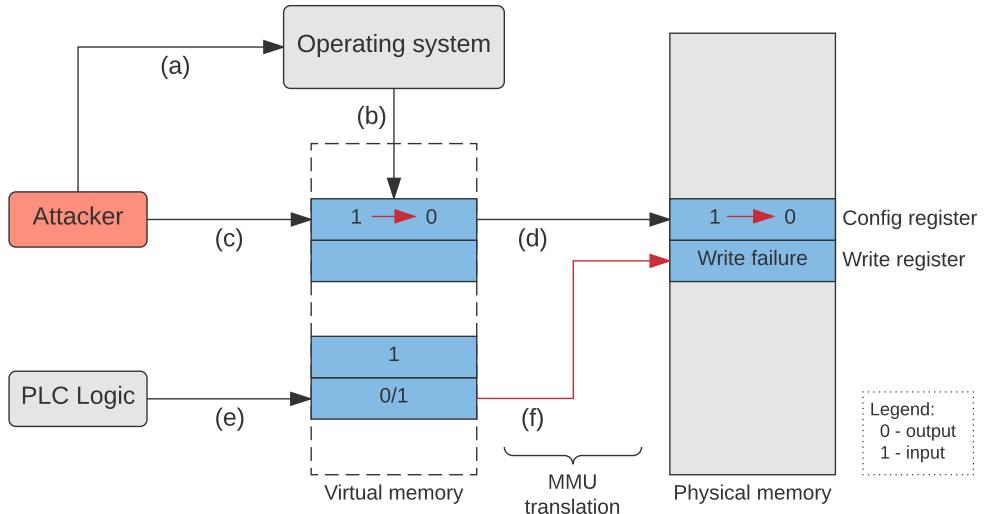


Figure 3.9: Pin Control Attack memory illusion

can do the following: first, it has to request a mapping for I/O memory (a); once a virtual mapping is provided by the operating system (b), the malicious process is able to alter the pin configuration (e.g. change an output pin to input) through virtual memory (c). This change is immediately reflected into physical memory via MMU translation (d). When the PLC logic, which is a normal process in the system, tries to update the value of the pin through virtual memory (e), the target address of the write instruction arrives to the MMU, which translates it to the corresponding physical address. Unfortunately, since the pin has been changed to input, the execution of the instruction does not actually affect physical memory (f). Therefore, the write silently fails, but no signal error is reported back to the CPU, and from the process virtual perspective everything went correctly. As explained later in Chapter 4, the fact that the virtual address of the instruction

actually reaches the MMU will be a crucial mechanism for the design of our defense.

As reported in [1], only by leveraging the configuration of pins they crafted an attack which is able to do the following:

- reconfigure an I/O pin as input when the PLC logic is attempting to write;
- reconfigure an I/O pin as output and write a malicious value when the PLC logic is attempting to read.

In this way, the attacker can disable specific output operations and feed the PLC logic with malicious input at the same time. In other words, Pin Control Attack takes the whole PLC logic as a black box. Instead of altering the logic code, it simply controls input and output values by means of the above operations. Whether this approach can lead to useful results (for the attacker) is highly dependent on the actual PLC logic and, of course, on the attacker purpose. In Section 3.3.1 we show that this mechanism may be very interesting for the attacker, and we also discuss about some hardware limitations of this approach.

Moreover, we imagine that many other attack possibilities may exist. An attacker can tamper with the I/O configuration in many other ways depending on the specific I/O peripheral and on its features (e.g. event detect, interrupts, clock signals, etc.), and the effects of the attack are unpredictable. If the attacker can analyse the reference manual of the target SoC (mostly publicly available) and it has enough competence and time, the only limit to Pin Control Attack becomes fantasy. To give an idea of what such an attack can do, imagine a simple SoC pin which can be multiplexed between a memory controller and a PWM controller. If this pin is actually connected to an external memory, thus multiplexed to a memory controller, a Pin Multiplexing attack can lead to dangerous signals sent from a PWM controller to a memory module, which may burn the memory. Furthermore, if a subset of pins is multiplexed to a specific controller (e.g. I2C, SPI, DMA, etc.), the control registers of the device can be targeted as well, obtaining an indirect effect on the corresponding I/O pins.

On the other side, from our analysis on a real PLC, we found that another attack vector is viable at a different abstraction level than hardware configuration. Commonly, the I/O peripherals are controlled by operating system drivers, which in turn are used from user space applications like the PLC runtime. As we show in Section 3.3.2, an attacker can target these drivers, or even these applications, to obtain equivalent effects without dealing with the underlying hardware and I/O registers directly.

### 3.3 Attack Implementation

In this section we first describe the available implementation presented in [1], which was the starting point of our analysis. Next, we introduce a possible attack implementation on a real PLC. Both implementations are designed for Linux-based systems, and they have two different variants: kernel side and user side. Each variant imposes different requirements for the attacker, which will be discussed in more detail in the next sections.

#### 3.3.1 Raspberry Pi

The system used for our experiments with the first implementation is a *Raspberry Pi 1 Model B* based on an ARMv6 architecture, running the following kernel:

```
Linux raspberrypi 4.4.22+ #912 Mon Sep 26 19:00:13 BST 2016 armv6l GNU/Linux
```

The Raspberry Pi 1 features a Broadcom System on Chip named *BCM2835*. With reference to the *BCM2835* documentation [51], we set up the system I/O by connecting a button as input, an LED and a servo motor as outputs. Button and LED are accessed via 2 GPIO interfaces, one configured

as input and one as output, respectively. To connect the micro servo, we needed an external PWM controller. The controller is attached to the system through the I<sub>2</sub>C interface, which requires two pins: one for the data line, *Signal DAta* line (SDA), and one for the clock line, *Signal CLock* line (SCL). The resulting system on which we conducted our experiments is shown in Fig. 3.10, and its I/O configuration is summarised in Tab. 3.1.

