The Importance of Maintaining Hardware Security is the same as Maintaining Software.

By:

Group 4

Muhammad Fakhri Amir

Zahwa Aprilia

CLASS 3CS2

FACULTY OF ENGINEERING

CEP-CCIT FTUI

2025

PREFACE

We express our deepest gratitude to Almighty God for His boundless mercy and grace in completing this manuscript, which is part of the Center of Excellence Program (CEP) at the Center for Computing and Information Technology (CCIT), Faculty of Engineering, University of Indonesia. We also extend our appreciation to mentors and colleagues whose support has been invaluable in shaping this work.

Because software is vulnerable to cyberattacks, security in the field of information technology has historically placed a strong emphasis on protecting it. Nevertheless, this focus frequently obscures the vital necessity of safeguarding the hardware elements that serve as the foundation of every technological system. Similar to how software flaws can result in major security breaches, hardware flaws also present considerable hazards that could jeopardize the integrity of the entire system.

The purpose of this study is to emphasize how crucial it is to maintain both software and hardware security. It promotes a balanced strategy for protecting technology infrastructure by encouraging a thorough awareness of both facets. Ultimately, strong defense mechanisms that improve the overall resilience of information systems are ensured when hardware is protected with the same vigilance as software.

CEP- CCIT Faculty of Engineering

Universitas indonesia

Table Of Contents

CHAPTER 1
INTRODUCTION

I.1 Background

As electronic systems with integrated computing platforms and networking interfaces become more complicated, hardware security has grown in importance within the field of information technology. While software protection has historically been the focus of cybersecurity efforts, hardware threats, such as illegal changes to device functioning, offer serious hazards that jeopardize national security, user privacy, and system integrity. These attacks have serious repercussions yet can be more difficult to carry out. Malicious interventions are made easier throughout the lifecycle of an integrated circuit due to the global and complex structure of the supply chain, which involves numerous organizations in the design, manufacture, and deployment phases.

The serious risks of ignoring hardware security are demonstrated by real-world incidents, including as servers with corrupted microchips, communication equipment with explosive alterations, and cryptographic hardware with hidden backdoors. Examples like this demonstrate how hardware vulnerabilities are pervasive systemic problems that affect a variety of industries, from consumer electronics to military equipment. Ensuring hardware security is just as important as software protection since hardware defects immediately compromise software defenses. A comprehensive approach that incorporates rigorous evaluation models, regulatory standards, and supply chain openness is necessary to address hardware security. Hardware and software security should be equally prioritized and funded in order to strengthen defenses, lower vulnerabilities, and improve the dependability of technological systems in both essential and civilian applications.

I.2 Writing Objective

Emphasize the critical need for hardware security alongside software security by reviewing real-world hardware attacks, proposing a comprehensive assessment model to evaluate attack and defense complexities, and highlighting how the increasing complexity and obscurity of the integrated circuit supply chain contribute to hardware vulnerabilities. The paper aims to bridge the gap between academic research and actual hardware security incidents, advocate for enhanced security policies, and stress the importance of supply chain transparency as a key strategy to mitigate hardware security risks.

I.3 Problem Domain

The context of contemporary electronic systems, where worldwide supply networks and intricate integrated circuits (ICs) pose a number of vulnerabilities. In contrast to software security, hardware assaults are frequently disregarded even though they have the potential to have serious repercussions, including jeopardizing human life, compromising system integrity, revealing private data, and harming vital infrastructure. Malicious interventions at different stages of the hardware lifespan are made possible by the multi-actor, intricate, and opaque IC supply chain, which increases the attack surface. In order to properly mitigate risks and safeguard both critical and civilian applications, hardware security efforts must be aligned with the rigor and priority traditionally assigned to software security. This emphasizes the urgent need for comprehensive assessment models, regulatory frameworks, and transparency measures.

I.4 Writing Methodology

Analyzing real-world hardware security attacks and research cases to bridge the gap between theory and practice. In order to evaluate assaults and defenses across six categories Class, Resources, Difficulty/Security Level, Impact/Risk Acceptance, Identification, and Exploitation it presents an assessment scheme based on the IC design life cycle. A structured framework for comparing attack costs and defense efforts is provided by the method, which also examines pertinent rules and standards. It emphasizes the necessity of supply chain transparency and hardware security measures that are comparable to software security.

I.5 Writing Framework

CHAPTER I INTRODUCTION

Include Background, Writing Objective, Problem Domain, and Writing Methodology.

CHAPTER II BASIC THEORY

Contains all theories about Definition of Hardware, Definition of Integrated Circuit (IC) Supply Chain and Attack Surface and Types of Hardware Attacks.

CHAPTER III PROBLEM ANALYSIS

Includes Relationship Between IC Supply Chain and Hardware Attacks and How Handling Hardware Attack.

CHAPTER IV CONCLUSION AND SUGGESTION

Conclusions and Suggestions Include Material and Analysis.

