Implications of Physical Fault Injections on Single Chip Motes

Sara Faour, Mališa Vučinić, Filip Maksimovic, David Burnett, Paul Mühlethaler, Thomas Watteyne, Kristofer Pister

Implications of Physical Fault Injections on Single Chip Motes

Sara Faour*, Mališa Vučinić*, Filip Maksimovic*, David Burnett†, Paul Muhlethaler*
Thomas Watteyne*, Kristofer Pister‡

*Inria, Paris
†Portland State University
‡University of California, Berkeley
e-mail: first.last@inria.fr*, dburnett@pdx.edu†, ksjp@berkeley.edu‡

***Abstract*—Single-chip motes are wireless sensor nodes that integrate computation, communication, power and sensing on a single chip. We consider the security threats these novel devices are subject to when employed in safety-critical applications. Fault injection attacks are a prominent form of physical attacks that pose a threat to the normal and secure functioning of targeted devices, potentially compromising their intended behavior. These attacks have been studied mainly on commercial off-the-shelf devices which rely on external components such as crystal oscillators and passives. Such external components are absent from single-chip motes, resulting in a uniquely different attack surface compared to commercial systems. In this paper, we first survey the features of the common fault injection methods, and then study and compare their implications on single-chip motes.**

***Index Terms*—Single chip mote, fault injection attacks, crystal-free, hardware security.**

I. Introduction

Advances in wireless communication have been a major factor in allowing the development of large networks of sensors. These networks are used for environmental monitoring, security and surveillance, healthcare and smart buildings [1]. The size and cost of the wireless sensor nodes, or **motes**, are critical factors due to their intended use in diverse settings. A lower cost makes it feasible to deploy large networks enabling extensive data collection, and a smaller size would allow the motes to be discreetly placed in areas where traditional sensors would be impractical or impossible to deploy. For example, they can be injected in the body through a syringe for therapeutic reasons [2].

The "Smart Dust" project [3] proposed in 1997 aimed at realizing a cheap and low-power mote on a micro scale. Ever since, we could observe a proliferation of commercial-off-the-shelf (COTS) motes, used in applications from passive monitoring to real-time control. One thing in common for all COTS motes is their need for a printed circuit board (PCB) to assemble them with other components like the crystal oscillator and the radio. Research projects involving low-power motes often prioritize the integration of commercial hardware onto compact PCBs rather than exploring novel embedded architectures for low-power applications [4].

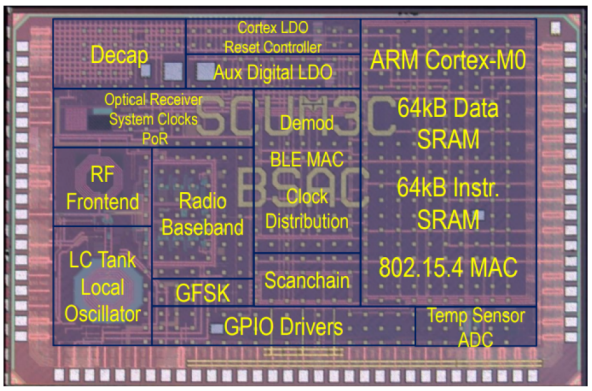

Fig. 1. Annotated die photo of the Single Chip Mote version SCμM-3C.

The advancement of the fabrication technology in the last few decades enabled decreasing the size of integrated circuits (ICs) and even eliminating the need for the assembly of individual components on a PCB. This allows the direct fabrication of complex structures in a continuous manner by integrating multiple manufacturing steps into a single continuous process. The technology unlocks the potential for miniaturization, enabling the development of compact, yet high-performance motes.

One attempt in full integration avoiding the use of a PCB is the Michigan Micro Mote, a 1 mm^3 general-purpose sensor node platform designed with five stacked IC dies, fabricated in three different technologies [5], with wireless communication, battery, power management, solar harvesting, processor and memory. One downside to this design is the increased complexity when manufacturing, aligning, and bonding the different dies.

Another attempt in full integration is the Single Chip Mote project, which aims at developing a complete self-contained mote on a single chip, including sensing, computation, communication, and power, with no external components. The project is still a work in progress: the current version shown in Fig. 1 is a $2 \times 3 \times 0.3$ mm^3, 4.2 mg chip fabricated in 65nm CMOS process. It contains an integrated crystal-free 802.15.4-compatible radio transceiver, Bluetooth Low Energy (BLE) beacon transmitter, external sensor interface, contactless

optical bootloader, and Cortex-M0 microprocessor with 64 kB each of program and data SRAM [6]. The mote is small, lightweight, and has minimal external components. It requires only three wires: power, ground, and a bondwire antenna.

Given these two successful attempts, the "Smart Dust" vision starts to be a reality. However, transitioning to massive networks of single chip motes requires a careful study of the security threats that these motes are vulnerable to. Single chip motes have a novel embedded architecture presenting many differences compared to board-based systems. Thus, the level of threats that these chips are subject to may also differ.

To the best of our knowledge, physical security of smart dust and single-chip motes has not been explored previously. The goal of this paper is to present a preliminary study of the security implications on single chip motes compared to board-based systems, when an attacker has physical access to the target. Fault attacks are the noticeable type of physical attacks, in which the normal behavior of the system is affected due to fault injections. In this study, we generalize our conclusions to both today's and future classes of single chip motes.