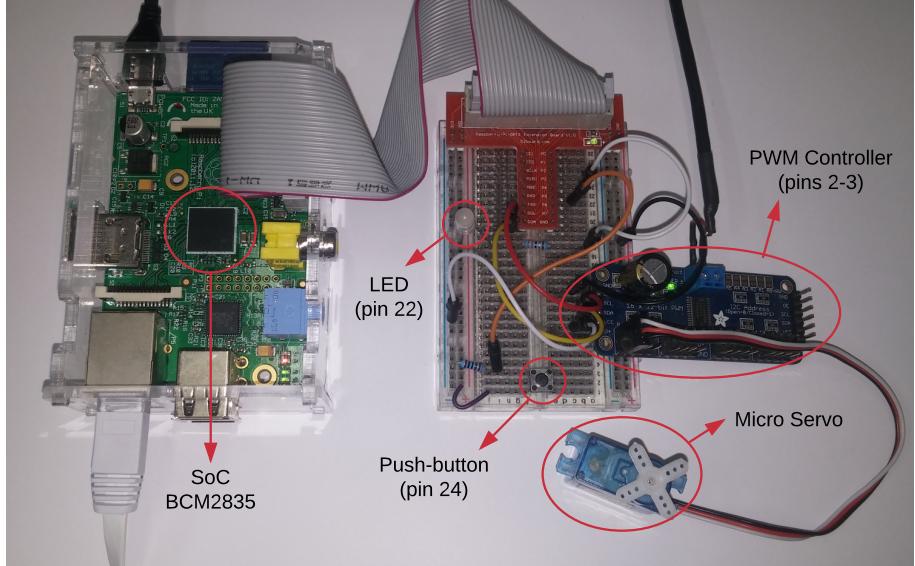


Figure 3.10: Raspberry Pi system used for experiments

Pin	Multiplexing	Configuration	Connected to
24	GPIO	Input	Button
22	GPIO	Output	LED
2	I <sub>2</sub> C SDA	-	PWM controller (servo)
3	I <sub>2</sub> C SCL	-	PWM controller (servo)

Table 3.1: I/O configuration of our Raspberry Pi testing system

To enable PLC capabilities on such a system, we installed a PLC runtime on it. In particular, we used *CODESYS Control for Raspberry Pi SL* provided by 3S-Smart Software Solutions GmbH [52]. Through the CODESYS Development System [53], we designed the PLC logic shown in Fig. 3.11, whose code is executed for each scan cycle. We chose a 10 ms scan cycle interval, however, since this PLC runtime is not real-time, the timing may be affected by small errors ( $\approx 50 \mu\text{s}$ ). At each scan cycle, the logic reads from pin 24 (push-button), and writes the outputs accordingly. The motor is driven with a sinus wave which makes it going forward and backward in the interval  $[-45^\circ, 45^\circ]$ . If the button is not pressed, which corresponds to value 1 (high), the LED is toggled every 2 s and the motor completes a round in 2 s. If the button is pressed, that is value 0 (low), both LED and motor frequencies are multiplied by 4, and the new round time becomes 500 ms. The timing of the write operations, which is a multiple of the scan cycles, is controlled by software counters embedded into the logic. Thus, while the input is high the counters are updated at normal speed; while the input is low they get updated 4 times faster. Furthermore, the logic does not write to the outputs at each scan cycle, but only when their values change (e.g. the LED pin is written only every 2 s). This is typically different from the normal behaviour of a real-time PLC, as discussed in Section 3.3.2.

Given the system above, a possible implementation of Pin Control Attack can target input or output pins, having different effects. By re-configuring an output pin as input, it is possible to disable the PLC logic write operations, leading to a Denial of Service (DoS) condition. More

```

PROGRAM PLC_Logic
VAR CONSTANT
    PI: LREAL := 3.141592653589793;
END_VAR

VAR
    button: BOOL;
    led: BOOL;
    counter: INT := 0;
    t: LREAL := 0;
END_VAR

button := dIn.24;
IF (button) THEN
    counter := counter + 1;
    t := t + PI * 2 / 200.0;
ELSE
    counter := counter + 4;
    t := t + PI * 2 / 50.0;
ENDIF

Adafruit_PWM.alrPWM[0] := 0.45 + 0.5 * SIN(t);

IF (counter >= 200) THEN
    led := NOT led;
    dOut.22 := led;
    counter := 0;
    t := 0.0;
ENDIF

```

Figure 3.11: PLC logic loaded into Raspberry Pi

interesting, by changing an input pin into output and writing its own values, an attacker can actually control the behaviour of the outputs. In our case, if the attacker is able to intercept PLC logic read operations and write its own values, he can actually decide the frequency of the outputs. For instance, as demonstrated by our attack experiments, if the attacker feeds the logic with 0 and 1 alternatively at each scan cycle, the round time of the outputs becomes the average between 2 s and 500 ms, factually having a frequency that is not even programmed into the logic. But there is a limitation to this attack approach, implied by the architecture described in Section 3.1.1 and confirmed by the experiments: the read operation is not reliable if the pin is configured as output pin. In our case, if we reconfigure pin 24 as output, the malicious value written into the write register is not always the same value read by the PLC logic. That is probably because the voltage on the pin is actually driven by two entities at the same time, the external sensor (the button) and attack code, so it is not deterministic whether, at the time of reading the pin level register, the voltage is considered a 1 or a 0.

The authors of Pin Control Attack described two different ways of intercepting read (or write) operations, and they implemented them into the following attack variants:

1. a Linux loadable kernel module which is able to intercept logic read and write operations by leveraging the *Debug subsystem*;
2. a user code which maps the physical I/O memory, or re-use PLC logic mapping, and manually watches the I/O values to synchronise itself with the PLC logic operations.

Once the target operation has been caught, the attack modifies the I/O configuration according to its purpose. Both implementations are able to evade the HIDSs analysed in Section 3.2.1, because they reside into kernel and user dynamic memory, respectively, and they do not alter any control flow. Here follows a brief description of these two possible implementations, focused on the findings of our experiments. For a more detailed analysis of the original version of the attacks refer to [1].

## Kernel module

This variant requires root privileges, in order to be able to insert a loadable module into the kernel. The kernel module makes use of debug registers, available in many embedded architectures, to catch PLC logic operations. A debug register takes a virtual address, and optionally a process context, and raises a CPU exception when the address is accessed within the given context. The access type may be read, write or execute: the first two are intended for data addresses, the last one

for instruction addresses. Thus, to use a debug register, the attacker needs to know the mapped virtual address used by the PLC logic to read/write the I/O pins. These addresses are typically mapped by the PLC runtime before starting the logic, and can be easily obtained by looking into the `/proc/<pid>/maps` file, which lists the current mappings owned by a process identified by `pid` (process id). As discussed in Section 3.2.2 the attacker needs to know the running PLC logic, and the mapping between the I/O pins and the physical process he wants to tamper. With reference to our target system, if the attacker knows that the input button is connected to pin 24 and wants to intercept a read operation, then he can get the physical address of the read register from the SoC documentation [51] (0x20200034), and finally the virtual address from the current PLC runtime mappings (e.g. 0xb6f40034). With this information, he can install a debug exception handler by setting a debug register: the malicious handler will be called whenever the PLC logic tries to read from that address. Inside the handler, the attacker can decide whether to change the pin configuration and which value wants to feed the PLC logic with. The use of debug registers gives the attacker a great timing accuracy on read and write operations, but the overhead may be detectable by power consumption-based intrusion detection systems.