CHAPTER II

BASIC THEORY

II.1 Basic Concepts of Hardware

Security Hardware security is a field that focuses on the protection of physical components of computer systems such as processors, chips, or electronic devices from attacks and manipulation. Unlike software security, which protects operating systems or applications, hardware security emphasises low-level protection that is directly inherent to the physical components.

The basic principles of security generally refer to the CIA Triad:

1. Confidentiality

   Confidientiality focuses on protecting information from unauthorized access. The aim is to ensure that sensitive data can only be accessed by authorized individuals or systems.
2. Integrity

   Integrity means maintaining the accuracy and consistency of information, and ensuring that data is not unlawfully altered.
3. Availability

   Availability ensures that information and systems can be accessed by authorized usera when needed, whitout unnecessary distruptions.

In the context of hardware, the CIA Triad is expanded to include several additional aspects, namely:

1. Dependability

   Encompasses the reliability, security, and availability of chips to ensure long-term trust worhiness.
2. Isolation

   Separatio between critical and non-critical parts of the system to prevent the spread of attacks.
3. Transparency of Supply Chain

   Openness of information among all parties involved in the chip manufacturing.
4. Secure Handling

   Safe handling of chips during distribution, use, and recycling to prevent tampering.

II.2 Integrated Circuit (IC) Supply Chain and Attack Surface

The Integrated Circuit (IC) supply chain is a complex process involving many parties from design, fabrication, to distribution of chips. This complexity creates opportunities for vulnerabilities to emerge.

The IC supply chain consists of several phases, and each phase has vulnerabilities (attack surfaces) that can be exploited by attackers. Here are the stages:

1. Design Phase

At this stage, the IC architecture is created and designed using Electronic Design Automation (EDA) software. Chip design typically integrates Intellectual Property (IP) cores sourced from third-party vendors. The final outcome of this phase is a digital logic design (such as RTL, netlist, or bitstream) that is ready for production at the semiconductor fabrication plant.

2. Fabrication Phase

After the design is completed, the IC design is sent to the fabrication house to be physically produced into chips in the form of silicon wafers. The fabrication process involves the creation of layers of transistors, interconnections, and highly complex lithography processing, resulting in IC dies ready for packaging.

3. Testing and Integration Phase

Chips that have been produced will undergo a series of functional tests to ensure their quality and reliability. After passing the tests, the IC is integrated into the target system or device, for example, mounted on a motherboard, IoT device, or military system.

4. Operation Phase (IN-Field Use)

in this phase, the IC is actively used by end users in various electronic devices. The chip begins to interact with firmware, software, and other systems, functioning according to the roles defined since the initial design.

5. Recycling / Disposal Phase

When chips are no longer used, they are usually discarded or recycled. At this stage, the IC can be processed again to retrieve its components or marketed again as second-hand chips.

II.3 Types of Hardware Attacks

Although it's more difficult to access physical equipment than software-based assaults like malware, phishing, or hacking attempts, hackers have developed strategies to target hardware over time. Although obsolete firmware, a lack of encryption, and the use of a default password on numerous devices pose the greatest risks to hardware security, other customized assaults are just as harmful.

The following are common types of hardware attacks and what they entail:

1. Side-Channel Attack : Stealing information indirectly by analyzing electrical emissions, power consumption, or radiation from devices. It is typically used to extract cryptographic keys.
2. Rowhammer Attack : Exploiting a vulnerability in modern DRAM by repeatedly "hammering" memory cells so that neighbouring bits change, allowing for privilege escalation in the system.
3. Eavesdropping Attack : Interception of data transmitted between devices, for example, stealing card numbers or passwords through unsecured networks or with skimmer devices.
4. Modification Attack : The attacker alters the normal operation of the device by injecting malware or exploiting vulnerabilities, allowing them to perform man-in-the middle attacks and modify data.
5. Triggering Fault Attack : An attacker deliberately induces a fault in the hardware for the system to behave unexpectedly and expose security vulnerabilities.

CHAPTER III
PROBLEM ANALYSIS

III.1 Relationship between IC Supply Chain and Hardware Attacks.

The IC supply chain is a lengthy process involving many parties from design, fabrication, testing, integration, to disposal. This complexity means that each stage has its own potential attack.

1. Desain Phase

   IC architecture is designed using EDA tools and integration of IP cores from third-party vendors. At this stage, the design can be a target for theft (IP theft) or the insertion of hidden hardware trojans within the IP core or design software.

2. Fabrication Phase

   The IC design that has been completed is produced in semiconductor factories into physical chips. As fabrication is often carried out by third parties abroad, there is a risk of overproduction which is then sold illegally, as well as the circulation of counterfeit chips that appear genuine but are of poor quality and dangerous.

3. Testing and Integration Phase

   The IC that has been produced is tested for functionality before being installed in systems such as servers or IoT devices. This stage is also risky because malicious additional chips could be inserted, such as in the Supermicro Hack (2018) case where tiny chips were embedded on motherboards to create a backdoor.