The contributions of this article are twofold:

1) We survey different fault injection techniques from the state-of-the-art.
2) We analyze, for the first time, how single chip systems may have different responses to a variety of fault injection techniques compared to a board-based system, from an attacker point of view.

The remaining of this article is organized as follows. Section II describes the main points that distinguish single chip motes from board-based systems. Section III surveys the commonly used fault-injection-based attacks and evaluates the single chip mote architecture against each of these attack techniques. Section IV concludes this work.

II. Single Chip Motes: A Primer

Single-chip mote design is different from board-based systems. Two important points of difference are: the absence of external components such as crystal oscillators for timing, and the need to fabricate these chips using a single fabrication process imposing some constraints on the type of memory that may be included in the design.

A. Crystal-free timing

Crystal oscillator is an electronic oscillator circuit incorporating, typically, a piezoelectric resonator: the crystal. The most common type of resonator used is made from quartz crystal and cut to minimize sensitivity to temperature at the temperature of interest. When a voltage source is applied to a small thin piece of quartz crystal, it begins to change shape due to the piezoelectric effect. This piezoelectric effect is the property of any material by which an electrical charge produces a shape change and vice versa: a mechanical force applied to the crystal produces an electrical charge. When included as part of a circuit including feedback and a mechanism to replenish energy lost to heat each cycle, an oscillator is formed. The quality factor of the crystal describes, e.g., how narrow a range of frequencies it will resonate at and translates into the purity and stability of the frequency produced by the oscillator.

The resonant frequency of the crystal depends on its size, shape, elasticity, and the speed of sound in the material. Due to their highly stable mechanical resonance and fabrication along particular crystallographic faces, crystals maintain their frequency with high stability over temperature and supply variations. The stability of an oscillator is quantified by its drift, typically measured in parts per million (ppm). Typically, crystal oscillators' stability is in the 10-30 ppm range for regular crystals, even down to 2-3 ppm or better for temperature-compensated versions [9] that incorporate mechanisms to measure the temperature and apply a correction factor to the output. Typical wireless standards are written such that they can be satisfied using frequency sources based on crystal oscillators. As such, crystal-based systems can easily satisfy the maximum frequency drift requirements required by the different standards for wireless communication, such as BLE (typically $\pm$20 ppm to $\pm$50 ppm), or IEEE 802.15.4 ($\pm$40 ppm).

Although crystal oscillators have become cheaper and smaller and offer better performance, their main drawback remains that they are inherently external ("off-chip") components: using them requires special fabrication and packaging steps, and process integration beyond the steps required to produce the core CMOS chip.

There is a growing trend towards adopting MEMS oscillators as an alternative to crystals. MEMS oscillators are complex, silicon-based structures often with a temperature sensor and compensation circuitry [10]. A silicon resonator is used in lieu of a quartz crystal resonator, again with high quality factor and incorporated into a feedback circuit, such as the BAW resonators [11]. Similarly to crystal oscillators, these oscillators are "off-chip" external components.

We define a true single-chip "crystal-free" mote design as a solution that eliminates the need for external electronic components, including a crystal or other oscillators. Eliminating off-chip oscillators means any oscillators must be integrated alongside the rest of the circuits of the CMOS IE. These "on-chip" oscillators reduce overall system footprint and, with careful design to incorporate power source and antenna, can eliminate the need for a printed circuit board (PCB) altogether.

On-chip oscillators are composed of integrated components available in standard CMOS processes like resistors, capacitors, inductors, transistors and logic gates. As such, these components do not require any special fabrication and packaging steps during the fabrication of the circuits they are embedded alongside.

On-chip oscillator center frequency and stability are much more susceptible to thermal and flicker noise, process, voltage and temperature variations compared to crystal oscillators. Process variations are caused by changes in manufacturing conditions such as temperature, pressure, deposition and etch rates, and dopant concentration gradients. For this reason, real-world examples of single-chip crystal-free radios [12] show that the on-chip oscillators have 10,000+ ppm frequency

Table 1. Summary of FIAs on board-based systems according to [7], [8], and on single chip motes according to our work. Gray color highlights the differing criteria.

Technique	Invasiveness		Precision (space)		Precision (time)		Technical skill		Cost	
Clock glitch	non-invasive	invasive	low	complete	high	high	moderate	very high	low	very high
Underfeeding*	non-invasive	invasive	high	complete	none	none	low	very high	low	very high
Voltage spike*	non-invasive	invasive	low	complete	moderate	moderate	moderate	very high	low	very high
EM pulse	non-invasive	non-invasive	moderate	moderate	moderate	moderate	moderate	moderate	moderate	moderate
Heat*	non-invasive	non-invasive	low	low	none	none	low	low	low	low
Light radiation	semi-invasive	semi-invasive	low	low	low	low	moderate	moderate	low	low
Light pulse	semi-invasive	semi-invasive	moderate	moderate	moderate	moderate	moderate	moderate	moderate	moderate
Laser beam	semi-invasive	semi-invasive	high	high	high	high	high	high	high	high
FIB	invasive	invasive	complete	complete	very high	very high	very high	very high	very high	very high
HIM	invasive	invasive	complete	complete	very high	very high	high	high	very high	very high

EM: Electromagnetic, FIB: Focused ion beam, HIM: Heavy-ion micro-beam.
* Internal oscillators of single chip motes are less stable than crystal oscillators when the supply voltage or the temperature change.

error off their nominal value depending on time scale [13]. This is to be compared with 10-30 ppm of drift for crystal oscillators. When the internal oscillators change in response to temperature and voltage, intermittent wireless communication will provide a means for the mote to recalibrate its oscillators as long as the change is slow enough. If the change is fast, the mote will lose wireless contact and need to re-join the network.

