Noname manuscript No.
(will be inserted by the editor)

Hardware-Layer Intelligence Collection for Smart Grid Embedded Systems

Charalambos Konstantinou · Michail Maniatakos

Received: date / Accepted: date

Abstract Smart grids include a variety of microprocessor-based embedded systems, interconnected with communication technologies. In this interaction, hardware is the lower level of abstraction. Insecure and unprotected hardware design of smart grid devices enable system operation compromise, eventually leading to undesirable and often severe consequences. In this paper, we discuss how the hardware of grid equipment can be used to collect intelligence utilized towards beneficial or malicious purposes. We consider different access scenarios and attacker capabilities as well as equipment location in the grid. The outcome of "hardware hacking" is examined in both device and grid operation levels. Finally, we present hardware hardening techniques, aiming to make components attack-resistant and reduce their vulnerability surface.

Keywords Security · Hardware · Embedded systems · Intelligence · Smart grid

1 Introduction

Despite the on-going effort to transform the electric power grid into an advanced, decentralized infrastructure with information and communication technologies, legacy components continue to dominate the infrastructure of contemporary power grid systems. The equipment used in the electricity sector typically has a lifecycle typically exceeding 20 years [1]. Retroactively adding cybersecurity mechanisms can be extremely challenging, due to the limited computational capabilities of legacy devices.

Legacy devices are slowly replaced by modern embedded systems. Such systems are often based on designs with Commercial Off-The-Shelf (COTS) products. The use of COTS components in industrial control settings is attractive since it provides the immediate benefit of robust hardware and stable, readily available software modules. At the same time, vulnerabilities of COTS systems can be ported to the critical infrastructure which, due to its always-on and life-critical operation, can not be easily brought down for maintenance and security patching [2].

In addition to COTS-based designs, smart grid systems include proprietary information due to custom standards and protocols. Also, many designs use specialized software and hardware. These customized system implementations and interfaces are often designed to support specific processes and may not have any security capabilities built-in. Additionally, proprietary systems are not exposed to public auditing, thus requiring more time to patch their security vulnerabilities. For example, a heap buffer overflow vulnerability identified in proprietary industrial automation systems for historian servers could potentially lead to a Stuxnet-type attack [3].

Hence, despite the grid transformation, the mix of legacy, modern, and proprietary components provide opportunities for advanced cyber-intrusions. In this evolving ecosystem, the role of hardware layer in the cybersecurity context of grid modernization is critical. At the lowest level of abstraction, hardware can be considered the root of trust. All other layers (firmware, software, network, process) rely and build on it [4]. Therefore,

C. Konstantinou
FAMU-FSU College of Engineering, Center for Advanced Power Systems, Florida State University, Tallahassee, FL
E-mail: ckonstantinou@fsu.edu

M. Maniatakos
Center for Cyber Security, New York University Abu Dhabi, Abu Dhabi, UAE

compromising the hardware layer effectively compromises all the layers above it.

The hardware layer of electronic equipment includes microcontrollers, data storage disks, flash memories, communication ports, etc. In order to undermine the operation of a device at the hardware level, it is necessary to corrupt and/or manipulate a combination of hardware objects. Smart grid devices include various embedded systems such as Programmable Logic Controllers (PLCs), Phasor Measurement Units (PMUs), Remote Terminal Units (RTUs), Supervisory Control and Data Acquisition (SCADA) servers, workstations, relays, and communication routers. These systems are susceptible to both invasive and non-invasive hardware attacks. For example, hardware backdoors can be exploited by adversaries to enable remote control of the target device [5]. The activation of hardware attacks can rely on a specific timing or functional condition which when activated will degrade the system performance or even disable the circuit logic [6, 7].

The intelligence collected at the hardware level can be utilized towards both beneficial and malicious purposes. For instance, attackers can introduce hardware backdoors to the system overriding the control of the operation status of a device. The cyber-attacks to the Ukraine electric system in 2015 and 2016, and the resulted service outages to customers, demonstrated the eventual impact of such attacks [8, 9]. In the 2015 incident, the adversaries uploaded malicious firmware the Serial-to-Ethernet converters of the substation devices, rendering them inoperable and unrecoverable. On the other hand, hardware-collected intelligence can be utilized to perform vulnerability assessments and penetration tests in order to identify security weaknesses and potential risks within the industrial operation [10]. Due to the real-world consequences of smart grid operations, these assessments and tests must be performed regularly. In addition, they should take into consideration the sensitive smart grid dependencies and connectivity and also account for all possible operating conditions.

Security standards, guidelines, and regulatory documents play a key role in smart grid cybersecurity. These publications provide guidance in understanding smart grid interoperability, interconnections, architectural designs, and structural layers in order to achieve seamless, secure, and reliable operation of the electric power system. Standards and guidelines, however, often omit to include provisions about protecting the hardware layer, assuming that the hardware is always secure. Recent work has disproved this assumption: an adversary can modify the content of flash memories within the hardware level of RTUs in order to instrument False Data Injection (FDI) attacks [11].

In the 2016 report of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the number of ICS-CERT responses to cybersecurity threats across the energy infrastructure sector was $\simeq$ 20% [12]. The internals of devices are often easy to access, identify, and probe. Adversaries typically start with gathering information about the device operation and its configurations, through the internet and/or by purchasing target hardware [13]. Armed with the intelligence gathered during the reconnaissance phase, the next step is to find possible vulnerabilities. This can be achieved, assuming device possession, by tearing down the hardware and disassemble its electronics and software. In case of firmware access, reverse engineering of the firmware file contents can provide valuable insights. Furthermore, the analysis of external interfaces such as debug and communications connections can provide extensive data with regards to the system operation. Also, reverse engineering of Integrated Circuits (ICs) can provide valuable information, such as cryptographic keys and contents of non-volatile memories.

In this paper, in order to highlight the importance of secure hardware designs, we describe methodologies for information extraction via the hardware, assuming various access levels and capabilities. Depending on the device location in the grid, the use of the collected information is discussed for both device and grid operation level. Finally, we present defense methodologies which can be applied towards protecting and monitoring the hardware layer of grid infrastructure.

The rest of the paper is organized as follows: Section 2 further motivates the process of hardware-based information extraction. Section 3 discusses the different techniques for intelligence extraction, under different assumptions about the capabilities of the attacker and the proximity to the actual device. Section 4 examines hardware-based monitoring and protection methodologies for smart grid embedded systems, followed by conclusions in Section 5.

2 Uses of Collected Information

As discussed in the introduction, information collected at the hardware level of smart grid systems can be used to enhance or undermine security, depending on the intention of the person or group of people who acquire(s) this information. Specifically, the intelligence could be obtained by the legitimate user of the device (e.g., utility, manufacturer, etc.) and used to enhance the protection of the equipment. Insider threats, however, e.g., disgruntled employees, can be a significant security risk to any organization. Hardware intelligence can also be

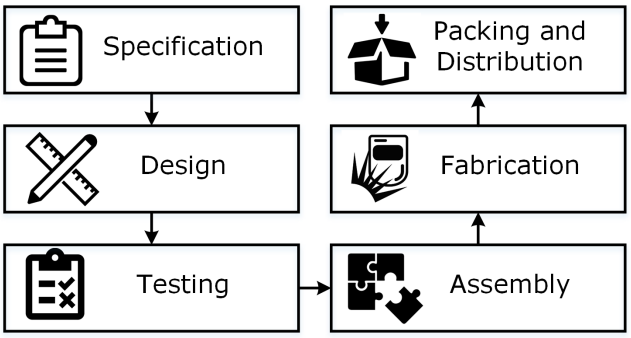


Fig. 1: Hardware supply chain.

acquired by illegitimate users such as ethical and malicious hackers. Ethical hackers use the obtained data in order to test and evaluate the system security, compared with adversaries that have malicious or criminal intent.

2.1 Enhancing Security

The major obstacles towards secure industrial systems are legacy equipment, practical difficulties in vulnerability management, and convergence problems between the operational and the information technology world. Nevertheless, performing penetration tests and risk analysis assessments are part of recommended security services for the utility operators [2]. Penetration testing aims to identify ways of gaining access to a system by using common tools and techniques developed by hackers. The results of penetration testing should be examined in-depth (risk analysis) and the discovered vulnerabilities should be mitigated.