### User code

This version does not need root privileges as the previous one. Since it is executed from user space, to have access to the I/O physical memory it needs to either request a new mapping to the kernel or use the existing mapping of the PLC runtime. In both cases, the requirement is to have the same privilege level of the PLC runtime, and this may be obtained by exploiting a code execution vulnerability affecting the CODESYS PLC runtime [14, 15]. The requirement needed to obtain the PLC runtime mapping is the same as the kernel module variant. To intercept read and write operations, the attacker cannot use debug registers, because the access to the debug subsystem is mediated by the kernel `ptrace` API. Therefore, this version can only monitor the value of an output pin to get the relative time, and also infer timing information of other pins by using its knowledge of the PLC logic. In our case, if the attacker monitors the pin 22, when its value changes he knows from the logic that at the same time the button input has been read, and the servo motor has just finished a round. This information can be used to set relative timers, which will be activated on the next I/O events. If the target system has real-time capabilities, as almost all real PLCs do, this technique can be even more accurate than our experiments in a non real-time environment. Moreover, its overhead is much less than the corresponding debug register one, and it may not be easily detectable.

### 3.3.2 PLC

As done for Raspberry Pi, we analysed a real PLC and considered the attack possibilities on this system as well. The provided PLC is a *PFC200 750-8202* model from *Wago* vendor. It runs a Linux kernel with the RT-preempt patch, which gives it hard real-time capabilities. In particular, the system runs the following kernel version on an ARMv7 architecture:

```
Linux PFC200-4106BA 3.18.13-pfcxxx-02.00.02_00+14-rt10 #1 PREEMPT RT armv7l GNU/Linux
```

Furthermore, Wago gives complete (root/kernel) access to its system, and the user can even program its own PLC runtime [54]. As discussed in Section 3.1.2, different kind of I/O modules can be attached to the PLC. For our analysis, we attached a Digital I/O module to the communication bus. PLC and I/O module are based on an *AM3517* SoC from *Texas Instruments* and an *XE164* SoC from *Infineon*, respectively. The digital I/O module has 16 different pins, 8 for input and 8 for output, and we connected a button as input and an LED as output, obtaining the system shown in Fig. 3.12.

The PLC runtime environment is the *e!RUNTIME* provided by Wago, which is always based on CODESYS. From the Wago *e!COCKPIT* engineering software, we programmed a simple logic which toggles the value of the LED every 500 ms only when the button is not pressed (high input). If the button is pressed, the LED is turned off until the button is released. The logic, in *Structured*

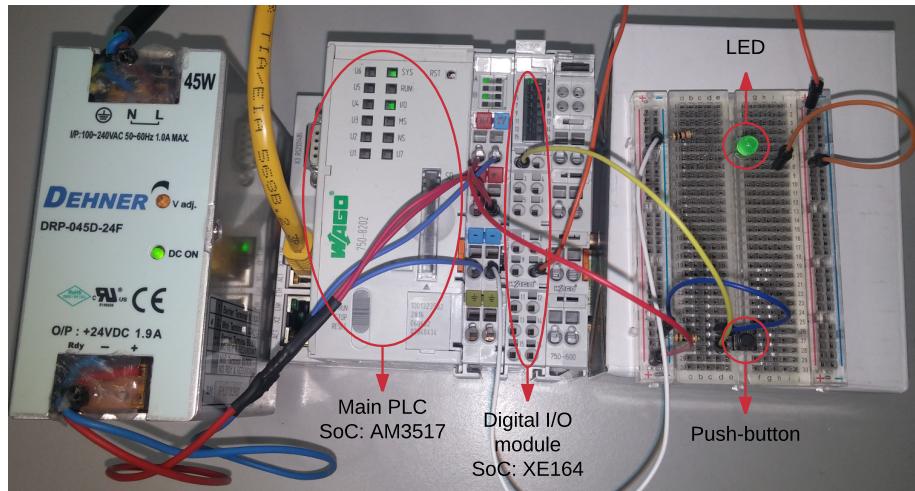


Figure 3.12: Wago PLC system used for experiments

*Text (ST)* language, is shown in Fig. 3.13. It assumes a scan cycle of 10 ms, and uses a software counter to achieve the timing of 500 ms. The picture also shows the mapping between the variables and the I/O pins of the external module. Differently from the Raspberry Pi system behaviour, here the outputs are updated on every scan cycle, even if the value has not been changed during the last 10 ms. Given this system, we started the analysis of the PLC runtime to better understand the overall architecture, already reported in Section 3.1.2, and the Wago implementation.

	Variable	Mapping	Channel	Address	Type	Default Value	Unit	Description
1	PROGRAM PLC_PRG			_IN	%IB1	BYTE		Input Channels
2	VAR			_IN	%IX1.0	BOOL	FALSE	Digital input
3	counter: INT := 0;			_IN	%IX1.1	BOOL	FALSE	Digital input
4	led: BOOL := FALSE;			_IN	%IX1.2	BOOL	FALSE	Digital input
5	button: BOOL := TRUE;			_IN	%IX1.3	BOOL	FALSE	Digital input
6	END_VAR			_IN	%IX1.4	BOOL	FALSE	Digital input
7				_IN	%IX1.5	BOOL	FALSE	Digital input
8				_IN	%IX1.6	BOOL	FALSE	Digital input
9				_IN	%IX1.7	BOOL	FALSE	Digital input
10	IF (button) THEN			_OUT	%Q0	BYTE		Output Channels
11	counter := counter + 1;			_OUT	%QX0.0	BOOL	FALSE	Digital output
12	IF (counter = 50) THEN			_OUT	%QX0.1	BOOL	FALSE	Digital output
13	counter := 0;			_OUT	%QX0.2	BOOL	FALSE	Digital output
14	led := NOT led;			_OUT	%QX0.3	BOOL	FALSE	Digital output
15	END_IF			_OUT	%QX0.4	BOOL	FALSE	Digital output
16	ELSE			_OUT	%QX0.5	BOOL	FALSE	Digital output
17	led := FALSE;			_OUT	%QX0.6	BOOL	FALSE	Digital output
18	END_IF			_OUT	%QX0.7	BOOL	FALSE	Digital output

Figure 3.13: PLC logic loaded into Wago PLC

## PLC e!RUNTIME analysis

For our research we used the following materials and tools:

- **Board Support Package** (BSP) provided to us by Wago [54], which allows to build and configure a complete disk image of the system running inside the PLC. It essentially consists of: the kernel source code with all the patches applied by Wago, the libraries and the applications used into the system. For most of the Wago libraries, only the binary code is provided.
  - **AM35x manual**: the Technical Reference Manual of AM35x processor, from [55].
  - **strace** tool [56], useful to analyse the behaviour of the PLC runtime, in particular the system calls used for accessing the I/O.