B. Non-volatile memory constraints

Non-volatile memory is a type of memory that can store data without the need for a continuous power supply. We distinguish between two main categories of non-volatile memory: 1) non-writable non-volatile memory, e.g. Read-Only Memory (ROM) and One-Time Programmable (OTP) memory; 2) writable non-volatile memory, e.g. flash memory and Electrically Erasable Programmable Read-Only Memory (EEPROM).

Non-writable non-volatile memory can be programmed once and is typically used to store the boot code and unique device identifiers or keys. This memory is often generated using a memory compiler that takes the ROM data as input and produces a transistor layout as output. The "compiled" memory consists only of transistors and metal available in the CMOS process being used, so fabrication of this memory is naturally compatible with the process used for fabricating the rest of the chip. Therefore, this type of memory can be included in system design of single chip motes.

Writable non-volatile memories allow both read and write operations and are typically used to store and update program data. However, they typically require specialized fabrication processes and steps that must be supported in a given CMOS process. Many CMOS processes do not include options for non-volatile memories. The specific fabrication requirements vary depending on the type of non-volatile memory technology. For example, the fabrication of flash memory involves additional steps to create the floating gate structures and the necessary insulation layers. Hence, current single-chip motes do not include writable non-volatile storage, so every time that power is removed from the chip, both the program and data stored in SRAM are lost.

III. Fault Injection Attacks (FIA)

The goal of Fault Injection Attacks (FIAs) is to inject faults into the system hardware. A fault is usually accomplished by manipulating either environmental parameters or inputs, causing the software to behave abnormally. These attacks have been used to manipulate the system behavior, such as to corrupt memory contents or to coerce microprocessors into misinterpreting and skipping program instructions. The attacker exploits this altered behavior for a variety of malicious purposes: they may be able to extract secret keys and bypass critical security protections, such as authentication checks. The attack techniques include altering the power supply voltage or the clock signal, disturbing the device using radiation or electromagnetic pulses, overheating it or exposing it to intense light or ion beams. We discuss the following attacks based on the common categorization depending on 1) cost; 2) invasiveness; 3) transiency; 4) precision:

- **Cost.** Similarly to Barenghi *et al.* [7], we consider as *low cost* the injection techniques that require equipment costing less than 3000 USD, and as *high cost* otherwise. It is important to know that we refer to the equipment cost as the cost needed to buy the equipment. However, using the equipment may be available as a service. For example having a Focused Ion Beam Station (FIB) station is very expensive (100 000+ USD), but for a few hundred dollars per hour an attacker can have a trained technician to perform his task.
- **Invasiveness.** If an attack involves significant alteration of the system, whether during the attack preparation or execution, we consider it as *invasive*. Relevant preparation techniques include depackaging the chip and removing any protective layers (decapsulation) to directly induce faults into its internal components. These processes risk irreparable damage or destruction of the target under evaluation. *Non-invasive* FIAs require little-to-no tampering of the system. They can be accomplished by utilizing pin-probing or bus-snooping for example, without damaging the package. *Semi-invasive* FIAs require depackaging the chip to get access to the chip surface. However, semi-invasive methods do not require electrical contact to the metal surface, so the passivation layer of the chip remains intact and no mechanical damage to the silicon is caused.
- **Transiency.** We consider errors that can be rectified by resetting the system or stopping the source of the fault as *transient faults*. In contrast, *permanent faults* alter the

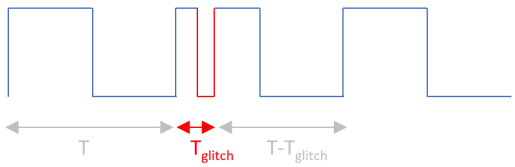

Fig. 2. Using an FIA to introduce an additional positive clock edge.

state of targeted components, and their impacts persist even after device restarts and resets.

- **Precision.** *Spatial precision* refers to the level of accuracy with which the fault generator can inject a fault into a specific location of the system. *Temporal precision* is defined as the accuracy of the fault injection process in inducing a fault at a specific time.

We also identify the degree of technical skill and knowledge of the implementation required to perform the injection. Table. 1 summarizes the important characteristics of the fault injection techniques from the state-of-the-art described in the next section, and highlights the limitations and the improvements imposed by applying these attacks on single chip motes compared to board-based systems.

A. Clock Glitching

Definition. Clock glitches tamper with the system clock signal to induce hardware synchronization issues. To inject a clock glitch, it is possible to shorten the length of a single cycle through the introduction of additional edges to the clock signal, see Fig. 2. This shorter cycle is likely to violate setup time, hold time, and/or timing closure constraints of components in the digital system to which the clock is supplied.