Given today's globalized supply chain, trusting hardware requires establishing a chain of trust, starting from the IC manufacturer to the administrator of the asset. The supply chain can abstracted in six main phases, as shown in Fig. 1 [6]:

- Specification phase, defining the system characteristics;
- Design phase, developing the technology;
- Fabrication phase, in which the designers create a mask set and use wafers to fabricate the IC masks;
- Testing phase, using test vectors to verify the system functionality;
- Assembly phase, assembling the tested hardware units on a Printed Circuit Board (PCB); and
- Packing and distribution phase, packaging and delivering the product to the user/customer.

Each step requires vigilance and the ability to detect changes to phase-specific processes. In addition to penetration tests and determining trust due to supply chain challenges, grid utilities often test the purchased devices in a Hardware-In-the-Loop (HIL) laboratory testbed. In the past, such testbeds were designed to verify the symbiotic relationship of the equipment with other products and assess as well as testing several configuration and application scenarios in a controlled environment. Recently, however, HIL testbeds are also used for cybersecurity assessment and educational purposes. The HIL environment can assist the utility to verify the hardware functionality of a device and test potential security solutions. HIL testebeds can also be utilized to address identified vulnerabilities in a non-destructive way and without the hazards of testing in a production environment.

Information collected at the hardware layer can be utilized also for military intelligence. As an example, a detailed list of the equipment hardware features used in national nuclear power plants allows nations to avoid technological surprise. Furthermore, side-channel data such as electromagnetic emanations can assist in identifying interference with other systems [14]; typically power plants are located near or along with military installations [15].

It is evident that the information collected from the hardware can be utilized by different parties. Device owners – typically utilities – can use the acquired intelligence to ensure the interoperability of security solutions across the infrastructure. Manufacturers can utilize the acquired intelligence to guarantee that security systems are designed and implemented in accordance with all applicable requirements. Third-party independent inspection teams can also provide approvals and audit the hardware security of grid equipment. Furthermore, devices used in military installations can be tested and certified for hardware emission security, and thus added in an approved product list [16].

2.2 Undermining Security

Given the growing presence of microprocessor-based hardware equipment in smart grid implementations, the cyber-threat landscape is constantly evolving. As a consequence, malicious adversaries have more opportunities for Denial-of-Service (DoS) attacks, i.e., temporarily or permanently disruptions to the device operation or even the power system. For example, modifications at the hardware/firmware level of a recloser controller could disable the communication of the device to the SCADA master station [17]. Moreover, compromised hardware units could result in devices that operate maliciously and even restrain the booting sequence, i.e., fully compromise the device by realizing a DoS or Distributed DoS (DDoS) attack [18].

The task of providing security services for the smart grid heavily depends on authentication, authorization, and message integrity of smart grid devices. Collected intelligence from the hardware layer could potentially lead to system vulnerabilities, leading to extraction of authentication session details that can be replayed to grant access to smart grid systems. Authentication mechanisms can be bypassed via emanation analysis, i.e., the analysis of eavesdropping information based on the emanations given off by the device hardware. An antenna sited close to the chip can read the electromagnetic field variations induced in the surrounding area of the device, e.g., the attacker can attach an antenna close to the IC and analyze the waveform depicted in the oscilloscope and thus fully or a partially recovery the authentication keystrokes [19].

Another potential ramification of hardware "emitted" information is to bypass security mechanisms and features in the device causing privilege escalation. As a case study, a fabrication attack at the transistor level can lead to privilege escalation at a modern operating system which is typically used in server computers of utility substations [20, 21]. Additionally, the residing data of non-volatile memories that exist in RTU hardware platforms can be utilized towards FDI attacks able to bypass Bad Data Detection (BDD) schemes and violate the correct operation of state estimation in the grid [11].

In smart grid systems, the Advanced Metering Infrastructure (AMI) covers the fundamental functions of an advanced metering system. A typical AMI consists of resource-constrained smart meters and integrated service switches. Since the AMI handles sensitive data, its protection is of paramount importance. Energy theft is one of the most significant issues related to smart grids. It is estimated that utility companies lose more than $25 billion every year due to energy theft around the world [22]. Besides meter reversal, a user can replace a smart meter with a device that successfully interacts with the grid, but reports zero usage (cloning) [23]. Thus, the hardware design of smart meters in AMI should be capable of detecting and reporting hardware tampering to identify energy theft or billing fraud.

Besides energy theft, Intellectual Property (IP) theft can allow competitor manufacturers to gain a marketplace advantage. IP theft accounts for 62% of the cybercrime damages, while many analysts concur that the extent of IP stolen in reality cannot be measured with confidence currently [24]. IP reverse engineering has emerged as a major concern for IP owners as adversaries possess increasingly sophisticated tools for revealing the IP design. Hence, IP theft of smart grid devices should be addressed with proper hardware security measures and tamper-evident mechanisms.

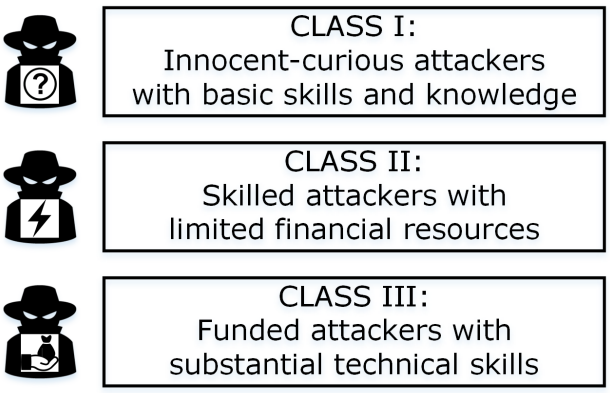


Fig. 2: Attackers categories.

The use of hardware collected intelligence can be the foundation of various attack vectors. However, it is infeasible to enumerate all scenarios and effects of how such information can be utilized in the smart grid. Nonetheless, it is possible to identify attackers categories based on their skills and knowledge as well as their financial resources [25, 26]. Fig. 2 presents the three classes of attackers based on these pillars:

- ***Class I***: Innocent-curious attackers are motivated to learn device details but, although they may have sufficient funds, they possess only basic skills and knowledge of how to extract information from the hardware level.
- ***Class II***: Clever individuals, either insiders or outsiders, as well as a group of attackers able to access information regarding hardware units and infiltrate to the system. However, this class of adversaries cannot gain access to critical equipment or areas of the system that can cause undesirable state changes to the smart grid due to their limited financial resources.
- ***Class III***: Funded individuals, organizations, and nation-states with large budgets and substantial technical education and experience of how to intrude hardware systems and access vital assets of the grid in order to execute a sophisticated attack using the most advanced tools.

3 Equipment Access Level

An important dimension towards quantifying the amount of information that can be extracted from the device is the level of device access, i.e., whether users possess a physical copy of the device and whether they can tear it down (physical breach).

Table 1: Methods to collect information at the hardware level based on the equipment access.

Device	Distance	Category	Technique	Min. class of attacker	Data asset	References
Possession	Zone 0	Chassis intrusion	Micro-probing	III	User, Device	[27]
			Laser cutting	III	User, Device	[28]
			Focused Ion Beam (FIB)	III	User, Device	[27, 29, 30]
			Failure analysis using decapsulation	II	User, Device	[13, 29, 31, 32]
			Circuit bending	II	Device, System	[33]
			External interfaces and exposed buses	II	User, Device, System	[13, 34–37]
			Flash memory	II	User, Device, System	[11, 38]
	Zone 1	Interface access	Control of environmental conditions	II	Device, System	[39–42]
			Side-channel analysis	II	User, Device	[43, 44]
			Protocol decoding	II	User, Device, System	[45–47]
Non-Possession	Zone 2	Proximity access	GPS spoofing	II	Device, System	[48–56]
			Optical observation	I	User, Device, System	[57–59]
			Side-channel analysis	II	User, Device	[43, 60–62]
	Zone 3	Network interface	Replay attacks	I	Device, System	[63–65]
			Covert channels	II	User, Device, System	[66–69]

Regarding physical security, there are multiple embodiments of hardware mechanisms that provide protection against physical attacks, ranging from tamper resistant security modules, security bits and one-way screws, to opaque or hardened fencing shielding assets from off-site attacks. In the hardware level of a device, enclosures and housings have to be bypassed in order to get access to internal circuitry. In addition, anti-tamper detection mechanisms should raise an alert of unauthorized attempts to the appropriate personnel. For instance, sensors installed near the PCB of a device can detect operational or environmental changes. Authentication module cards can be used for cryptographic computation and secure authentication to avoid success of any kind of impersonation attacks. Anti-tamper mechanisms can also response to tampering efforts, i.e., take appropriate countermeasures upon the detection of tampering such as enable logging features, zeroization[1], and even disable or destroy the device.

