Volume 9, Issue 9, September– 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1231

Hardware Security Breaches: Alarming Exploits Beyond Tampering

Johnbasco Vijay Anand. J[1]
Cyber Security Head,
NeST Digital Private Limited,
Bangalore, 560 048

Abstract:- Side Channel Attacks (SCAs) and Fault Injection Attacks have emerged as significant threats to the security of electronic devices. This paper explores these hardware attack vectors in the context of recent incidents [11] involving pagers and walkie-talkies. We shall deep dive into the possible mechanisms of these attacks, how they can be combined for increased efficacy, and their implications for device security. This paper discusses only the possible ways [1] the adversaries could have exploited and may include other attack vectors such as supply chain attack and few others. The aim of this paper as we discuss the potential attack mechanisms is only to focus on mitigations and awareness of the reader to perform advanced security testing.

I. INTRODUCTION

In today's interconnected world, communication devices like walkie-talkies, pagers and other critical systems have become essential tools for various sectors, ranging from public safety to private enterprise. However, the recent wave of unexplained failures in these devices has drawn attention to alarming security vulnerabilities at the hardware level. Traditionally considered more secure than their software counterparts, hardware components are now increasingly targeted by sophisticated attacks. These attacks not only exploit flaws in the physical construction of chips but also leverage side channels and fault injection techniques [3] to compromise the integrity and functionality of the device. As we've seen with recent incidents, the consequences can be catastrophic, causing widespread disruptions to vital communication networks.

One of the most concerning aspects of these hardware attacks is the growing prevalence of supply chain attacks, which compromise devices even before they reach the end user. By introducing malicious elements, such as hardware Trojans, during the design or manufacturing process, attackers can create backdoors that provide unauthorized access to sensitive systems. These malicious modifications [4] are often undetectable through standard testing procedures, allowing compromised devices to be deployed in critical environments. Once activated, these Trojans can disable security mechanisms, leak sensitive information, or render devices inoperative. The result is a compromised communication network [3] that is vulnerable to external exploitation, leading to large-scale failures.

When supply chain attacks are combined with techniques like Side Channel Attacks (SCAs) and Fault Injection Attacks, the risk multiplies. SCAs allow attackers to extract sensitive data by observing subtle physical characteristics of the device, such as power consumption or electromagnetic emissions. Meanwhile, fault injection techniques [2] manipulate the device's operation by introducing errors in voltage or timing, enabling attackers to bypass security features or corrupt data. These combined methods can be devastating, as attackers can gain full control of communication devices, creating far-reaching consequences for security, privacy and the integrity of entire systems.

In this paper, we focus on several recent attack vectors that have led to catastrophic consequences [11]. These attacks go beyond compromising the basic CIA triad of hardware systems; they pose direct threats to human life. Confidentiality is no longer just about protecting Personally Identifiable Information (PII); it's about ensuring that users maintain trust and confidence in the system, whether it's software or hardware. The true danger lies in eroding that confidence, making systems unsafe to use regardless of their design.

II. SIDE CHANNEL ATTACKS

SCAs exploit the indirect information emitted by electronic devices during operation. These attacks are generally non-invasive[5] and passive, requiring no physical tampering with the device. The two Phases of SCA are monitoring and data analysis phase

➢ *Monitoring Phase*

Attackers measure the device's physical characteristics under normal operation. This includes:

- Power Consumption Analysis: The attacker measures fluctuations in the device's power consumption, typically during cryptographic operations, to extract sensitive information like encryption keys.
- Electromagnetic Radiation Monitoring: The attacker records electromagnetic emissions produced by the device to infer patterns and reveal data being processed.
- Timing Information Analysis: The attacker monitors the time taken by the device to complete specific computations, identifying variations that can expose internal processes or secrets.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1231

- Acoustic Signal Observation: The attacker listens to sounds emitted by the device, such as keystrokes, to deduce the data being entered or processed.
- Optical Emission Analysis: The attacker observes light signals, such as LED activity, to gather clues about the device's internal states or operations.
- Thermal Monitoring: The attacker monitors the heat output of the device, using temperature changes to infer operations or sensitive data being processed.

➢ *Data Analysis Phase*

The Collected data is processed using statistical and mathematical techniques to extract sensitive information, such as cryptographic keys or proprietary algorithms.