- **kprobes** kernel feature [57], used to intercept function calls related to the I/O from kernel space.

We report the findings of our analysis as follows. With reference to the architecture described in Section 3.1.2, we discovered that the Wago implementation uses a communication bus between PLC and I/O named *KBUS*. It is implemented as a kernel driver, whose code is available as kernel patches included into the BSP. The KBUS is basically a serial BUS built upon the Serial Peripheral Interface (SPI) protocol, used together with Direct Memory Access (DMA) to perform faster transfers. From strace, we found that the PLC runtime uses the driver through `ioctl` calls to send and receive inputs and outputs at each scan cycle, as reported below.

```
[...]
04:10:01.545185 clock_gettime(CLOCK_MONOTONIC, {122, 590121662}) = 0
04:10:01.545831 clock_gettime(CLOCK_REALTIME, {1335924601, 545923773}) = 0
04:10:01.546293 ioctl(11, _IOC(_IOC_WRITE, 0x4b, 0x01, 0x18), 0xb54a47d0) = 4
04:10:01.549585 clock_gettime(CLOCK_REALTIME, {1335924601, 549739477}) = 0
04:10:01.550047 clock_gettime(CLOCK_MONOTONIC, {122, 595045151}) = 0
04:10:01.550508 nanosleep({0, 3785000}, NULL) = 0
[...]
```

The code shows one PLC scan cycle, which is basically made of an `ioctl` call, plus the corresponding calls needed to achieve the timing of 10 ms (`clock_gettime` and `nanosleep` functions). Each `ioctl` call from user space is directed to the internal `kbus_ioctl` function of the KBUS driver. The operations performed at each scan cycle are outlined in the scheme of Fig. 3.14, which shows