The location of the device in the grid is also related with the physical security of the equipment. Generation and transmission devices are typically equipped with advanced security technology since they are susceptible to more serious risks compared to hardware devices at the distribution and consumer level. This is evident by the attack incidents in the energy sector. One of the most prominent examples is the Metcalf transmission 500 kV substation attack [70]. In April 2013, gunmen shot 17 transformers over the course of 19 minutes. Prior to the attack, a series of fiber-optic telecommunications cables in an underground vault were cut. The attack inflicted substantial damage to the substation requiring over $15 million worth of repairs as the substation was down for 27 days. Under slightly different circumstances, there could have been notable wide-scale power outages [71].

In addition to the device location in the smart grid, the operational purpose and criticality of the equipment plays a major role in the hardware intelligence collection process. From an adversary perspective, the payload of the acquired information would be beneficial if the attack could lead to undesirable effects causing not only device disruption but also a chain reaction to the power system. As an example, the impact of exploiting vulnerabilities of a monitoring Human Machine Interface (HMI) platform [72] is less significant than substation Serial-to-Ethernet converters [73] or relay controllers [17]. A hard-coded password vulnerability in a HMI monitoring product provides access to the device and enables adversaries to observe a particular smart grid routine. On the other hand, exploitation of firmware vulnerabilities in equipment that connects serial devices to Ethernet networks can have severe consequences, as evident by the Ukrainian incident [8].

The collection of hardware intelligence requires extensive knowledge about vulnerability discovery and exploitation as well as reverse engineering tools. Determination and persistence are key factors in this process. The first objective is to understand the device functionality in the grid and identify, if possible, the hardware components of the device. In case of physical access to the PCB of the equipment, any interface accessible – such as debug ports and communication connections – could enable extraction of program code and data, and even potentially be an avenue for attack [33]. Interfaces such as JTAG (Joint Test Action Group – IEEE Std 1149.1) and serial access ports can be used beyond their specification purposes. The JTAG protocol, for instance, is a serial protocol similar to the synchronous SPI protocol with an extra mode selec-

[1] In cryptography, zeroization is the method of erasing sensitive information such as cryptographic keys and critical memory from a cryptographic module to prevent their disclosure if the equipment is tampered.

tion pin TMS (Test Mode Select) [74]. The JTAG test access port cannot only be used to apply test vectors but also to transfer debugger data and enable serial access to the internal scan chains. Furthermore, access is typically given to the instruction memory to allow uploading and modification of both firmware and software. Thus, unauthorized users can use JTAG for reverse engineering and acquire IP [75].

In addition to debug ports and interfaces, the residing hardware code and data can be obtained from on-board memory units [11]. Then, one can disassemble, modify, recompile, and reprogram the device. It is also feasible to gather hardware-based data using tools such as a logic analyzer, oscilloscope, dedicated sniffers, etc. Such data allows the identification of protocols used in the device and generate, for instance, malformed packets triggering unintended operations to the device. Mechanical anti-tampering mechanisms, such as encapsulation of critical components using epoxy or other adhesives, can be bypassed using epoxy removal and IC delidding [76]. The aim of delidding is to get access to the actual die of the hardware component, e.g., memory, microprocessor, etc. Once the die is accessible, silicon analysis using advanced tools and equipment can allow extraction of information such as cryptographic keys and non-volatile memory code.

The access and manipulation of hardware configuration data in smart grid systems can lead to loss of confidentiality, availability, and integrity of information, as well as to disruption of critical services. Thus, the information extracted from the hardware level can be classified into different categories of assets based on the system's threat analysis model:

- ***User data***: The stored information in the hardware layer may include confidential data of the legitimate user such as credentials and cryptographic keys, contact details (e.g., operator's email), etc.
- ***Device data***: The hardware units of smart grid embedded systems may contain device data assets such as functionality configuration parameters, IP, etc.
- ***System data***: The extracted information from hardware can be system-related details including organization security policies, network infrastructure design data, etc.

Table 1 summarizes the techniques of how to collect intelligence at the hardware layer based on the device access level and the distance from the equipment, the minimum class of attacker required to perform such technique, and the asset level of the extracted data.

3.1 Possession of device

In case the legitimate or unauthorized user possesses the hardware equipment, there are two access categories depending on whether the device can be physically tampered with or not, i.e., chassis intrusion or interface access only.

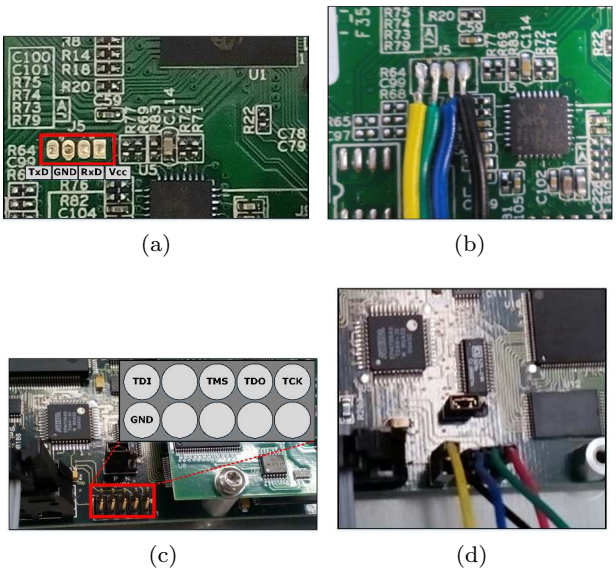
3.1.1 Chassis intrusion

In this scenario, tampering mechanisms need to be bypassed. Tampering mechanisms are divided into four groups [77, 78]:

(a) Resistance: Consists of features and specialized materials aiming to make tampering difficult. Examples of tamper resistance include locks, screws, tight airflow channels, hardened steel enclosures, etc.
(b) Evidence: Refers to techniques ensuring that there is proof after the act of tampering, i.e., irreversible physical or cyber evidence which can be observed in a subsequent audit. Examples of tamper evidence include seals, stamps, tapes, etc.
(c) Detection: Consists of mechanisms with the ability to sense efforts compromising the integrity of hardware and its residing data. Tamper detection methods may also initiate protection mechanisms. Examples of tamper detection include switches such as pressure contacts and magnetic switches, sensors such as temperature and radiation sensors, and circuitry such as flexible circuitry and fiber optics.
(d) Response: Refers to countermeasures taken upon the detection of tampering with the purpose of preventing modification, misuse, or disclosure of device data. For instance, a tamper response technique could erase portions of memory to prevent access to critical information.

In this category, the attacker or the legitimate user possesses physically the device, i.e., the distance between the hardware and the user is negligible (***Zone 0***), and he/she is able to defeat and bypass the tamper-protection mechanisms. The full access to the device and its internal structures allow to break tamper seals with impunity, extract information from chips, and understand in-depth the device functionality. Provided below is a list of methodologies to collect hardware intelligence with the requirement of direct device access and using both damaging and non-damaging analysis tools.

- **Micro-probing** is the technique of attaching probe tips to internal wiring of a chip for signal eavesdropping. It is often used to extract contents of memory such as user or/and device secret keys [27]. Micro-probing can also be used for internal fault attacks as it allows



(a) (b) (c) (d)

Fig. 3: The identification and the connection to (a)-(b) UART and (c)-(d) JTAG pinout.

to observe, manipulate, and interfere with the device. Micro-probing requires a station that typically includes a microscope, micromanipulators and micropositioners, probes, device test socket, and amplifiers. Due to advances in chip packaging and highly-integrated chips (sub-micron), micro-probing often becomes difficult for tightly integrated hardware components.