III. FAULT INJECTION ATTACKS

Once attackers have gathered sufficient information through SCAs, they can launch a Fault Injection Attack [6] to induce abnormal behavior in the device. Fault Injection Attacks are hardware-based attacks that exploit vulnerabilities by deliberately introducing (INJECTING) errors [5] into a system's operation. They are particularly dangerous because they can bypass traditional security measures that protect against software-based threats. Faults of different types are injected into the hardware and listed below are few of the potential threats in the recent times:

➢ *Voltage Glitching*

By suddenly altering the supply voltage—either increasing or decreasing it—attackers can create faults within the circuit. This abrupt change can cause the device to behave unpredictably, potentially granting access to privileged information or disrupting normal operations. In order to perform voltage glitching a faultier [12] device is connected to the target device and the glitch is performed as shown in Fig – A. It is also observed that,

$$P\alpha\ C\ V^2\ f$$

Where P is the Dynamic Power required to charge and discharge capacitors in a system.

V is the voltage and f is the frequency of the operation.

When logical values change from 0 to 1 or vice versa, it results in higher power consumption compared to when the logical value remains constant. The leakage current of a logical device is also related to the input value to that device.

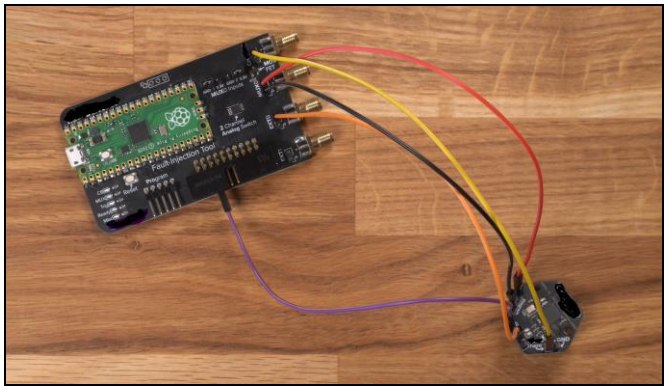

Fig 1 Faultier Voltage Glitching Device Connected to a Tagging Device where the Voltage Glitch is Aimed.

➢ *Clock Glitching*

Manipulating the clock signal that synchronizes the operations of a device can introduce errors during critical processes like encryption. This can weaken cryptographic defenses, allowing attackers to extract sensitive data.

➢ *Data Corruption and Manipulation*

Attacks targeting the data used by software, such as user inputs, hard-coded values, or configuration settings, can alter the program's behavior. This can lead to unauthorized actions or the exposure of confidential information.

➢ *Electromagnetic (EM) Glitching*

EM glitching uses electromagnetic fields[3] to induce faults non-invasively. Attackers can disrupt a device's operation without physical contact, making this method stealthy and effective.

➢ *Laser Fault Injection*

By directing a laser at specific points on a chip, attackers can influence signal timing and flip bits in memory components like SRAMs. This precise method [7] allows for targeted manipulation of a device's internal processes.

With any of the above Fault Injection techniques, the attackers could glitch at precise moments, causing the device to malfunction. This might lead to:

- Corrupting Memory or Registers through which the Attackers can flip bits in memory or registers, potentially altering critical instructions or data, which could cause the device to bypass security checks or expose sensitive information.
- Device crash, potentially resetting the system or allowing attackers to execute arbitrary code.
- Bypassing Authentication or Encryption by manipulating cryptographic operations, attackers could bypass authentication mechanisms or even extract cryptographic keys directly.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1231

IV. SUPPLY CHAIN ATTACKS

Supply chain attacks pose a significant threat to hardware security by compromising devices before they reach end users. In this type of attack, malicious actors tamper with hardware components during manufacturing, distribution or assembly. This can involve right from the hardware design [8] by introducing backdoors at the digital logic design, inserting hardware Trojans, backdoors or faulty components into devices like communication systems, enabling attackers to exploit vulnerabilities once deployed. These attacks are particularly dangerous because they are often undetectable by standard testing methods, making the affected hardware unreliable and insecure, potentially leading to breaches in the CIA triad (Confidentiality, Integrity, Availability) while the OEM may still consider the vulnerable ones as a Trusted IC [9].

In recent middle east (Lebanon communication devices explosions) case [11], though the investigations are ongoing, supply chain compromises may have happened to embed malicious modifications that allow attackers to control, monitor or even sabotage devices, highlighting the need for rigorous hardware security measures throughout the product lifecycle.

V. COMBINING DIFFERENT ATTACK VECTORS

The catastrophic effect of a combined security attack [11] including SCA, Fault Injection and Supply chain attack can be best explained with a case study as explained below.