Attacker objectives. Shortening the length of a single cycle can trigger instruction misses caused by forcing the execution of an instruction before the CPU has completed the previous one. A short cycle can also cause data misreads by attempting to read values before the memory has latched out the request. These errors are transient and thus such faults can be induced without leaving any tamper evidence.

Setup. To alter the clock signal, the attacker needs to have direct control over the clock line by connecting an external clock source. This is easily achieved for a system using an external clock generator, i.e., a crystal oscillator. In some devices, clock glitching can also be achieved purely in software by controlling the energy management regulators [14].

The clock alteration techniques are required to supply a regular clock within the working range of the system, while preserving the ability of altering a single clock edge. This implies that the equipment inducing the alteration must be working at a higher clock frequency than the attacked system, and this is inherently more difficult as the target system working frequency increases. Clock glitches are generally considered to be a simple fault injection method: the target devices are easy to operate with, and no familiarity with the device implementation specifics is required. They can be achieved without any special and expensive tools, i.e., using low-end field-programmable gate array (FPGA) boards, e.g., at a price of 130 USD [15].

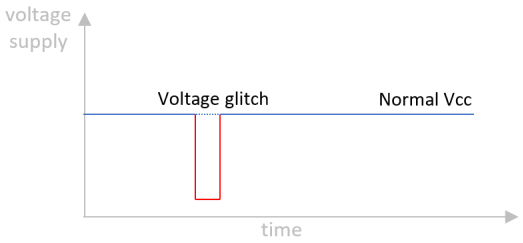

Fig. 3. Voltage FIA.

Implications on single chip mote. A single chip mote, with its "crystal-free" architecture, uses internal oscillators as frequency and clock reference for the system. To introduce a clock glitch on a single chip mote, instead of accessing the clock line trace printed on the PCB, sometimes seen using naked eye, we need to access a micro scale trace interconnecting the on-chip clock circuit and the other circuits of the chip. The attacker has to deal with a different dimension: it is not feasible to introduce a clock glitch while maintaining the same level of setup simplicity described earlier. To launch this attack, the attacker needs to be able to create tiny channels or access points on the chip surface through which a probing wire can be attached or connected. This setup involves a much more advanced, expensive and spatially precise tool, known as focused ion beam (FIB) and described in Section III-F. In this attack, the temporal precision of the clock glitches is determined by the clock injection source. Moreover, additional steps to decapsulate the chip and remove any protective layer is necessary, leading to an invasive attack.

B. Voltage Glitching

Definition. Voltage glitches manipulate the supply voltage, causing a faulty behavior in the system. The attacker attempts either to feed the system with a power supply below the considered nominal value (underfeeding) for a certain period, or to create well-timed power spikes into the supply line of the circuit, see Fig. 3.

Attacker objectives. By under-powering the system, the attacker can cause some delays in the correct setup of the logic gates of the circuit, hence resulting in erroneous output. This method affects the running software continuously and might cause faults throughout the computation. To be able to perform more sophisticated attacks, the attacker needs to be able to precisely time the power spike. The injection of precise power spikes can corrupt the contents of memory units or disrupt microprocessors leading to misinterpret and even skip program instructions. These glitches modify the state of latches of flip-flops, influencing the control and data path logic of the circuit [16].For example, if the voltage spike happens during memory reading, wrong data may be retrieved. Precisely timed spikes were also used to skip security-critical checks, e.g. digital signature verification, bypass system-level access control features, and to recover information about cryptographic key material under execution [17].

Setup. To underfeed the supply voltage of the system, the attacker needs to tap into the power supply line of the device

and connect a power supply unit. Without precise timing, the faults tend to occur uniformly throughout the computation, thus the attacker should be able to discard the results that are not useful to perform an attack. This requires only basic skills and can be easily achieved in practice without leaving an evidence of tampering. Moreover, no knowledge of the implementation details of the device is needed.

However, to execute a timed power spike injection, the attacker requires a specialized circuit capable of reducing the supply voltage below a specific threshold. This custom circuit must be synchronized with the microcontroller by utilizing the same clock signal, enabling precise timing for the spike injection. The accuracy of the voltage drop, in terms of both duration and synchronization with the target device, directly determines the temporal precision of the fault injection. For such attacks it is required to have a deep knowledge of the attacked architecture. Also, the difficulties in applying this technique increase with the clock rate of the attacked circuit, since a better temporal precision will be required to correctly time the injection of the spike. These methods require few tens of USD of equipment in order to setup the attack, as the necessary equipment could be only wires and a power source [14]. Therefore, when the attacker has access to the supply line of the device, voltage glitching is generally easy and cheap to implement.

Implications on single chip mote. Single-chip motes include on-chip voltage regulators. To underfeed the voltage of the single chip mote, the attacker needs to tap into the silicon and to access the power supply line trace to branch his power supply unit. This requires using an FIB workstation, mentioned in the previous attack. If the attacker wants to inject a timed voltage spike on the chip, then the setup will be even more complicated. This is because the attacker now has to access both the power supply line and the clock line, in order to listen to the chip clock and obtain a precise timing for the voltage glitch. Even if the attacker could read the clock signal without accessing the clock line directly, e.g. using side-channel analysis, the setup will not be as simple as for a board-based system, where the attacker can read the clock signal by only using a wire probe. Thus, in both untimed and timed scenarios of the voltage glitching attack, a single chip mote requires much more advanced equipment and skills compared to a board-based system.