– **Laser cutting** is used to remove the passivation layer in order to observe the metal layer. This technique requires a laser cutting system which may cost a few thousand dollars. Despite the high cost, it has shown that laser cutting microscope station can recover residing secret keys and authentication values from the device internals [28].

– **Focused Ion-Beam (FIB)** is a technique that uses an ion source to bombard the chip with ions in order to get access to modules, e.g., make holes in protective layers and allow for probing and extraction of critical user and device specific data without authorization. Besides creating test points, FIB systems are used in imaging, repairing, and failure analysis [27, 29, 30].

– **Failure analysis using decapsulation** allows to remove encapsulated components and silicon die using chemical or/and mechanical means in order to expose the internal components of the package. One of the most common methods of decapsulation is via wet chemical etching with etchants such as fuming nitric acid and sulfuric acid [13, 29, 31, 32].

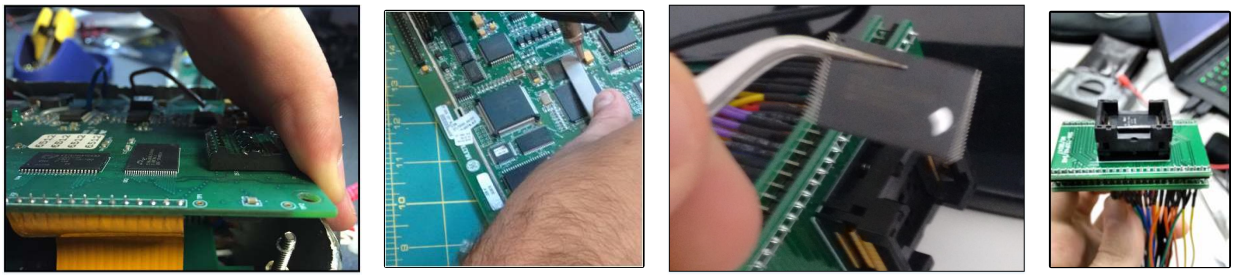
– **Circuit bending** is the process of modifying the components or structure of an electronic circuit [33]. That may include shorting particular lines, replacing or even adding hardware in order to observe particular behaviors in device or/and system level. For example, the circuit modification in a droop speed control module can result in an increase generator speed maximizing the mechanical stress and cause the rotor to pull out of synchronism.

– **Exposed buses** allow a device to interact with other components in the system: "a product's lifeline to the outside world" [13]. Such interfaces include JTAG, USB, Ethernet, RS232/485, UART, etc. For example, UART (Universal Asynchronous Receiver/Transmitter) ports designed for asynchronous serial communication and debugging purposes, can provide a terminal session running as root without requiring any additional authentication [34]. Such session can provide access to confidential cryptographic data, access control lists, IP assets, access tokens, etc. A logic analyzer, an oscilloscope, other tools [35], or even the variations of the multimeter can assist in identifying the UART pins [36]. Since the UART port is not designed to be utilized by the end users, no pins or connectors are attached. Thus, it is necessary to attach headers or solder the pinout connection, i.e., reconnect the debug circuitry. Fig. 3 shows the UART and JTAG ports connections for an embedded platform. In addition to external interfaces, exposed buses in the circuitry can provide access to the device's internal data [37].

– **Flash memory** is the most dominant electronic non-volatile storage medium. As such, it has widespread use in embedded systems. There are three main acquisition techniques to extract firmware code and data from flash chips [38]: 1) Using flasher tools, 2) through JTAG test access port, and 3) via physical extraction from the chip. The chip-off data acquisition process is shown in Fig. 4. The access to the memory contents allows to disassemble and analyze the system components. For firmware residing flash memories, the objective is to locate and extract functional blocks (e.g., binary code, scripts, configuration files, web interfaces, etc.) from the firmware package [79]. As a result, one can reveal information about the system features, leverage code vulnerabilities, and even replace the hardware-stored key with a known value or modify parts of the image in order to alter the system functionality [11, 28].

3.1.2 Physical interface access

In this category, the device is accessed physically by the attacker or the legitimate user, however, the system hardware cannot be tampered. The space between the user and the hardware of the device can be up to a certain point in which the physical and network characteristics of the equipment can be observed, e.g., within



(a) (b) (c) (d)

Fig. 4: Flash memory data acquisition process: (a) Printed Circuit Board (PCB), (b) de-soldering, (c) flash chip, (d) memory chip in the TSOP (Thin Small-Outline Package) socket in order to be read via a commercial or user-build chip reader.

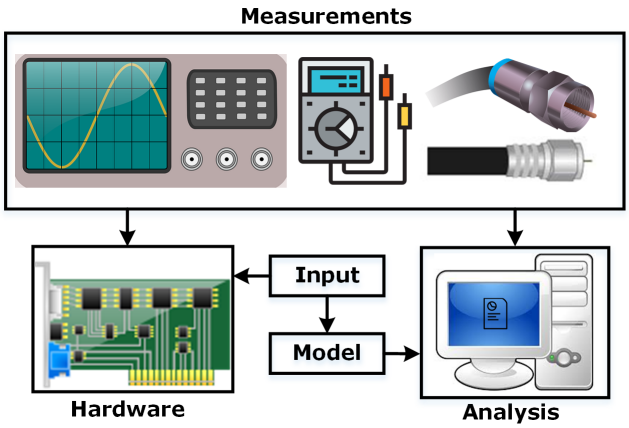


Fig. 5: Side-channel analysis methodology: it compares observations of the side-channel measurements with model estimations of the leakage.

a few feet (***Zone 1***). Thus, the access and monitoring of hardware could allow protocol decoding via Man-in-the-Middle (MitM) interception, fault injection, side-channel attacks, etc. In the following paragraphs, we describe procedures of how to collect intelligence at the hardware level without breaking physical tamper mechanisms on the device.

– **Control the environmental conditions:** The manipulation of the environment around a device enables a variety of attack vectors, such as data modification, circumvention of authentication algorithms, reset of protection bits, etc. Abnormal environmental conditions may subject the device to Ultra-Violet (UV) radiation light, laser, electrical noise, X-rays, extreme temperature, electromagnetic fields, etc. [40–42]. The exposure of the device to such environmental conditions could inject faults to the hardware components affecting the device as well as the system operation. For example, fault injection techniques could control individual bits of SRAM in a microcontroller and flip specific bit values in order to disable protection routines [39].

– **Side-channel analysis**: As shown in Fig. 5, side-channel information is based on the exploitation of implementation-based weaknesses which allow the leakage of secret information through covert channels, such as power consumption, electromagnetic emanation, acoustic information, fault propagation, vibrations, timing and thermal variations [43, 44]. For example, non-invasive measurements of computation time, i.e., measuring the required time to finish a cryptographic process may allow extraction of encryption keys [80]. Also, clock and timing variations, e.g., speed up or slow down the system clock, could result in an unintended operation or even induce failure to the device hardware units. Additionally, the power consumption of a device can be utilized towards revealing and breaking cryptographic schemes. Since the power consumption of a device depends on its current activity and the state of its components (due to the nature of CMOS transistors [81]), different power analysis techniques (e.g., simple power analysis, differential power analysis, etc.) can be used to extract cryptographic keys and other secret information from the hardware [44]. Furthermore, glitches inserted in the power supply and clock signals could undermine the device security. Glitch attacks, besides electrical pulses, could also be based on thermal and electromagnetic field radiation pulses that cause fast changes in the signals supplied to the hardware components of the device.