4. Operation Phase

   ICs are used in real devices and start interacting with both software and users. At this stage, threats arise such as side-channel attacks that analyse power

consumption or electromagnetic emissions to steal confidential information, as well as physical attacks in the form of chip modification or fault injection.

5. Recycling / Disposal Phase

   This is where leftover chips may be polished and sold again. It is also possible to analyze used integrated circuits to steal internal designs or contribute to the black market's trafficking of fake chips. This demonstrates that ICs are susceptible to malevolent attacks long after their life cycle is over.

   Thus, every phase of the IC supply chain has vulnerabilities that can be exploited by attackers. Hardware security must not only be considered when the chip is used, but must also be maintained from the design stage to disposal.

III.2 Handling Hardware Attacks in the Supply Chain

Efforts to address hardware attacks in the IC supply chain must be carried out comprehensively, taking into account each stage.

1. Desain Phase

   An important step that can be applied is to ensure the use of IP cores from trustworthy vendors, as well as to implement techniques such as logic locking and obfuscation to make the design difficult to modify or steal. Thorough validation of EDA software tools is also necessary to prevent the insertion of trojans from the design phase.

2. Fabrication Phase

   One effective method is split manufacturing, which involves dividing the production process across several different locations so that no single factory dominates the entire design. In addition, the application of Physical Unclonable Functions (PUFs) can help distinguish original chips from counterfeit chips, making the circulation of counterfeit hardware more difficult.

3. Testing and Integration Phase

   The use of hardware attestation mechanisms is crucial for verifying the authenticity of the chips used. Physical tampering detection can be carried out with tamper detection, allowing any attempts to infiltrate additional chips to be identified immediately. Third-party supply chain audits are also an important step in maintaining transparency and security.

4. Operation Phase

   Protection can be achieved by implementing cryptographic algorithms that are resistant to side-channel attacks, for example through masking or blinding techniques. In addition, secure boot can ensure that only trusted firmware can be executed on the hardware. Real-time monitoring of chip behaviour also helps to detect the presence of suspicious anomalous activity.

5. Recycling / Disposal Phase

   Security can be strengthened with data sanitisation procedures to remove all sensitive information before chips are reprocessed. The circulation of used chips must also be monitored through official certification to prevent them from re-entering the market as counterfeit hardware.

CHAPTER IV
CONCLUSION AND SUGGESTIONS

IV.1 Conclusion

In addition to software security, hardware security is crucial, as flaws in physical components such as integrated circuits (ICs) can seriously jeopardize system integrity, privacy, and national security. Every step of the IC supply chain, from design and production to operation and disposal, poses different security risks and possible attack surfaces because of its complexity and worldwide reach. Comprehensive mitigation solutions, such as trusted IP sourcing, split manufacturing, hardware attestation, secure cryptography approaches, and supply chain transparency, are necessary to counter common hardware assaults such side-channel analysis, chip tampering, and fault injection. In the end, enhancing software defenses in addition to hardware security is crucial to guaranteeing the dependability, resilience, and general dependability of contemporary electronic systems.

IV.2 Suggestion

To enhance hardware security effectively, it is recommended to implement comprehensive measures across all stages of the integrated circuit supply chain, including adopting trusted IP cores and advanced design protection techniques such as logic locking during the design phase, applying split manufacturing and Physical Unclonable Functions (PUFs) in fabrication to prevent counterfeit chips, enforcing rigorous hardware attestation and tamper detection in testing and integration, utilizing cryptographic protections, secure boot, and continuous monitoring during operation, and ensuring thorough data sanitization and official certification in the recycling and disposal phase; additionally, promoting supply chain transparency, conducting regular third-party audits, and aligning hardware security practices with software security standards are essential steps to reduce vulnerabilities and strengthen overall system resilience.

BIBILIOGRAPHY

[1] IPQI. (2025, July 26). Pengertian Integrated Circuit (IC) dan Cara Kerjanya Terlengkap. Elektronikindo.com. https://elektronikindo.com/pengertian-integrated-circuit-ic/

[2] Maragkou, S., Rappel, L., Sauter, T., Jantsch, A., & Dettmer, H. (2025, April 16). The Pains of Hardware Security: An assessment model of Real-World hardware security attacks. IEEE Journals & Magazine | IEEE Xplore. https://share.google/ZA860XQOnFVH671La

[3] Rexy. (2024, March 8). Mengenal 5 tahapan siklus manajemen rantai pasok (Supply chain Management) - IPQI. IPQI. https://ipqi.org/mengenal-5-tahapan-siklus-manajemen-rantai-pasok-supply-chain-management/

[4] Yasar, K. (2022, June 28). Definition Hardware Security. TechTarget. https://www.techtarget.com/searchitoperations/definition/hardware-security