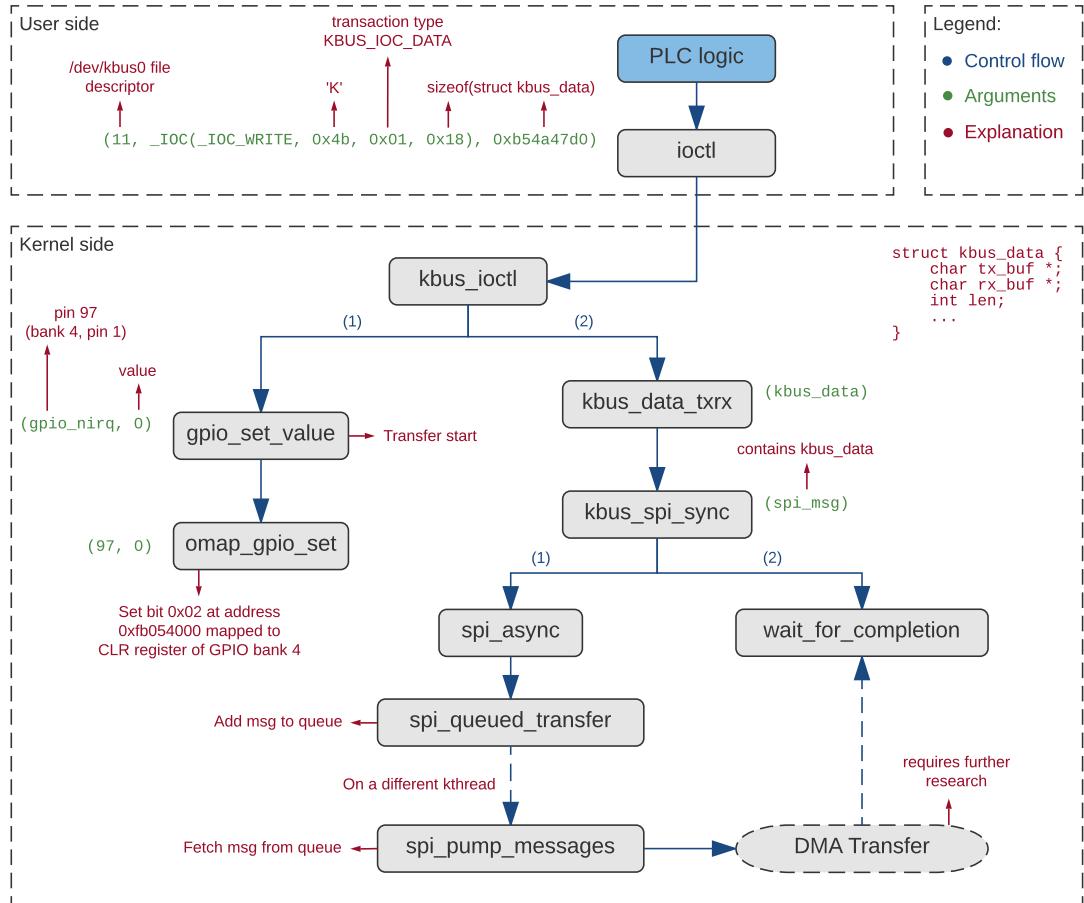


Figure 3.14: PLC I/O operations executed for each scan cycle

the results of our reverse engineering analysis on Wago PLC e!RUNTIME. From a quick look at the chart, we immediately deduce that the complexity is much bigger with respect to the CODESYS runtime for Raspberry Pi. The important difference between CODESYS and e!RUNTIME is that the former performs I/O by directly mapping physical addresses and reading from (or writing to) I/O pins, while the latter has to transfer data to the external I/O module. Thus, e!RUNTIME uses its I/O pins to communicate with I/O modules, by means of the KBUS driver interface. KBUS is an abstraction layer built upon different lower-level drivers: basically GPIO, SPI and DMA. The main operation of the kbus driver is managed through the `kbus_ioctl` call. The first argument (11) is the file descriptor number related to the `/dev/kbus0` file, which allows the kernel to forward the request to the KBUS driver. The second argument contains different information used by the driver to select the specific sub-function. In our case, the request is for a data transfer, and the third argument (0xb54a47d0) is a pointer to a `struct kbus_data`. The data structure contains, among other members: a pointer to a transmit buffer (`tx_buf`), a pointer to a receive buffer (`rx_buf`) and a buffer length. Since `tx_buf` and `rx_buf` are actually pointing to the same buffer used for both directions, only one length is required. In our configuration, with the digital I/O module alone, the buffer contains at least 2 bytes: one for input pins and one for output pins (8 bits each). Thus, every `ioctl` call serves both as read and write operation. On each call, the input part of the buffer is filled in by the KBUS driver, while the output related to the previous scan cycle is written to the bus. From the new input obtained, the logic computes new output values, waits for the necessary time, and calls `ioctl` again with the updated buffer. We report below the output of one of our kprobes to show the actual content of the buffer during a call to `ioctl`:

```
ioctl: len = 2, bytes = [0x40, 0x00]
```

The first byte indicates that the PLC logic is sending a 1 to the second output pin (0x40), to turn the LED on. The second byte represents the input value related to the previous scan cycle, which will be overwritten by the KBUS driver during the current call. In the above case, 0x00 means that all the digital input lines were low.

Each I/O operation begins with a call to `gpio_set_value`, which writes on a GPIO pin, indicating to the I/O module that a transfer is starting. The pin used for this purpose is the GPIO pin 97, i.e. pin 1 of GPIO bank 4 (each bank controls 32 pins). The value written into the pin is 0, since the signal is active low. Afterwards, the data buffer is encapsulated into an SPI message, starting an SPI transfer. The SPI interface leverages four pins of the AM3517 SoC, two for data input and output (MOSI: Master Output Slave Input, and MISO: Master Input Slave Output), one for synchronisation (SCL: Serial CLock) and one for chip select (SS: Slave Select). The PLC SoC is the SPI master, and, according to our actual configuration, the digital I/O module is the only SPI slave available. The transfer is delegated to the DMA controller, while the current thread, which corresponds to the PLC runtime thread, goes to sleep into a wait condition (`wait_for_completion`). Each DMA transfer uses an interrupt to signal when it has completed, or if some error occurred. Further analysis is required to understand the behaviour of a DMA transfer and its corresponding IRQ handler, but that goes beyond the purpose of this master thesis. Our best guess is that the DMA handler resets the initial GPIO pin and wakes up the PLC runtime thread.

Another interesting feature of the KBUS driver is that it exposes a `write` operation to the user, through which it is possible to enable/disable the above interrupt. The e!RUNTIME makes use of this system call to disable the interrupt while a new logic gets uploaded into the PLC, and then re-enables it before starting the logic. If a new logic comes, together with a new I/O configuration, the interrupt gets disabled because the runtime needs to reprogram the I/O module and the KBUS interface according to the new requirements. This behaviour gives us a hint to build another type of attack. Our findings about possible attacks are described in the next section.

## PLC attack

One of the first attack attempts we made was hooking the `kbus_ioctl` function and tampering the values inside the buffer. The effect was more powerful as the one achieved by Pin Control

Attack, because we were able to control both inputs and outputs. Anyway, this approach required function hooking, which is forbidden by our threat model (Section 3.2.2). A second attempt was multiplexing the SPI data pins to GPIO, to prevent the SPI controller to write to its I/O pins. This condition, unfortunately, led to an indefinite wait of e!RUNTIME, noticeable by the operator running the e!COCKPIT software. However, a better understanding of the SPI hardware protocol may allow the attacker to send fake data to the I/O module, through a technique known as *GPIO bit bang*. The bit banging technique consists of emulating in software all the operations made by a hardware controller (e.g. SPI) on I/O pins.

After having a good knowledge of the KBUS driver, we finally crafted three different attacks able to break the I/O communication without e!RUNTIME noticing anything and without hooking any function. The first two attacks are about Pin Configuration and Pin Multiplexing. From the previous analysis, we know that the pin 97, multiplexed as GPIO and configured as output, is used by KBUS to send the *transfer start* signal. If we either multiplex or configure the pin in a different way, we are able to prevent e!RUNTIME from reading and writing values to the I/O. This implementation demonstrates that I/O attack is perfectly applicable to real PLCs, even though it is still less powerful with respect to the original version described in Section 3.3.1. In fact, our version enables the attacker to perform only one of the operations defined for Pin Control Attack: disabling the output. Actually, since read and write are performed within the context of the same SPI transfer, also the input gets disabled at the same time. However, this is irrelevant because the PLC logic cannot write to output in any case, independently from the input. As discussed before, whether this operation may allow the attacker to alter the physical process, or not, is highly variable case by case. For instance, in our target system, we proved that by repeating the attack every 50 ms with a trivial script, we were able to modify the logic behaviour: the LED output started blinking every 50 ms instead of the original 500 ms. Furthermore, we found another interesting attack vector, which leverages the interrupt line used by the DMA controller and the `write` interface provided by the KBUS driver. Our experiments show that if this interrupt is masked while the PLC logic is running, the system is not able to read/write the I/O, thus obtaining again the same effect as the previous implementation. Although it is still very simple, this kind of attack, which we can call *IRQ Configuration Attack*, has some similarities with Pin Control Attack, such as the stealthiness and the hardware-level target. The PLC runtime is not able to notice our attacks, no failures or errors are reported and no function hooks are required. For both attack versions, the CPU overhead depends on the actual implementation, since the attacker can decide at which frequency disabling/enabling the I/O. Generally speaking, the overhead is very low, because only one operation is needed to do/undo the attack, respectively, which is typically translated into two or three processor instructions.

As discussed above, we believe that more sophisticated attacks are possible, since the basic hardware concepts described in Section 3.1 are still valid for a real PLC. The only difference is that, in this particular case, I/O pins are used as part of more complex protocols (SPI, DMA, etc.) and they are multiplexed to the corresponding controllers inside the SoC. Therefore, to understand how each pin is used and to obtain more elaborated attacks (e.g. faking data via GPIO bit bang), further research effort is required.