However, a single chip mote is more sensitive to any voltage glitch due to its "crystal-free" nature. It uses on-chip oscillators that are less stable than crystal-oscillators when the power supply voltage changes. Even for a very small voltage variation, they start to oscillate at a different frequency and compensation is required.

C. Electromagnetic Fault Injection (EMFI)

Definition. A practical way to induce faults without having to tap into the device and attach any wire as in clock/voltage glitching, is to cause strong electromagnetic (EM) disturbances near it. The eddy currents induced in the circuit by strong EM pulses cause temporary alterations of the level of a signal, which may be recorded by a latch.

Attacker objectives. High-precision probes connected to EM pulse generators can be used to perturb specific regions of the system while shielding other components. Different methods are used to perturb data in CPU registers, the pipeline, Memory Management Unit (MMU), caches or external memory [17]. For example, injecting a fault in the bootloader code loaded into cache memory allows the attacker to skip into an unreachable code region of the bootloader containing a command line interface for debugging purposes. Also, triggering instruction corruption errors allows the modification of a program workflow. Besides using EMFIs to trigger general instruction and data corruption faults, some works used it to examine cryptographic implementations.

Setup. To inject an EM pulse, the attacker needs a near-field injection probe. He can either manufacture it from very low-cost components having a moderate knowledge in electronics, or buy it with a couple of hundreds USD. Generally, a ferrite core, a copper wire, a connector, and a heat shrinking tube are enough to create a custom probe. Furthermore, pulse injectors can be bought for a price of few thousands USD. For more powerful and precise equipment, the attacker can use high voltage EM pulse generators that would generally range between 10 000 and 20 000 USD. Hence, the cost of the equipment required to perform these attacks ranges from few hundreds to tens of thousands USD [14].

EMFI is considered a fault injection technique with a poor spatial resolution, especially when considering that of laser platforms, mainly because EMFI probes are quite large. We refer to the spatial resolution as the measure of the smallest area that can be targeted by an EMFI probe, without causing unwanted faults in neighboring circuitry. Besides the probe size, the spatial resolution is affected by the pulse amplitude and its polarity, the injector position and its orientation. In a recent work, the authors could show a possible enhancement to the spatial resolution of EMFI [18], with an order of few hundreds of micrometers square.

Moreover, EMFI does not need a device decapsulation for chips enclosed in a standard epoxy package. However, decapsulation is required when chips have a grounded metal packaging, i.e. a heat sink, which acts as an EM shield. Decapsulation can be performed with low-cost equipment (nitric acid and common glassware), thus not raising the cost of the attack considerably. Since the EM pulse may affect undesired parts of the device, it is necessary to shield the components which should not be disturbed using a properly grounded metal plate or mesh.

Implications on single chip mote. In general, an increase in target device density and complexity requires the EM injector to direct electromagnetic radiation at a smaller area of the target device. For example, suppose that two bytes of SRAM memory require 96 transistors on a chip die and the goal of the EMFI is to disturb the read of these two bytes value. In this case, the spatial resolution of the injection probe should be able to fault some subset of the 96 transistors. However,

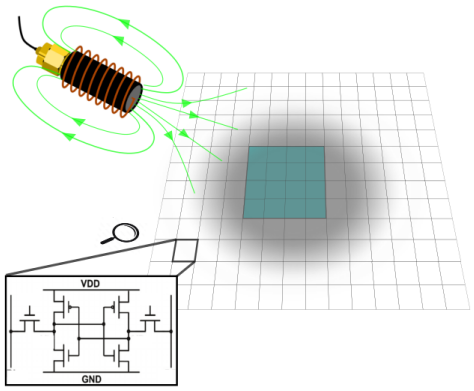

Fig. 4. Illustration of an EM fault injection probe setup. Blue cells depict the target block of SRAM memory. Shaded cells depict unwanted faults in the neighboring area of the target block. The architecture of a single 6-transistor SRAM cell (single bit) is shown at the left bottom.

the distance between transistors and the size of the transistors, determined by the fabrication process, is decreasing significantly over time. Therefore, the spatial resolution necessary for faulting is also increasing by the same factor. An illustration of this example is shown in Fig. 4. Thus, the fabrication process used to fabricate a chip plays an important role in making this kind of attack successful or not. The more advanced (smaller) the process is, the less the spatial resolution of the attack is. Companies often use larger transistors due to the cost constraints. However, some companies prioritize energy efficiency and heat generation, so they would typically use smaller processes. Due to this variety of process fabrication used in both COTS devices and single chip motes, it is hard to make general conclusions.

D. Heating Attacks

Definition. Heating attacks alter the environmental conditions of the system, by causing the temperature to rise beyond the specified maximum limit for a normal functioning.

Attacker objectives. The exposure to extreme temperatures causes multi-bit errors in dynamic random-access memory (DRAM). Data corruption or loss also results in non-volatile memory due to read/write threshold mismatches. For example, these generated bit errors can cause security vulnerabilities on a personal computer [19]. Furthermore, this attack can be used to facilitate other FIAs, such as the clock glitching attack [20]: combined with other faults, it leads to higher success rates for inducing erroneous instruction repetitions, replacements, and modifications of their destination registers in a microcontroller.