The following analysis presents some of the possible attack scenarios based on theoretical data points and technical research. It is important to note that these are hypothetical examples and do not reference any specific real-world incidents. This discussion is intended for educational purposes only and should not be construed as a description of actual events.

- *Case Study:*

A Hypothetical Analysis of Potential Attack Vectors in the Lebanon Communication Devices Explosion The recent explosion [11] of communication devices, such as pagers and walkie-talkies in Lebanon, raises critical concerns regarding potential security vulnerabilities in hardware design. While investigations are still ongoing, various attack vectors, including Side Channel Attacks (SCAs), Fault Injection Attacks and Supply Chain Compromises[4], could hypothetically have contributed to such an event. This case study explores possible scenarios, focusing on how these attack techniques might have been utilized, while acknowledging that this is a theoretical exploration based on available technical data.

- *Possible Side Channel Attack (SCA):*

One potential vector could involve Power Analysis to extract sensitive operational data from communication devices. Attackers could have monitored power consumption patterns in the pagers to identify key operations or trigger an unexpected device response. By exploiting power consumption fluctuations during specific computations, attackers might have used this information to manipulate the devices remotely or bypass security mechanisms. In a real-world scenario, SCAs could act as reconnaissance tools to further exploit vulnerabilities, such as triggering hidden backdoors or malicious functions embedded within the device.

- *Potential Fault Injection Attack:*

A plausible Fault Injection Attack technique that might have been employed is Voltage Glitching. By rapidly altering the voltage supply to the communication devices, attackers could have caused the pagers and walkie-talkies to malfunction, potentially triggering an explosive event. Such attacks could induce errors in the device's processing system, leading to system instability or bypassing security controls. In this hypothetical case, the sudden detonation of multiple devices may point to a coordinated fault injection, possibly combined with prior reconnaissance through SCA, to trigger the explosion at a precise time.

- *Supply Chain Compromise Hypothesis:*

Another critical vector that could have played a role is a Supply Chain Attack. During the manufacturing or distribution phase, malicious actors might have compromised the hardware components, embedding hardware Trojans [9] or integrating explosive materials into the design. This hypothetical supply chain infiltration could have resulted in pagers and walkie-talkies being fitted with modified batteries or chips that contained hidden triggers or remote-controlled explosives. The use of such a Trojan could explain how these devices were manipulated post-distribution, allowing attackers to remotely activate the malicious functions at a specific time.

- *Case Study Conclusion:*

This theoretical case study demonstrates how multiple attack vectors could potentially be combined to exploit vulnerabilities in communication devices. Side Channel Attacks could gather essential information, Fault Injection Attacks might trigger system malfunctions and Supply Chain Compromises [8] could introduce pre-existing vulnerabilities that remain hidden until remotely activated. It is crucial to recognize that this analysis is based on hypothetical scenarios and does not suggest definitive conclusions about the recent incidents, which are still under investigation. The intent here is to provide insight into possible attack strategies and their implications for hardware security.

- *Disclaimer:*

The above analysis presents potential ways these attacks could occur and is not a definitive account of real-world events. This article is speculative and intended solely for educational purposes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1231

VI. INEVITABLE HARDWARE SECURITY TESTING

The complexity of modern hardware demands robust testing methodologies to ensure system security, especially against threats such as Hardware Trojans. Testing is critical because attackers can exploit vulnerabilities that standard checks might overlook.

Test time approaches focus on running test patterns to identify anomalies in system behavior. However, covering all potential vectors is impractical due to the sheer number of test vectors required for large circuits. To mitigate this, random test-based methods have emerged, but these are not foolproof, as rare test vectors might fail to activate hidden hardware Trojans[7]. A complementary strategy involves side channel analysis (SCA), where power consumption, timing delays and electromagnetic (EM) emissions are monitored during system execution to detect irregularities. For example, power side channel analysis measures supply current at both quiescent and transient stages to spot variations. Although effective, these methods are sensitive to noise and fabrication variations, leading to potential false alarms.

In addition to test time approaches, runtime monitoring is a critical layer of protection. By continuously observing system behavior in real time, this approach can catch Trojans missed by initial testing. While runtime monitoring enhances detection, it does come with trade-offs, as it requires dedicated resources and may introduce performance overhead.