To conclude our PLC analysis, we briefly describe the implementation of our attacks on Wago PLC. Pin Configuration and Pin Multiplexing attacks are basically the same as for Raspberry Pi system. They can be executed in both kernel and user variants, requiring the corresponding privilege level as discussed in Section 3.3.1. One important difference here is that e!RUNTIME does not have its own mapped virtual addresses in user space, because the I/O is managed in kernel space by the KBUS driver. Thus, we distinguish two cases:

- **kernel-side attack:** the attacker can either remap the I/O physical addresses taken from the AM3517 manual [55], or re-use the addresses already mapped by the pin control subsystem;
- **user-side attack:** the attacker can only request a new mapping to the kernel, because no other available mappings exist in user space.

Re-using already mapped addresses is theoretically feasible, because the control registers are actually mapped into the kernel, as reported by the output below.

```
root@PFC200-4106BA:~ cat /proc/iomem
[...]
48002030-48002267 : pinctrl-single
48002a00-48002a5b : pinctrl-single
[...]
```

However, the attacker needs to know the kernel virtual addresses (e.g. by looking at page tables) in order to have access to the mapped registers.

Finally, for our IRQ configuration attack, we implemented it in two different variants as well: kernel side and user side.

**Kernel side** This version requires root privileges, since it is designed as a loadable kernel module. The module leverages the `disable_irq` function provided by the Linux kernel, which requires the interrupt line number to disable. Thus, the attacker needs to know the target system model, but no knowledge of the PLC logic nor of the I/O mapping is required, because the system uses the same configuration independently from the current logic. We found the interrupt line number by inserting a kernel probe for the `disable_irq` function, and triggering the PLC runtime to disable the interrupts while loading a new logic.

**User side** This version requires at least the same privilege level of the PLC runtime, who is able to enable/disable the interrupt with the following operations (from strace):

```
[...]
04:09:46.008222 open("/dev/kbus0", O_RDWR) = 11
[...]
04:09:46.009237 write(11, "\x01\x00\x00\x00", 4) = 0
[...]
04:09:46.070565 write(11, "\x00\x00\x00\x00", 4) = 0
[...]
```

Writing a 1 into the `/dev/kbus0` file disables the interrupt, while a 0 enables it. We can implement the attack by emulating these PLC runtime operations from user space. The effect of this second variant is the same as the kernel module one, but it requires less privilege and it could be exploited through a remote code execution vulnerability of the PLC runtime, which is again based on CODESYS [14, 15].

## **Chapter 4**

# **Pin Control Defense**

TODO Pin Control Defense design and implementation.

## Chapter 5

# Experimental Results

TODO Experimental Results.

## **Chapter 6**

# **Conclusions**

TODO Conclusions.

# Bibliography

- [1] A.Abbasi, M.Hashemi, “Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack”, Black Hat Europe, London (UK), Nov. 3-4, 2016, pp. 1-35, <https://www.blackhat.com/docs/eu-16/materials/eu-16...Programmable-Logic-Controller-Rootkit-wp.pdf>.
- [2] A.Abbasi, “Ghost in the PLC: stealth on-the-fly manipulation of programmable logic controllers I/O”, Technical Report TR-CTIT-16-02, Centre for Telematics and Information Technology (CTIT), University of Twente, Enschede (NL), Feb. 23, 2016, <http://eprints.eemcs.utwente.nl/26859/>.
- [3] “Pin Control Subsystem”, <https://www.kernel.org/doc/Documentation/pinctrl.txt>.
- [4] N.Falliere, L.O Murchu, E.Chien, “W32.Stuxnet Dossier”, Version 1.4, Febr. 2011, [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf).
- [5] R.Grandgenett, W.Mahoney, R.Gandhi, “Authentication Bypass and Remote Escalated I/O Command Attacks”, CISR ’15: Proceedings of the 10th Annual Cyber and Information Security Research Conference, Oak Ridge, Tennessee (USA), April 7-9, 2015, DOI <10.1145/2746266.2746268>.
- [6] D.Papp, Z.Ma, L.Buttyan, “Embedded systems security: Threats, vulnerabilities, and attack taxonomy” Privacy, Security and Trust (PST) 13th Annual Conference, Izmir (Turkey), July 21-23, 2015 pp. 145-152, DOI <10.1109/PST.2015.7232966>.
- [7] Z.Basnicht, J.Butts, J.Lopez Jr., T.Dube, “Firmware modification attacks on programmable logic controllers”, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, pp. 76-84, DOI <10.1016/j.ijcip.2013.04.004>.
- [8] D.Peck, D.Peterson, “Leveraging ethernet card vulnerabilities in field devices”, Proceedings of the SCADA Security Scientific Symposium, Miami Beach, Florida (USA), Jan. 18-19, 2009, pp. 1-19.
- [9] A.Cui, M.Costello, S.J.Stolfo, “When Firmware Modifications Attack: A Case Study of Embedded Exploitation”, 20th Annual Network & Distributed System Security Symposium, San Diego, California (USA), Febr. 24-27, 2013, DOI <10.7916/D8P55NKB>.
- [10] S.McLaughlin, “On Dynamic Malware Payloads Aimed at Programmable Logic Controllers”, In 6th USENIX Workshop on Hot Topics in Security, 2011.
- [11] S.McLaughlin, P.McDaniel, “SABOT: Specification-based Payload Generation for Programmable Logic Controllers”, CCS ’12: Proceedings of the 2012 ACM conference on Computer and Communications Security, New York (USA), Oct. 16-18, 2012, pp. 439-449, DOI <10.1145/2382196.2382244>.
- [12] D.Beresford, “Exploiting Siemens Simatic S7 PLCs”, Black Hat USA 2011, Las Vegas, Nevada (USA), Aug. 3-4, 2011, [https://media.blackhat.com/bh-us-11/Beresford/BH\\_US11\\_Beresford\\_S7\\_PLCs\\_WP.pdf](https://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_WP.pdf).
- [13] J.Klick, S.Lau, D.Marzin, J.Malchow, V.Roth, “Internet-facing PLCs as a Network Backdoor”, Proceedings of IEEE Conference on Communications and Network Security (CNS), Florence (Italy), Sept. 28-30, 2015, pp. 524-532, DOI <10.1109/CNS.2015.7346865>.
- [14] ICS-CERT, “ABB AC500 PLC Webserver CoDeSys Vulnerability”, April 30, 2013, <https://ics-cert.us-cert.gov/advisories/ICSA-12-320-01>.
- [15] ICS-CERT, “3S CODESYS Gateway-Server Vulnerabilities (Update A)”, March 13, 2014, <https://ics-cert.us-cert.gov/advisories/ICSA-13-050-01A>.