Setup. The temperature of a chip can be increased using a 50W light bulb, with a thermometer to measure the temperature [19]. Hence, the level of heating can be tuned through modifying the distance from the chip. The setup of this attack thus requires minimal technical knowledge, and the equipment has a low-cost and is easily available. However, heating attacks are among the most destructive of FIAs, leading to permanent damage after intensive exposure for a long time.

Implications on single chip mote. State-of-the-art demonstrates that heating attacks are successful in tampering with dynamic random-access memory (DRAM) and non-volatile memory. However, due to the current technological limitations, state-of-the-art single chip motes do not have either DRAM nor non-volatile memory: they use SRAM memory, as discussed in Section II. SRAM is much more stable to temperature variations compared to other memory. Thus, compared to board-based systems that mostly have DRAM and non-volatile memory, single chip motes are less exposed to memory faults. Furthermore, board-based systems are exposed to the risk of damage in earlier stages of heating compared to single chip motes. The reason is simple: a CMOS die has a much higher maximum temperature (approx 350 °C) than PCBs. By approaching the maximum temperature of a PCB (approx 200 °C) the components will start to desolder, and at a much higher temperature, the ICs on the board, as well as any single chip mote, will be destroyed. However, one of the main characteristics of single chip motes is their temperature sensitivity: any variation in the ambient temperature will affect the frequency of the internal oscillators if no calibration algorithm is implemented.

E. Optical Fault Injection

Definition. Optical fault injections are based on the ionization effects on transistors caused by exposure to high energy light source. When photons with sufficient energy strike the semiconductor material of a transistor, they can transfer their energy to the electrons in the material, promoting them to a higher energy state and creating electron-hole pairs. The presence of these additional charge carriers can impact the transistor conductivity, create current surges, and introduce unintended electrical effects.

Attacker objectives. Directing strong ultraviolet (UV) radiation at the silicon surface can cause the blanking of non-volatile memory such as erasable EEPROM and FLASH memory cells. These memory cells may store constants needed for the execution of cryptographic algorithms (e.g., the AES S-Boxes). Using UV radiation can also cause the reset of the internal protection fuses of the targeted microcontroller [21]. Similarly, a camera flash coupled with a magnifying lens can be used to target registers and skip instructions on a microcontroller, and to change the values in RAM and SRAM memory [22]. Furthermore, a more precise technique that security evaluation labs would typically choose, is laser fault injection. An attacker can use laser beams to probe the memory revealing its content without changing it [23]. A laser FIA can also cause the bypass of a secure boot process and the authentication check step, or to recover the encryption key [17]. While laser attacks can corrupt only NVM reading or writing, X-ray attacks can be used to directly modify non-volatile memory content.

Setup. Optical fault injection is considered a semi-invasive attack technique: the chip package needs to be removed to expose the chip to the optical source. Although depackaging can be performed with low-cost equipment, the main drawback is the possibility of damaging the circuitry or the bonding

wires. The injection is normally done on the backside of the chip, as the components are less protected.

Assuming the attacker is able to successfully decapsulate a chip, he can perform fault injection attacks by illuminating the die with a high energy light source such as an UV lamp or a camera flash to cause random faults. This technique requires that the illuminated area has not been covered by a metallic layer such as metal wires, which may provide a shield against radiation. To shield the circuit parts which need not be exposed, they can be covered with a readily available UV-resistant dye, or with an aperture made from aluminum foil. Furthermore, in order to obtain a sufficiently focused light beam from a camera flash, a precision microscope must be used. Although the price of this setup could be relatively high, it was recently shown that it is possible to use an inexpensive ball lens to focus the camera flash offering an equipment costing 500 USD.

Thus in order to enhance the previous technique and to introduce faults with a better precision, laser FIAs can be used. Using these intense sources of ultraviolet, infrared or visible light, an attacker can target single components on the chip, such as transistors and logic gates. A standard setup of laser FI would consist of the following parts: laser source, objective lens, motorized positioning table, and a controlling device. A digital oscilloscope can be also used to precisely align the laser activation with the execution of the target routine on the device. While the cost of a fully assembled setup would normally be less than 50 000 USD, it is possible to assemble a working setup as good as laser FI under 500 USD using a solid-state laser diode instead. The main limitation of this fault injection technique is the fact that it is not possible to achieve subwavelength precision. In fact, the width of the gate is continuously shrinking with advancements in lithography technology, thus limiting the smallest number of gates hit by the radiation.

The perturbation induced by a laser beam is limited in resolution by its wavelength to tens of micrometers [8]. To modify the state of a single transistor, it is possible to use a nanofocused X-ray beam (spatial resolution of a few tens of nanometers) [24]. The advantage of this method is that there is no need to remove the chip package as it is transparent to the beam. The method also offers the advantage of deeply penetrating through materials. However, the technique is extremely expensive, in the range of millions of USD.