Beyond traditional methods, innovations like Trusted Platform Modules (TPMs), Physical Unclonable Functions (PUFs) and watermarking provide hardware-based security features. TPMs ensure cryptographic keys are securely generated and stored, enhancing authentication mechanisms [6]. Meanwhile, PUFs leverage the unique physical characteristics of individual components to generate unclonable identifiers, adding another layer of security against cloning and tampering.

Testing is also vital in securing FPGA-based systems, which are increasingly used for flexible cryptographic implementations. These systems are susceptible to both software and hardware attacks, including side channel exploits and Trojan insertions. Effective testing in FPGAs requires a combination of secure design practices and robust testing to mitigate vulnerabilities. The role of hardware testing [8] extends beyond detection—it is foundational in ensuring that devices perform securely and reliably in the real world, making it a crucial element in building trusted systems.

Thus, hardware testing is inevitable in safeguarding devices from the ever-evolving landscape of hardware-based threats. The combination of test time approaches, runtime monitoring and secure design practices must be integrated to create a comprehensive defense strategy. analysis presents potential ways these attacks could occur and is not a definitive account of real-world events. This article is speculative and intended solely for educational purposes.

VII. CONCLUSION

As our reliance on communication devices grows, so does the urgency of securing the hardware that powers them. This paper explored possible attack vectors like SCAs, Fault Injection and Supply Chain attacks—highlighting how each could compromise critical systems. The potential for these attacks to cause widespread damage underscores the need for proactive hardware security. By adopting comprehensive testing approaches [8], such as side channel analysis, runtime monitoring and leveraging technologies like TPMs and PUFs[5], we can ensure that the integrity, confidentiality and availability of devices are maintained.

As we are increasingly dependent on secure communication, hardware security is no longer optional; it is vital to maintaining trust in technology. We must prioritize hardware security as an essential part of overall system protection, addressing vulnerabilities before they lead to real-world consequences. The path forward demands rigorous, continuous testing and innovation to defend against evolving threats, ensuring that the devices we depend on remain safe and reliable.

- *Author Profile*

Johnbasco Vijay Anand is an advisory cyber security architect at NeST Digital Private Limited and he heads the cyber security competency. He is also a parttime Ph.D. scholar in the area of Quantum Key Distribution. He holds dual master(s) degree in Physics and Computer Application. His area of interest includes Hardware Security, Quantum Fault injection analysis, Quantum-Resistant Hardware and is also interested in advanced research in cyber security hardening using Quantum Computing and Artificial Intelligence.

REFFERENCES

[1]. The Hardware Security Threat Landscape and Possible Countermeasures: A Survey. ACM Computing Surveys (CSUR), vol. 53, no. 6, 2020.
[2]. M. Tehranipoor and F. Koushanfar, "Trustworthy Hardware: Trojan Detection and Prevention Methods in Supply Chain," IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10-25, 2010.
[3]. J. Rajendran, et al., "Hardware Trojans: Threats and Emerging Solutions," Proc. IEEE, vol. 102, no. 8, pp. 1229-1247, 2014.
[4]. G. T. Becker, F. Regazzoni, C. Paar, and W. Burleson, "Stealthy Dopant-Level Hardware Trojans: Extended Version," IEEE Trans. on CAD of Integrated Circuits and Systems, vol. 33, no. 12, pp. 1778-1791, Dec. 2014.
[5]. P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proc. Advances in Cryptology (CRYPTO), pp. 388-397, 1999.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1231

[6]. Y. Jin and D. Sullivan, "Hardware Security: Threat Models and Security Requirements," in IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016.
[7]. M. Potkonjak et al., "Hardware Trojan Design and Implementation Challenges," in IEEE Int. Conf. on Computer Design (ICCD), 2011.
[8]. D. Mukhopadhyay, R. S. Chakraborty, and C. Paar, "Hardware Security: Design, Threats, and Safeguards," IEEE Computer Society, 2013.
[9]. T. Xu, W. Burleson, and D. Holcomb, "Using Environmental Noise as a Source of Entropy for Purely Digital True Random Number Generators," IEEE Trans. on Computers, vol. 62, no. 8, pp. 1524-1537, 2013.
[10]. M. T. Rahman and M. Tehranipoor, "A Comprehensive Survey of Defense Mechanisms against Hardware Trojan Attacks," IEEE Trans. on Design and Test, vol. 30, no. 1, pp. 26-45, Jan. 2013.
[11]. https://en.wikipedia.org/wiki/2024_Lebanon_pager_explosions
[12]. https://www.hextree.io/