- [16] ICS-CERT, "Schneider Electric Modicon M340 Buffer Overflow Vulnerability", Dec. 17, 2015, <https://ics-cert.us-cert.gov/advisories/ICSA-15-351-01>.
- [17] ICS-CERT, "Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities (Update A)", Oct. 27, 2015, <https://ics-cert.us-cert.gov/advisories/ICSA-15-300-03A>.
- [18] ICS-CERT, "Rockwell Automation MicroLogix 1100 PLC Overflow Vulnerability", Jan. 26, 2016, <https://ics-cert.us-cert.gov/advisories/ICSA-16-026-02>.
- [19] ICS-CERT, "Eaton ELCSoft Programming Software Memory Vulnerabilities", June 30, 2016, <https://ics-cert.us-cert.gov/advisories/ICSA-16-182-01>.
- [20] P.Chen, X.Xing, B.Mao, L.Xie, "Return-oriented rootkit without returns (on the x86)" ICICS 2010: 12th International Conference on Information and Communications Security, Barcelona (Spain), Dec. 15-17, 2010, pp. 340-354, DOI [10.1007/978-3-642-17650-0\\_24](https://doi.org/10.1007/978-3-642-17650-0_24).
- [21] S.Checkoway, L.Davi, A.Dmitrienko, A.Sadeghi, H.Shacham, M.Winandy, "Return-Oriented Programming without Returns", CCS '10: Proceedings of the 17th ACM conference on Computer and Communications Security, Chicago, Illinois (USA), Oct. 4-8, 2010, DOI [10.1145/1866307.1866370](https://doi.org/10.1145/1866307.1866370).
- [22] R.E.Johnson, "Survey of SCADA Security Challenges and Potential Attack Vectors", ICITST 2010: International Conference for Internet Technology and Secured Transactions, London (UK), Nov. 8-11, 2010, pp. 80-85.
- [23] B.Miller, D.Rowe, "A survey of SCADA and critical infrastructure incidents", RIIT '12: Proceedings of the 1st Annual conference on Research In Information Technology, Calgary, Alberta (Canada), Oct. 10-13, 2012, pp. 51-56, DOI [10.1145/2380790.2380805](https://doi.org/10.1145/2380790.2380805).
- [24] G.P.H.Sandaruwan, P.S.Ranaweera, V.A.Oleshchuk, "PLC Security and Critical Infrastructure Protection", ICIIS 2013: IEEE 8th International Conference on Industrial and Information Systems, Peradeniya (Sri Lanka), Dec. 17-20, 2013, pp. 81-85, DOI [10.1109/ICI-InfS.2013.6731959](https://doi.org/10.1109/ICI-InfS.2013.6731959).
- [25] A.Clark, Q.Zhu, R.Poovendran, T.Baar, "An Impact-Aware Defense against Stuxnet", ACC 2013: 1st American Control Conference, Washington, DC (USA), June 17-19, 2013, pp. 4140-4147, DOI [10.1109/ACC.2013.6580475](https://doi.org/10.1109/ACC.2013.6580475).
- [26] D.Hadiosmanovi, R.Sommer, E.Zambon, P.H.Hartel, "Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes", ACSAC '14: 30th Annual Computer Security Applications Conference, New Orleans, LA (USA), Dec. 08-12, 2014, pp. 126-135, DOI [10.1145/2664243.2664277](https://doi.org/10.1145/2664243.2664277).
- [27] X.Wang, C.Konstantinou, M.Maniatakos, R.Karri, S.Lee, P.Robison, P.Stergiou, S.Kim, "Malicious Firmware Detection with Hardware Performance Counters", IEEE Transactions on Multi-Scale Computing Systems, Vol. 2, Issue 3, July-Sept. 2016, pp. 160-173, DOI [10.1109/TMSCS.2016.2569467](https://doi.org/10.1109/TMSCS.2016.2569467).
- [28] ARM, "TrustZone", <https://developer.arm.com/technologies/trustzone>.
- [29] P.Koeberl, S.Schulz, A.Sadeghi, V.Varadharajan, "TrustLite: A Security Architecture for Tiny Embedded Devices", EuroSys '14: Proceedings of the Ninth European Conference on Computer Systems, Amsterdam (Netherlands), April 13-16, 2014, DOI [10.1145/2592798.2592824](https://doi.org/10.1145/2592798.2592824).
- [30] A.Fuchs, C.Krauß, J.Repp, "Advanced Remote Firmware Upgrades Using TPM 2.0", in the book "ICT Systems Security and Privacy Protection: 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30 - June 1, 2016, Proceedings" edited by J.Hoepman, S.Katzenbeisser, Springer International Publishing, 2016, pp. 276-289, DOI [10.1007/978-3-319-33630-5\\_19](https://doi.org/10.1007/978-3-319-33630-5_19).
- [31] B.Lee, J.Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment", The Journal of Supercomputing, 2016, pp. 1-16, DOI [10.1007/s11227-016-1870-0](https://doi.org/10.1007/s11227-016-1870-0).
- [32] S.Zonouz, J.Rrushi, S.McLaughlin, "Detecting Industrial Control Malware Using Automated PLC Code Analytics", IEEE Security & Privacy, Vol. 12, Issue 6, Nov.-Dec. 2014, pp. 40-47, DOI [10.1109/MSP.2014.113](https://doi.org/10.1109/MSP.2014.113).
- [33] L.Garcia, S.Zonouz, D.Wei, L.P.de Aguiar, "Detecting PLC Control Corruption via On-Device Runtime Verification", Resilience Week (RWS), Chicago, Illinois (USA), Aug. 16-18, 2016, pp. 67-72, DOI [10.1109/RWEEK.2016.7573309](https://doi.org/10.1109/RWEEK.2016.7573309).
- [34] A.Cui, S.J.Stolfo, "Defending Embedded Systems with Software Symbiotes", in the book "Recent Advances in Intrusion Detection: 14th International Symposium, RAID 2011, Menlo