Implications on single chip mote. With the absence of non-volatile memory in today's single chip motes, cf. Section II-B, we are not concerned with the simplest attack technique using a UV lamp or a camera flash for erasure. Even when a camera flash with a magnification lens or a laser is used, state-of-the art attacks are proved to be successful on microprocessors fabricated using 350 nm, 250 nm, 130 nm and 90 nm CMOS process [22], [25]. However, there is no proof – to the best of our knowledge – that these techniques can succeed with more advanced fabrication technology such as the 65 nm process used to fabricate today's single chip motes. As mentioned above, the main limitation of using these injection methods is that they cannot achieve subwavelength precision. This is because conventionally the minimum length scale on which a beam of light can operate is equal to half its wavelength, unless light is coupled to matter, causing photonic effects that can be realized on a much smaller spatial scale. In fact, UV radiations have smaller wavelength compared to visible and infrared light, ranging from 100 to 400 nm. Thus, in theory, it is possible to target a single transistor fabricated using 65nm process using a UV laser. Furthermore, it is pretty easy to target these transistors using other radiations with smaller wavelength, such as the X-ray radiations. Thus, the spatial precision of these attacks depends on the fabrication process used, regardless if it is a COTS device or a single chip mote, as previously detailed for EMFIs.

F. Ion-based Fault Injection

Definition. The most powerful and precise fault injection techniques use focused ion beams (FIB) and heavy-ion microbeams (HIM). FIB systems typically use liquid metal ion sources, e.g. gallium ions, where the low atomic mass and relatively low energy of gallium ions make them suitable for high-resolution imaging and precision milling of materials at the micro/nanoscale. In contrast, HIM systems employ ions with high atomic masses such as gold ion, where the high energy and large mass of heavy ions enable them to penetrate deeper into materials.

Attacker objectives. FIB workstations are commonly used to debug and patch chip prototypes, or to reverse engineer unknown designs through adding probing wires to otherwise inaccessible parts of the circuit. More precisely, it is possible with FIB to arbitrarily modify the structure of a circuit, reconstruct missing buses, cut existing wires, mill through layers, and rebuild them. These options represent a big advantage of using FIB compared to nanofocused X-ray beams. Moreover, this capability to manipulate silicon substrates, opens up the possibility of conducting hardware-level reworking (microsurgery) on security-critical components, as well as the ability to extract hardware-fused keys. It is even possible to reconstruct an entire read bus of a memory containing a cryptographic key without damaging the contents of the memory [26]. However, HIM are mainly used to simulate radiation-induced failures or vulnerabilities, allowing researchers to assess the device's radiation tolerance and evaluate the effectiveness of mitigation strategies. It is especially important for electronic devices destined for space applications or high-radiation environments. In brief, while FIB focuses more on precision milling and fabrication at the micro/nanoscale, HIMs are mainly used for radiation testing and fault analysis of electronic devices.

Setup. On the one hand, a FIB system typically includes an ion source, an ion column for focusing and scanning the ion beam, and a sample stage where the target material is positioned. The FIB system is equipped with precise control mechanisms to position the ion beam and adjust its intensity. Imaging systems and detectors are also incorporated to observe the sample during the process. State-of-the-art FIBs can operate

at a precision of 2.5 nm [17], less than the gate width of the smallest etchable transistor. On the other hand, an HIM system typically involves an ion accelerator, which accelerates heavy ions to high energies, and a focusing system that focuses the ion beam to a microscopic spot size. The target material or device under test is placed in the path of the focused ion beam, and detectors are used to measure the effects of the injected ions. While heavy-ion microbeams can achieve reasonably high resolution, their spatial resolution is generally not as high as that of FIB systems. They are more commonly used for larger-scale irradiation experiments. FIB and HIM attacks impose substantial cost (100 000+ USD) and require access to specialised expertise and testing equipment. They are out of the practical bounds for the class of attackers normally considered when attacking devices such as credit cards or IoT devices. However, a consideration needs to be in place for very critical systems such as military communication equipment.

Implications on single chip mote. Since ion-based fault injections techniques operate at nanoscale, and can target even the smallest etchable transistor, then we notice an equivalence between performing such attacks on a single chip mote or on a PCB and its components.

IV. Conclusion

In this paper, we studied multiple techniques of fault injection attacks to evaluate their effects on single chip motes compared to board-based systems. Attacks that use radiation, electromagnetic pulses, or exposure to intense light or ion beams have about the same difficulty regardless if the target is a single chip mote or a PCB system. Clock and voltage glitching are easier to perform on PCB systems due to the ease of access to the interconnections. However, single chip motes can be easily affected by - intentional or unintentional - variations in the ambient temperature due to their less stable crystal-free oscillators.

References

[1] S. J. Ramson and D. J. Moni, "Applications of wireless sensor networks—a survey," in *2017 international conference on innovations in electrical, electronics, instrumentation and media technology (ICEEIMT)*. IEEE, 2017, pp. 325–329.

[2] Y. Shi, M. Choi, Z. Li, G. Kim, Z. Foo, H.-S. Kim, D. Wentzloff, and D. Blaauw, "26.7 a 10mm3 syringe-implantable near-field radio system on glass substrate," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*. IEEE, 2016, pp. 448–449.

[3] B. Warneke, M. Last, B. Liebowitz, and K. S. Pister, "Smart dust: Communicating with a cubic-millimeter computer," *Computer*, vol. 34, no. 1, pp. 44–51, 2001.

[4] R. Send, Q. R. Xu, I. Paprotny, R. M. White, and P. K. Wright, "Granular radio energy-sensing node (green): A 0.56 cm 3 wireless stick-on node for non-intrusive energy monitoring," in *SENSORS, 2013 IEEE*. IEEE, 2013, pp. 1–4.