– **Protocol decoding**: Many legacy systems in the smart grid environment are based on weak authentication and communication protocols which are often proprietary in-house implementations [82]. Hence, eavesdropping techniques enable high-resolution monitoring of the analog characteristics of supply and interface connections. Also, the recording of the transmitted signals

occurring on the sniffing lines can lead to valuable information, e.g., password data, log transactions and processes, sensitive business logic, etc. Protocol emulation and transmission of modified values could result in discovering errors and security loopholes in the protocol implementation [45]. For instance, it is has been shown that modified code on SD cards could perform MiTM attacks which are difficult to detect, since the SD card command processing is based on interrupt-driven callbacks processed by the microcontroller [46]. Also, it has been demonstrated that devices running legacy operating systems could transmit an obfuscated version of the system password over the serial port [47].

3.2 Non-possession of device

In this scenario, the user is able to either approach or/and interface with the device, but the physical access to the equipment is not possible. For example, NERC (North American Electric Reliability Corporation) – CIP (Critical Infrastructure Protection) 005 and 006 standards require the implementation of electronic and physical security perimeter, respectively, inside which all critical cyber-assets reside [83]. The appropriate level of physical protections required, largely depends on the device purpose and operation, its operation environment and location in the grid, as well as the value and sensitivity of the device data.

3.2.1 Proximity access

Due to the "secure premise" of the hardware components, access is only allowed to the physical proximity of the device. Therefore, one can observe the external characteristics of the equipment within a few yards, e.g., in the substation area. This access zone to the device is named ***Zone 2***.

– **GPS spoofing:** The requirement of rapid and precise data acquisition in the smart grid have promoted GPS time synchronization as a trusted wireless clock synchronization mechanism for synchronized sensor monitoring equipment. For example, PMUs rely on GPS synchronized signals in order to provide time-stamped circuit quantities of power lines, i.e., phasors. A spurious GPS signal can result, however, in modified timestamp reference for PMU measurements [48–52]. The vulnerability of the GPS-dependent grid infrastructure to GPS spoofing has been acknowledged by NERC [84]. According to NERC, each organization needs to ensure that reliability-critical applications are not affected by GPS signals disruption. Nevertheless, studies have shown that erroneous time stamping of PMU data can affect the reliability of applications such as voltage and small-signal stability monitoring, distance line protection, remedial action controllers, etc. [53–56]. For delivering the GPS spoofing attack, the adversary can be located in the physical proximity of a substation. Thus, the attack could be delivered over-the-air without requiring to bypass any physical security mechanisms present in the vicinity of substation, nor enter the substation. Fig. 6 shows an example scenario of the system and attacker model where the GPS-spoofed PMU data from one target substation can contribute to incorrect control actions at the utility command center [85].
– **Optical observation:** The identification of embedded devices controlling critical smart grid units can lead to infiltration into the system and the communication infrastructure. For instance, the observation of exposed substation equipment can result in discovering the models of controllers, device configuration parameters and parts (e.g., accelerometer sensors, wireless interfaces), communication protocols, etc. Besides substation devices, geographically dispersed devices such as smart meters are publicly exposed. The tampering of these devices could lead to billing fraud or energy theft. Proximity to a system also allows "shoulder surfing" type of attacks, i.e., obtain information such as passwords and other confidential data by looking over the legitimate personnel (victim) shoulder [57]. Other direct optical data such as reading and decoding LED status indicators could also provide the basis of observation-based attacks [57, 58]. In addition to optically exposed systems, publicly available information could provide intelligence about control units and the implemented communication protocols which could be the baseline for identifying related vulnerabilities [59].
– **Side-channel analysis:** Similar to the interface access category, side-channel information allows extraction of crucial information about a system assuming only physical proximity to the equipment (e.g., optical signal attacks for industrial routers). Although the majority of side-channel attacks require close proximity to a sensor node (e.g., to measure the power consumption), some side-channels can be inferred from longer distances. For example, side-channel attacks can exploit wireless sensor networks utilizing the Radio Frequency (RF) channel to communicate [60]. Long-range microphone technologies (using reflected light such as laser or infrared beam to detect sound vibrations) eliminate the requirement of direct physical access to the device [61, 62]. Such side-channel techniques enable eavesdropping on personnel allowing longer distance transfer of system information.

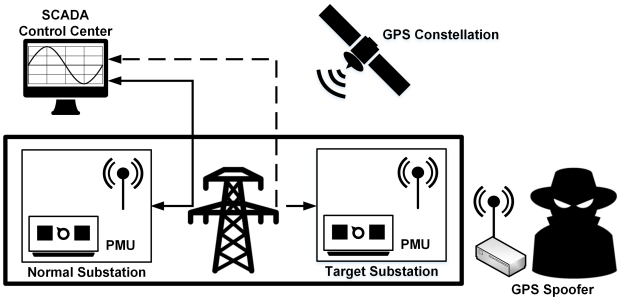


Fig. 6: GPS spoofing attack. Solid line represents PMU data collected with legitimate GPS satellites, dotted line represents PMU information collected with malicious GPS.

3.2.2 Network interface access

The communication and interaction of smart grid systems is achieved via the network layer. Due to the various entry points in the network, there is a large number of vulnerabilities stemming from the operation of the smart grid at this level. Such entry points include control networks and protocols that link the SCADA systems to lower-level control equipment. Firewalls and modems can also be listed as entry point candidates. In the scenario which the legitimate user or the adversary is able to interact with a smart grid device over a network, i.e., the distance between the user and the device does not have any physical bounds (***Zone 3***), information can still be extracted and used to mount cyber-attacks.

– **Replay attacks:** Industrial control traffic is often exchanged unencrypted due to real-time constraints. Assuming network interface access, the communication packets via a valid data transmission link can be repeated or delayed. Replay attacks intercept the data and re-transmit a desired process command into a protocol stream received by a smart grid hardware component [63, 64]. For instance, if an attacker (even with basic hacking skills and knowledge) captures the network traffic between the commands from master SCADA stations requesting tripping of relay controllers, then these packets can be replayed to perform the same trip task affecting both the device and the system operation. In cases which the transmitted traffic is in plain text, custom packets can be crafted to perform other tasks ultimately altering the behavior of the entire system. If the receiver in the communication path is an RTU, setpoint registers can be overwritten to falsify the measurements transferred to the system operation center [65, 86, 87].
– **Covert channels:** Hardware implementations can leak sensitive information over the network through timing and storage side-channels [66–68]. Timing channels require the sender to modulate the use of resources, such as the memory usage, over time in order to signal information that the receiver can observe and decode. For instance, it has been demonstrated that a remote attacker can successfully find key information of an OpenSSL webserver from non-constant execution time due to conditional branches in the algorithm [88]. The concept of storage channels includes writing certain object values which can be directly and/or indirectly read by the receiver.

4 Security for the smart grid

Comprehensive smart-grid protective mechanisms require defenses at all layers of abstraction. From the hardware to the process and the business level, protection must focus on security countermeasures against illegitimate users who aim to create significant safety issues to electricity customers and market participants as well as to operations and maintenance modules.

At the **policy level**, security standards provide the recommended strategy actions for protecting the grid against cyber and physical threats. The NIST-IR 7628 guidelines for smart grid cybersecurity provide a comprehensive overview for cybersecurity strategy practices, taking into account privacy and vulnerability classes [10]. The NERC-CIP set of requirements is designed to identify and protect all assets supporting the power system [83]. For instance, the CIP-005 standard requires the identification and protection of the electronic security perimeter(s) inside which all critical cyber-assets reside, as well as all access points on the perimeter. Furthermore, the International Society of Automation (ISA) has published the ISA99 (ANSI/ISA-62443) standards, recommended practices, and technical reports for implementing manufacturing and control systems securely. Several other reports exist in literature which provide the appropriate measures to meet smart grid security challenges [89–93].

Apart from security policies and standards, it is important to raise awareness regarding potential security risks and threats among involved parties such as engineers and manufacturers at the **business level**. Security awareness and training programs should be focused on helping employees realize that security issues are a shared responsibility. In recent years, security education has mostly focused on software assurance. However, hardware has become more vulnerable to breaches and requires appropriate attention. In addition to awareness, it is equally important that organizations involved in the grid infrastructure schedule regular security audits, acknowledge security issues, plan

for security attacks and outages, encourage secure operations and create security response teams, invest in training, and dedicate resources for better security.