- Park, CA, USA, September 20-21, 2011. Proceedings”, edited by R.Sommer, D.Balzarotti, G.Maier, Springer Berlin Heidelberg, 2011, pp. 358-377, DOI [10.1007/978-3-642-23644-0\\_19](https://doi.org/10.1007/978-3-642-23644-0_19).
- [35] A.Seshadri, A.Perrig, L.Doom, P.Khosla, “SWATT: SoftWare-based ATTestation for embedded devices”, Proceedings of IEEE Symposium on Security and Privacy, Oakland, California (USA), May 9-12, 2004, pp. 272-282, DOI [10.1109/SECPRI.2004.1301329](https://doi.org/10.1109/SECPRI.2004.1301329).
- [36] C.Castelluccia, A.Francillon, D.Perito, C.Soriente, “On the difficulty of software-based attestation of embedded devices”, CCS’09: Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, Illinois (USA), Nov. 9-13, 2009, pp. 400-409, DOI [10.1145/1653662.1653711](https://doi.org/10.1145/1653662.1653711).
- [37] C.A.Gonzalez, A.Hinton, “Detecting Malicious Software Execution in Programmable Logic Controllers Using Power Fingerprinting”, in the book “Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference, ICCIP 2014, Arlington, VA, USA, March 17-19, 2014, Revised Selected Papers”, edited by J.Butts, S.Shenoi, Springer Berlin Heidelberg, 2014, pp. 15-27, DOI [10.1007/978-3-662-45355-1\\_2](https://doi.org/10.1007/978-3-662-45355-1_2).
- [38] J.Reeves, A.Ramaswamy, M.Locasto, S.Bratus, S.Smith, “Intrusion detection for resource-constrained embedded control systems in the power grid”, International Journal of Critical Infrastructure Protection, 2012, Vol. 5, No. 2, pp. 74-83, DOI [10.1016/j.ijcip.2012.02.002](https://doi.org/10.1016/j.ijcip.2012.02.002).
- [39] J.Habibi, A.Panicker, A.Gupta, E.Bertino, “DisARM: Mitigating Buffer Overflow Attacks on Embedded Devices”, in the book “Network and System Security: 9th International Conference, NSS 2015, New York, NY, USA, November 3-5, 2015, Proceedings”, edited by M.Qiu, S.Xu, M.Yung, H.Zhang, Springer International Publishing, 2015, pp. 112-129, DOI [10.1007/978-3-319-25645-0\\_8](https://doi.org/10.1007/978-3-319-25645-0_8).
- [40] A.Francillon, D.Perito, C.Castelluccia, “Defending Embedded Systems Against Control Flow Attacks”, SecuCode ’09: Proceedings of the first ACM workshop on Secure execution of untrusted code, Chicago, Illinois (USA), Nov. 9, 2009, pp. 19-26, DOI [10.1145/1655077.1655083](https://doi.org/10.1145/1655077.1655083).
- [41] F.Abad, J.Woude, Y.Lu, S.Bak, M.Caccamo, L.Sha, R.Mancuso, S.Mohan, “On-Chip Control Flow Integrity Check for Real Time Embedded Systems”, 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), Taipei, Taiwan, Aug. 19-20, 2013, pp. 26-31, DOI [10.1109/CPSNA.2013.6614242](https://doi.org/10.1109/CPSNA.2013.6614242).
- [42] L.Davi, P.Koeberl, A.Sadeghi, “Hardware-Assisted Fine-Grained Control-Flow Integrity: Towards Efficient Protection of Embedded Systems Against Software Exploitation”, DAC ’14: Proceedings of the 51st Annual Design Automation Conference, San Francisco, California (USA), June 1-5, 2014, pp. 133:1-133:6, DOI [10.1109/DAC.2014.6881460](https://doi.org/10.1109/DAC.2014.6881460).
- [43] L.Davi, M.Hanreich, D.Paul, A.Sadeghi, P.Koeberl, D.Sullivan, O.Arias, Y.Jin, “HAFIX: Hardware-Assisted Flow Integrity Extension”, DAC ’15: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, California (USA), June 7-11, 2015, pp. 74:1-74:6, DOI [10.1145/2744769.2744847](https://doi.org/10.1145/2744769.2744847).
- [44] S.Das, W.Zhang, Y.Liu, “A Fine-Grained Control Flow Integrity Approach Against Runtime Memory Attacks for Embedded Systems”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 24, No. 11, Nov. 2016, pp. 3193-3207, DOI [10.1109/TVLSI.2016.2548561](https://doi.org/10.1109/TVLSI.2016.2548561).
- [45] T.Abera, N.Asokan, L.Davi, J.Ekberg, T.Nyman, A.Paverd, A.Sadeghi, G.Tsudik, “C-FLAT: Control-FLow ATtestation for Embedded Systems Software”, CCS ’16: Proceedings of the 23rd ACM Conference on Computer and Communications Security, Vienna (Austria), Oct. 24-28, 2016, pp. 743-754, DOI [10.1145/2976749.2978358](https://doi.org/10.1145/2976749.2978358).
- [46] S.Embleton, S.Sparks, C.C.Zou, “SMM rootkit: a new breed of OS independent malware”, Security and Communication Networks, Vol. 6, No. 12, Dec. 2013, pp. 1590-1605, DOI [10.1002/sec.166](https://doi.org/10.1002/sec.166).
- [47] F.Zhang, “IOCheck: A framework to enhance the security of I/O devices at runtime”, 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest (Hungary), June 24-27, 2013, DOI [10.1109/DSNW.2013.6615523](https://doi.org/10.1109/DSNW.2013.6615523).
- [48] Raspberry Pi Foundation, “Raspberry Pi”, <https://www.raspberrypi.org/>.
- [49] Red balloon security, “Symbiote Defense”, <http://www.redballoonsecurity.com>.
- [50] Trustworthy Cyber Infrastructure for the Power Grid, “Autoscopy Jr.”, <https://tcipg.org/technology/autoscopy-jr>.
- [51] Raspberry Pi Foundation, “BCM2835”, <https://www.raspberrypi.org/documentation/hardware/raspberrypi/bcm2835/README.md>.

- [52] 3S-Smart Software Solutions GmbH, “CODESYS Control for Raspberry Pi SL”, <http://store.codesys.com/codesys-control-for-raspberry-pi-sl.html>.
- [53] 3S-Smart Software Solutions GmbH, “CODESYS Development System V3”, <http://store.codesys.com/codesys.html>.
- [54] WAGO Kontakttechnik GmbH & Co., “Linux - Automation for the Future”, <http://global.wago.com/en/products/new-items/overview/basic-page-2600.jsp>.
- [55] Texas Instruments, “AM3517 Sitara Processor Technical documents”, <http://www.ti.com/product/AM3517/technicaldocuments>.
- [56] “strace: Linux syscall tracer”, <https://strace.io/>.
- [57] J.Keniston, P.S.Panchamukhi, M.Hiramatsu, “Kernel probes”, <https://www.kernel.org/doc/Documentation/kprobes.txt>.