[5] Y. Lee, S. Bang, I. Lee, Y. Kim, G. Kim, M. H. Ghaed, P. Pannuto, P. Dutta, D. Sylvester, and D. Blaauw, "A modular 1 mm^3 die-stacked sensing platform with low power i^2 c inter-die communication and multi-modal energy harvesting," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 1, pp. 229–243, 2012.

[6] F. Maksimovic, B. Wheeler, D. C. Burnett, O. Khan, S. Mesri, I. Suciu, L. Lee, A. Moreno, A. Sundararajan, B. Zhou *et al.*, "A crystal-free single-chip micro mote with integrated 802.15. 4 compatible transceiver, sub-mw BLE compatible beacon transmitter, and cortex M0," in *2019 Symposium on VLSI Circuits*. IEEE, 2019, pp. C88–C89.

[7] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[8] H. Li, G. Du, C. Shao, L. Dai, G. Xu, and J. Guo, "Heavy-ion microbeam fault injection into sram-based fpga implementations of cryptographic circuits," *IEEE Transactions on Nuclear Science*, vol. 62, no. 3, pp. 1341–1348, 2015.

[9] T. Watteyne, B. Kerkez, K. Pister, and S. Glaser, "Crystal-free network synchronization," *trans. Emerging Tel. Tech*, 2016.

[10] J. Van Beek and R. Puers, "A review of MEMS oscillators for frequency reference and timing applications," *Journal of Micromechanics and Microengineering*, vol. 22, no. 1, p. 013001, 2011.

[11] D. Griffith, T. Kallerud, B. Goodlin, Z. Hughes, E. T.-T. Yen *et al.*, "A±10ppm- 40 to 125°c BAW-based frequency reference system for crystal-less wireless sensor nodes," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2017, pp. 1–4.

[12] O. Khan, B. Wheeler, D. Burnett, F. Maksimovic, S. Mesri, K. Pister, and A. Niknejad, "Frequency reference for crystal free radio," in *2016 IEEE International Frequency Control Symposium (IFCS)*. IEEE, 2016, pp. 1–2.

[13] D. C. Burnett, B. Wheeler, L. Lee, F. Maksimovic, A. Sundararajan, O. Khan, and K. S. J. Pister, "CMOS oscillators to satisfy 802.15.4 and bluetooth le phy specifications without a crystal reference," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2019, pp. 0218–0223.

[14] J. Breier and X. Hou, "How practical are fault injection attacks, really?" *IEEE Access*, vol. 10, pp. 113 122–113 130, 2022.

[15] L. Claudepierre, P.-Y. Péneau, D. Hardy, and E. Rohou, "Traitor: a low-cost evaluation platform for multifault injection," in *Proceedings of the 2021 International Symposium on Advanced Security on Software and Systems*, 2021, pp. 51–56.

[16] R. Kumar, P. Jovanovic, and I. Polian, "Precise fault-injections using voltage and temperature manipulation for differential cryptanalysis," in *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*. IEEE, 2014, pp. 43–48.

[17] C. Shepherd, K. Markantonakis, N. van Heijningen, D. Aboulkassimi, C. Gaine, T. Heckmann, and D. Naccache, "Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis," *Computers & Security*, vol. 111, p. 102471, 2021.

[18] J. Toulemont, G. Chancel, J. M. Gallière, F. Mailly, P. Nouet, and P. Maurine, "On the scaling of emfi probes," in *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE, 2021, pp. 67–73.

[19] S. Govindavajhala and A. W. Appel, "Using memory errors to attack a virtual machine," in *2003 Symposium on Security and Privacy, 2003.* IEEE, 2003, pp. 154–165.

[20] T. Korak, M. Hutter, B. Ege, and L. Batina, "Clock glitch attacks in the presence of heating," in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2014, pp. 104–114.

[21] J.-M. Schmidt, M. Hutter, and T. Plos, "Optical fault attacks on AES: A threat in violet," in *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2009, pp. 13–22.

[22] O. M. Guillen, M. Gruber, and F. De Santis, "Low-cost setup for localized semi-invasive optical fault injection attacks: How low can we go?" in *Constructive Side-Channel Analysis and Secure Design: 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers 8*. Springer, 2017, pp. 207–222.

[23] S. Chef, C. T. Chua, J. Y. Tay, Y. W. Siah, S. Bhasin, J. Breier, and C. L. Gan, "Descrambling of embedded sram using a laser probe," in *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2018, pp. 1–6.

[24] S. Anceau, P. Bleuet, J. Clédière, L. Maingault, J.-l. Rainard, and R. Tucoulou, "Nanofocused x-ray beam to reprogram secure circuits," in *Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Springer, 2017, pp. 175–188.

[25] D. Petryk, Z. Dyka, R. Sorge, J. Schäffner, and P. Langendörfer, "Optical fault injection attacks against radiation-hard shift registers," in *2021 24th Euromicro Conference on Digital System Design (DSD)*. IEEE, 2021, pp. 371–375.

[26] R. Torrance and D. James, "The state-of-the-art in ic reverse engineering," in *Cryptographic Hardware and Embedded Systems-CHES 2009: 11th International Workshop Lausanne, Switzerland, September 6-9, 2009 Proceedings*. Springer, 2009, pp. 363–381.