The development of a secure grid environment must include mechanisms at the **engineering level** to defend against malicious adversaries at all layers of the infrastructure. In the **operation layer**, integration of energy and information technologies should contribute towards the resiliency of the system. As an example, the design of security-constrained economic dispatch and unit commitment operations must ensure that the power system is secure under consecutive loss of two components ($N-1-1$ criterion). In the **network layer**, strong authentication procedures must be adopted in order for the identity between communication parties to be verified. Furthermore, it is important to secure the communication link between grid elements without compromising performance. For instance, data exchange between utilities and smart meters must consider lightweight security and privacy preserving schemes. At the **software layer**, security controls must be adopted to minimize the exposure and propagation of malicious code and data. A typical mechanism is the deployment of control-flow integrity procedures enforcing the execution of a program to remain within the legitimate boundaries [94, 95].

All the aforementioned layers rely on the existing hardware components of the embedded device. Thus, protecting the **hardware layer** can provide a firm foundation to build security and trust for all the other layers. Hardware-assisted functionality can make systems more resilient and reduce recovery time in case of a malicious attack.

4.1 Hardware-assisted methodologies against cyber-attacks

We present an overview of the most common and recent hardware solutions used to secure modern embedded systems. As shown in Table 2, we categorize hardware-assisted methodologies into monitoring and protection solutions.

With regards to hardware-based security monitoring mechanisms, isolated rings and modes provide execution environments isolating supervisor processes from user processes. A prominent example is the Intel Software Guard Extensions (SGX), which are hardware features allowing execution of software in isolated mode (enclave) [96]. Similarly, ARM's TrustZone employs a normal and a secure virtual processor which both are backed by hardware-based access control in order to enhance isolation and enforce Digital Rights Management [97]. Hardware-assisted virtualization (HVM) is a platform virtualization approach that enables efficient embedding virtual machine software with hardware assistance. Despite the challenges related to developing HVM-based security solutions [98], HVM approaches typically instrument the hypervisor layer in root mode to collect information from non-root mode, and then send it to an external client. HVM can also contribute to restore a system to its previous state. This technology can assist during forensic investigation where a system needs to be restored to a pre-attack snapshot.

Similarly to the HVM operation abstraction, the System Management Mode (SMM) is a CPU operating mode which implements system control features such as power management and system hardware control. It offers a distinct and easily isolated processor environment: The system under monitoring executes in ordinary CPU modes (guest-analogous) and the SMM monitor (hypervisor-analogous) in SMM mode [99,100]. Furthermore, the Management Engine (ME) is a management mode in the form of microcontroller co-processor integrated in Intel chipsets and is part of the Intel's Active Management Technology (AMT) [101] [102]. The ME provides the necessary functionality for Boot Guard, SGX EPID provisioning and attestation services, remote corporate asset management, etc. Environments like ME are not an exclusivity of Intel: a similar solution is present in AMD processors, called Secure Processor [103].

Hardware Performance Counters (HPCs) are special-purpose registers and logic in the micro-architecture of processors. HPCs were initially designed as debugging tools for performance tuning and analysis: collecting information on processor events and the running processes. Despite the challenges of using HPCs for security applications, HPCs demonstrate a highly granular and low footprint method of detecting anomalous behavior [18, 104, 105]. In addition to leveraging special processor operating modes and purposely-developed hardware, security monitoring at the hardware layer can be achieved using specific hardware components such as GPUs (e.g., network intrusion detection [106]), PCI cards (e.g., PCI-based direct memory access) , and transactional memories [107]. Moreover, external hardware tools can monitor bus and memory data for real-time analysis and inspection [108, 109].

Protection mechanisms at the hardware layer could thwart adversaries from reverse engineering the hardware design. It is critical to protect hardware-based test interfaces and structures, e.g., disable/destroy JTAG access circuit scan chain pins. It is recommended to encrypt or at least obfuscate traffic to increase attack difficulty. Protection at the hardware layer can also be achieved via tamper-resistance approaches in both cy-

ber and physical level. Tamper-proof devices come in a variety of forms and capabilities. For example, steel housing can enhance the physical security of a system. Also, covering of the circuit and wires can protect from non-invasive type of attacks. Tamper-evidence ensures that there is visible evidence left behind when tampering occurs [110]. Tamper-detection sensors and circuitry could also assist in erasing sensitive parts of memory in case of intrusion. "Smart" cards for instance, can provide protection for cryptographic keys residing inside them. Light, frequency, temperature, voltage, and other types of sensors can also be utilized to detect attempts to access the hardware of a device.

The prevention of "compromising side-channel information" is an important requirement for secure hardware. Shielding using Faraday-cage housing for ICs can be effective in blocking external signals and thus prevent electromagnetic-based emanations and side-channel attacks. In addition, extra hardware components such as cryptographic chips and secure memory devices (e.g., Dallas Semiconductor DS2432 EEPROM, Atmel CryptoMemory family of devices, KeeLoq, Mifare, etc.) can also be used to provide hardware-based trust. For example, the functionality of TPM can assist in verifying software integrity via remote attestation as well as data binding (data to be encrypted using a secret key that can be migrated), and sealing to a certain TPM and configuration [111].

Moreover, asynchronous designs [112], dynamic and differential logic [113], dual-rail with pre-charge logic [114], integration of dummy gates at the layout-level [115], or even having gates with power consumption independent of the input values (to reduce the information provided by the measurement values) could thwart an adversary from attacking the hardware design. Besides adding dummy gates, it has been shown that camouflaging can be strengthen without much overhead by judiciously selecting the gates in the design to camouflage [116]. Additionally, the number of layers per chip and manufacturing in smaller technologies can prevent access and manipulation of chips.

5 Conclusions

In this survey paper, we emphasized the importance of quantifying and analyzing intelligence extracted from the hardware of smart grid devices. We have examined ways to collect and utilize the information based on the access level to the hardware components and the capabilities of the attackers. We also highlighted solutions and effective methods towards enhancing the security of embedded devices utilized in power system applications. The robustness and resiliency of embedded devices, and hence the security of smart grid implementations, starts with developing and incorporating monitoring and protection mechanisms at the hardware layer.

Table 2: Monitoring and Protection Solutions at the Hardware Layer.

Layer	Vulnerabilities & Threats
Monitoring	• Isolated Rings • Hardware Virtual Machines • System Management Mode • Management Engine and Secure Processor • Hardware Performance Counters • Hardware Components • External Monitoring Hardware
Protection	• Interfaces • Tamper Mechanisms: Resistance, Evidence, Detection • Side-Channel Emissions • Circuit Board Design and Routing • Hardware Components

References

1. Electric Power Research Institute (EPRI). Security architecture methodology for the electric sector, version 2.0. [Online]: `https://www.epri.com/#/pages/product/000000003002007887/`, 2016.
2. R. Leszczyna, E. Egozcue, L. Tarrafeta, V. F. Villar, R. Estremera, and J. Alonso. Protecting industrial control systems-recommendations for europe and member states. Technical report, Technical report, European Union Agency for Network and Information Security (ENISA), 2011.
3. D. Beresford. The sauce of utter pwnage. [Online]: `http://thesauceofutterpwnage.blogspot.com/`, 2011.
4. S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5):1039–1057, 2016.
5. Bloomberg Businessweek. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies). [Online]: `https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies`, 2018.
6. R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor. Trustworthy hardware: Identifying and classifying hardware trojans. *Computer*, 43(10):39–46, 2010.
7. C. Konstantinou, A. Keliris, and M. Maniatakos. Taxonomy of firmware trojans in smart grid devices. In *Power and Energy Society General Meeting (PESGM), 2016*, pages 1–5. IEEE, 2016.
8. R. Lee, M. Assante, and T. Conway. Analysis of the cyber attack on the ukrainian power grid. *SANS Industrial Control Systems*, 2016.
9. SANS Industrial Control Systems Security Blog. How do you say Ground Hog Day in Ukrainian? [Online]: `https://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian`, 2016.
10. NIST, US. Guidelines for smart grid cyber security. *NIST IR-7628, Aug*, 1-3, 2010.

11. C. Konstantinou and M. Maniatakos. A case study on implementing false data injection attacks against nonlinear state estimation. In *Proceedings of the 2Nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, CPS-SPC '16, pages 81–92, New York, NY, USA, 2016. ACM.
12. ICS-CERT, U.S. DHS. [Online]: `https://ics-cert.us-cert.gov/`, 2016.
13. J. Grand. Advanced hardware hacking techniques. *DEFCON*, 12:59, 2004.
14. Y. Han, S. Etigowni, H. Liu, S. Zonouz, and A. Petropulu. Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1095–1108. ACM, 2017.
15. United States Army. Army Nuclear Power Program (ANPP). [Online]: `https://en.wikipedia.org/wiki/Army_Nuclear_Power_Program`, 2018.
16. Defense Information Systems Agency. Department of Defense Information Network - Approved Products List). [Online]: `http://www.disa.mil/network-services/ucco`, 2018.
17. C. Konstantinou and M. Maniatakos. Impact of firmware modification attacks on power systems field devices. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 283–288. IEEE, 2015.
18. X. Wang, C. Konstantinou, M. Maniatakos, and R. Karri. Confirm: Detecting firmware modifications in embedded systems using hardware performance counters. In *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, pages 544–551. IEEE Press, 2015.
19. M. Vuagnoux and S. Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In *USENIX security symposium*, pages 1–16, 2009.
20. N. Tsoutsos and M. Maniatakos. Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation. *IEEE Transactions on Emerging Topics in Computing*, 2(1):81–93, 2014.
21. Schweitzer Engineering Laboratories. SEL-3355, Rack-Mount Rugged Computer). [Online]: `https://selinc.com/products/3355/`, 2018.
22. R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen. Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 19(2):105–120, 2014.
23. A. Shawkat. Smart grids: opportunities, developments and trends. *Smart Meter*, pages 109–133, 2013.
24. R. Anderson, C. Barton, R. Böhme, R. Clayton, Michel JG Van E., M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In *The economics of information security and privacy*, pages 265–300. Springer, 2013.
25. D. G. Abraham, G. M. Dolan, G. P. Double, and J. V. Stevens. Transaction security system. *IBM Systems Journal*, 30(2):206–229, 1991.
26. X. Liu, Z. Peidong, Z. Yan, and C. Kan. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *Smart Grid, IEEE Transactions on*, 6(5):2435–2443, 2015.
27. C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert. Breaking and entering through the silicon. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 733–744. ACM, 2013.
28. R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In *Security protocols*, pages 125–136. Springer, 1998.
29. S. Skorobogatov. *Semi-invasive attacks: a new approach to hardware security analysis*. PhD thesis, Citeseer, 2005.
30. P. Tuyls, G.-J. Schrijen, B. Škorić, J. Van Geloven, N. Verhaegh, and R. Wolters. Read-proof hardware from protective coatings. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 369–383. Springer, 2006.
31. X. Ma, DG Yang, and GQ Zhang. Decapsulation methods for cu interconnection packages. In *Electronic Packaging Technology and High Density Packaging (ICEPT-HDP), 2012 13th International Conference on*, pages 1387–1391. IEEE, 2012.
32. t4f. Ultra-low cost ic decapsulation. [Online]: `http://www.t4f.org/articles/ultra-low-cost-ic-decapsulation/`, 2018.
33. C. Taylor. The Common Methods of Hardware Hacking. [Online]: `https://www.sparkfun.com/news/1314`, 2013.
34. MWR Labs. Hacking Embedded Devices: UART Consoles. [Online]: `https://labs.mwrinfosecurity.com/blog/hacking-embedded-devices-uart-consoles/`, 2012.
35. J. Grand. Jtagulator: assisted discovery of on-chip debug interfaces. In *21st DefCon Conference, Las Vegas*, pages 1–88, 2013.
36. C. Heffner. Reverse Engineering Serial Ports. [Online]: `http://www.devttys0.com/2012/11/reverse-engineering-serial-ports/`, 2012.
37. A. Huang. bunnie's adventures hacking the Xbox). [Online]: `http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html`, 2013.
38. M. Breeuwsma, M. De Jongh, C. Klaver, R. Van Der Knijff, and M. Roeloffs. Forensic data recovery from flash memory. *Small Scale Digital Device Forensics Journal*, 1(1):1–17, 2007.
39. A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, 2012.
40. S. Govindavajhala and A. W Appel. Using memory errors to attack a virtual machine. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pages 154–165. IEEE, 2003.
41. J.-M. Schmidt and M. Hutter. *Optical and em fault-attacks on crt-based rsa: Concrete results*. na, 2007.
42. J.-M. Schmidt, M. Hutter, and T. Plos. Optical fault attacks on aes: A threat in violet. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 13–22. IEEE, 2009.
43. T. Le, C. Canovas, and J. Clédiere. An overview of side channel analysis attacks. In *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pages 33–43. ACM, 2008.
44. P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Advances in cryptology-CRYPTO99*, pages 789–789. Springer, 1999.
45. J. Grand. Hardware is the new software. *presentation at Hack In The Box Security Conference (HITBSecConf)*, 2009.
46. bunnie & xobs. The Exploration and Exploitation of an SD Memory Card. [Online]: `http://bunniefoo.com/bunnie/sdcard-30c3-pub.pdf`, 2013.

47. K. Kingpin and M. Mudge. Security analysis of the palm operating system and its weaknesses against malicious code threats. In *Proceedings of the 10th conference on USENIX Security Symposium-Volume 10*, page 11, 2001.
48. A. John. Vulnerability assessment of the transportation infrastructure relying on the global positioning system. *Volpe National Transportation Systems Center, Technical Report*, 2001.
49. T. E Humphreys, B. M Ledvina, M. L Psiaki, B. W O'Hanlon, and P. M Kintner. Assessing the spoofing threat: Development of a portable gps civilian spoofer. In *Radionavigation Laboratory Conference Proceedings*, 2008.
50. T. Humphreys. Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. *University of Texas at Austin*, 2012.
51. J. Bhatti and T. Humphreys. Hostile control of ships via false GPS signals: Demonstration and detection. *Navigation*, 2016.
52. D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren. A survey and analysis of the gnss spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)*, 48(4):64, 2016.
53. J.-A. Jiang, J.-Z. Yang, Y.-H. Lin, C.-W. Liu, and J.-C. Ma. An adaptive pmu based fault detection/location technique for transmission lines. i. theory and algorithms. *IEEE Transactions on Power Delivery*, 15(2):486–493, 2000.
54. X. Jiang, J. Zhang, B. J Harding, J. J Makela, and A. D Domı. Spoofing gps receiver clock offset of phasor measurement units. *IEEE Transactions on Power Systems*, 28(3):3253–3262, 2013.
55. Z. Zhang, S. Gong, A. D Dimitrovski, and H. Li. Time synchronization attack in smart grid: Impact and analysis. *IEEE Transactions on Smart Grid*, 4(1):87–98, 2013.
56. C. Konstantinou, M. Sazos, A. S Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos. Gps spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment. *IET Cyber-Physical Systems: Theory & Applications*, 2(4):180–187, 2017.
57. J. Loughry and D. Umphress. Information leakage from optical emanations. *ACM Transactions on Information and System Security (TISSEC)*, 5(3):262–289, 2002.
58. M. Kuhn. Optical time-domain eavesdropping risks of crt displays. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, pages 3–18, 2002.
59. C. Konstantinou, M. Sazos, and M. Maniatakos. Attacking the smart grid using public information. In *Test Symposium (LATS), 2016 17th Latin-American*, pages 105–110. IEEE, 2016.
60. V. Subramanian. *Proximity-based attacks in wireless sensor networks*. PhD thesis, Georgia Institute of Technology, 2013.
61. B. Galeyev. Special section: Leon theremin, pioneer of electronic art. *Leonardo Music Journal, MIT, USA*, 1996.
62. A. Glinsky. *Theremin: ether music and espionage*. University of Illinois Press, 2000.
63. Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 911–918. IEEE, 2009.
64. F. Pasqualetti, F. Dörfler, and F. Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pages 2195–2201. IEEE, 2011.
65. S. Pan, T. Morris, and U. Adhikari. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid*, 6(6):3104–3113, 2015.
66. C. Alcaraz, R. Roman, P. Najera, and J. Lopez. Security of industrial sensor network-based remote substations in the context of the internet of things. *Ad Hoc Networks*, 11(3):1091–1104, 2013.
67. S. Zander, G. Armitage, and P. Branch. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys & Tutorials*, 9(3):44–57, 2007.
68. S. Cabuk. *Network covert channels: Design, analysis, detection, and elimination*. Purdue University, 2006.
69. I. Moskowitz and M. Kang. Covert channels-here to stay? In *Computer Assurance-COMPASS'94 Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security. Proceedings of the 9th Annual Conference on*, pages 235–243. IEEE, 1994.
70. P. Parfomak. Physical security of the us power grid: high-voltage transformer substations. *Congressional Research Service*, 2014.
71. Foreign Policy. 'Military-Style' Raid on California Power Station Spooks U.S.). [Online]: `http://foreignpolicy.com/2013/12/27/military-style-raid-on-california-power-station-spooks-u-s/`, 2013.
72. ICS-CERT, U.S. DHS. KACO HMI Hard-coded Password. [Online]: `https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-224-01`, 2016.
73. ICS-CERT, U.S. DHS. Moxa NPort Device Vulnerabilities. [Online]: `https://ics-cert.us-cert.gov/advisories/ICSA-16-336-02`, 2017.
74. IEEE. IEEE Standard for Test Access Port and Boundary-Scan Architecture. *IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001)*, pages 1–444, May 2013.
75. MF Breeuwsma. Forensic imaging of embedded systems using jtag (boundary-scan). *digital investigation*, 3(1):32–42, 2006.
76. R. Russell. *Hack proofing your network*. Syngress, 2000.
77. J. Grand. Understanding hardware security. *Black Hat Japan*, 2004.
78. T. Caddy. *Tamper Detection*, pages 1277–1277. Springer US, Boston, MA, 2011.
79. J. Zaddach and A. Costin. Embedded devices security and firmware reverse engineering. *Black-Hat USA*, 2013.
80. P. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Advances in Cryptology-CRYPTO'96*, pages 104–113, 1996.
81. S. Sze. *Physics and Technology*. Wiley, New York, 1985.
82. M. Gjendemsjø. *Creating a Weapon of Mass Disruption: Attacking Programmable Logic Controllers*. Institutt for datateknikk og informasjonsvitenskap, 2013.
83. North american electric reliability corporation (NERC). NERC-CIP, Critical Infrastructure Protection, 2018.
84. North American Electric Reliability Corporation (NERC). Extended loss of GPS Impact on Reliability, 2012.
85. E. Martínez, N. Juárez, A. Guzmán, G. Zweigle, and J. León. Using synchronized phasor angle difference for wide-area protection and control. In *proceedings of*

the 33rd Annual Western Protective Relay Conference, Spokane, WA, 2006.
86. A. Keliris, C. Konstantinou, and M. Maniatakos. White Paper: GE Multilin SR Protective Relays Passcode Vulnerability. [Online]: `https://www.blackhat.com/docs/us-17/thursday/us-17-Keliris-And-Then-The-Script-Kiddie-Said-Let-There-Be-No-Light-Are-Cyberattacks-On-The-Power-Grid-Limited-To-Nation-State-Actors-wp.pdf`, 2017.
87. C. Konstantinou, M. Sazos, and M. Maniatakos. FLEP-SGS^2: a Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security. In *Innovative Smart Grid Technologies (ISGT), 2019 IEEE PES*, pages 1–5. IEEE, 2019.
88. D. Brumley and D. Boneh. Remote timing attacks are practical. *Computer Networks*, 48(5):701–716, 2005.
89. Executive Office of the President of the U.S. A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future, 2011.
90. M. Swanson. *Security self-assessment guide for information technology system*, volume 800. US Department of Commerce, Computer Security Division, Information Technology, National Institute of Standards and Technology, 2001.
91. United States Government Accountability Office. GAO-11-117, Electric Grid Modernization, 2011.
92. MIT. The Future of the Electric Grid, 2011.
93. ICS-CERT. Cross-Sector Roadmap for Cybersecurity of Control Systems, 2011.
94. M. Abadi, B. Mihai, E. Ulfar, and L. Jay. Control-flow integrity. In *Proceedings of the 12th ACM conference on Computer and communications security*, pages 340–353, 2005.
95. L. Davi, A. Dmitrienko, M. Egele, T. Fischer, T. Holz, R. Hund, S. Nürnberger, and A.-R. Sadeghi. Mocfi: A framework to mitigate control-flow attacks on smartphones. In *NDSS*, volume 26, pages 27–40, 2012.
96. V. Costan and S. Devadas. Intel sgx explained. *IACR Cryptology ePrint Archive*, 2016:86, 2016.
97. T. Alves and D. Felton. Trustzone: Integrated hardware and software security. *ARM white paper*, 3(4):18–24, 2004.
98. F. Zhang and H. Zhang. Sok: A study of using hardware-assisted isolated execution environments for security. In *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*, page 3. ACM, 2016.
99. Coreboot. [Online]: `http://www.coreboot.org/`, 2015.
100. Seabios. [Online]: `http://www.seabios.org/SeaBIOS`, 2015.
101. Intel. Intel Active Management Technology. [Online]: `https://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html`, 2008.
102. Intel. Intel AMT and the Intel ME. [Online]: `https://software.intel.com/en-us/blogs/2011/12/14/intelr-amt-and-the-intelr-me`, 2016.
103. AMD. AMD Secure Technology. [Online]: `https://www.amd.com/en/technologies/security`, 2013.
104. X. Wang, C. Konstantinou, M. Maniatakos, R. Karri, S. Lee, P. Robison, P. Stergiou, and S. Kim. Malicious firmware detection with hardware performance counters. *IEEE Transactions on Multi-Scale Computing Systems*, 2(3):160–173, 2016.
105. N. Patel, A. Sasan, and H. Homayoun. Analyzing hardware based malware detectors. In *Proceedings of the 54th Annual Design Automation Conference 2017*, page 25. ACM, 2017.
106. G. Vasiliadis, S. Antonatos, M. Polychronakis, E. P Markatos, and S. Ioannidis. Gnort: High performance network intrusion detection using graphics processors. In *International Workshop on Recent Advances in Intrusion Detection*, pages 116–134. Springer, 2008.
107. R. M Yoo, C. J Hughes, K. Lai, and R. Rajwar. Performance evaluation of intel® transactional synchronization extensions for high-performance computing. In *Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis*, page 19. ACM, 2013.
108. C. Konstantinou, E. Chielle, and M. Maniatakos. Phylax: Snapshot-based profiling of real-time embedded devices via jtag interface. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2018*, pages 869–872. IEEE, 2018.
109. M. El Shobaki. On-chip monitoring of single-and multiprocessor hardware real-time operating systems. In *Proceedings of the 8th international conference on real-time computing systems and applications (RTCSA)*, 2002.
110. S. H Weingart. Physical security devices for computer subsystems: A survey of attacks and defenses. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 302–317. Springer, 2000.
111. J. Osborn and D. Challener. Trusted platform module evolution. *Johns Hopkins APL technical digest*, 32(2):536, 2013.
112. S. Moore, R. Anderson, R. Mullins, G. Taylor, and J. JA Fournier. Balanced self-checking asynchronous logic for smart card applications. *Microprocessors and Microsystems*, 27(9):421–430, 2003.
113. K. Tiri, M. Akmal, and I. Verbauwhede. A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Solid-State Circuits Conference, 2002. ESSCIRC 2002. Proceedings of the 28th European*, pages 403–406. IEEE, 2002.
114. M. Stanojlović and P. Petković. Strategies against side-channel-attack. In *Proceedings of the Small Systems Simulation Symposium*, pages 86–89, 2010.
115. J. Lee, M. Tebranipoor, and J. Plusquellic. A low-cost solution for protecting ips against scan-based side-channel attacks. In *VLSI Test Symposium, 2006. Proceedings. 24th IEEE*, page 6. IEEE, 2006.
116. J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 709–720. ACM, 2013.