



HARDWARE SECURITY STANDARDS COMMITTEE (HSSC)
IEEE CIRCUITS AND SYSTEMS SOCIETY STANDARDS ACTIVITIES SUBDIVISION

HARDWARE SECURITY ATTACK LANDSCAPE AND COUNTERMEASURES

Authored by

N. Nalla Anandakumar, *HSSC Secretary and Continental Automotive, Singapore*

Marcus Janke, *HSSC Vice-Chair and Infineon Technologies AG, Germany*

Johann Knechtel, *New York University, Abu Dhabi*

Itamar Levi, *Bar-Ilan University, EnICs Labs, Israel*

Xiaojin Zhao, *Shenzhen University, China*

Kwen-Siong Chong, *Zero-Error Systems Pte Ltd., Singapore*

Selçuk Köse, *University of Rochester, United States*

Bah-Hwee Gwee, *Nanyang Technological University, Singapore*

John Chang, *JMEMTEK, Taiwan*

Lo Paul, *JMEMTEK, Taiwan*

Yi Wang, *HSSC Chair and Continental Automotive, Singapore*

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to the Hardware Security Committee of the IEEE Standards Association, the IEEE Circuits and Systems Society Standards Activities Subdivision, the TAB Committee on Standards Seed Funding, and the Hardware Security Attack Landscape and Requirements Framework Study Group for their support in the successful completion of this IEEE SA white paper. Special thanks go to Tom Thompson and Catherine Berger of the IEEE Standards Association for their invaluable guidance throughout this effort.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 19 November 2024. Printed in the United States of America.

PDF: STDVA27470 979-8-8557-1440-1

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at: <http://standards.ieee.org>.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA DOCUMENTS

This IEEE Standards Association (“IEEE SA”) publication (“Work”) is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable and reviewed by members of the activity that produced this Work. IEEE and the Hardware Security Attack Landscape and Requirements Framework Study Group expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the Hardware Security Attack Landscape and Requirements Framework Study Group disclaim any and all conditions relating to: results; and workmanlike effort. This document is supplied “AS IS” and “WITH ALL FAULTS.”

Although the Hardware Security Attack Landscape and Requirements Framework Study Group members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE SA OR Hardware Security Attack Landscape and Requirements Framework Study Group MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the Hardware Security Attack Landscape and Requirements Framework Study Group members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

ABSTRACT	6
1. INTRODUCTION.....	7
1.1. THE IMPORTANCE OF HARDWARE SECURITY	7
1.2. TYPES OF HARDWARE ATTACKS	7
TABLE 1 TYPES OF HARDWARE ATTACKS	8
1.3. OUTLOOK: IMPERATIVE FOR STANDARDS IN HARDWARE SECURITY— BRIDGING THE GAP	8
1.3.1. OVERVIEW	8
1.3.2. LOGICAL ATTACKS	8
1.3.3. OBSERVATIVE ATTACKS	9
1.3.4. FAULT-INJECTIVE/MANIPULATIVE ATTACKS	9
1.3.5. COMBINED ATTACKS	9
1.3.6. NEED FOR COMPREHENSIVE METRICS.....	10
2. LOGICAL ATTACKS.....	10
2.1. OVERVIEW	10
2.2. ATTACK SCENARIOS	11
2.2.1. COMMON ATTACKS ON DATA PROCESSING	11
2.2.2. ATTACKS ON MODERN CHIPLET SYSTEMS	11
2.2.3. REVERSE ENGINEERING AND PIRACY OF HARDWARE IP	12
2.2.4. HARDWARE TROJANS.....	12
2.3. COUNTERMEASURES.....	12
2.3.1. SECURING DATA PROCESSING.....	12
2.3.2. SECURING OF HARDWARE DESIGN	13
3. OBSERVATIVE ATTACKS AND COUNTERMEASURES.....	15
3.1. OVERVIEW	15
3.2. OBSERVATIVE ATTACKS.....	15
3.2.1. OVERVIEW	15
3.2.2. POWER ANALYSIS ATTACKS.....	15
3.2.3. TIMING ATTACKS	15
3.2.4. CACHE ATTACKS	16
3.2.5. ELECTROMAGNETIC ATTACKS	16
3.2.6. ACOUSTIC, THERMAL, AND OPTICAL ATTACKS	17
3.3. OBSERVATIVE ATTACK COUNTERMEASURES	17
3.3.1. OVERVIEW	17
3.3.2. AGAINST POWER ANALYSIS ATTACKS	17
3.3.3. AGAINST TIMING ATTACKS.....	18
3.3.4. AGAINST CACHE ATTACKS	18
3.3.5. AGAINST ELECTROMAGNETIC (EM) ATTACKS	18
3.3.6. AGAINST ACOUSTIC, THERMAL, AND OPTICAL ATTACKS	18
3.3.7. OTHER COUNTERMEASURES	19
4. FAULT INJECTION ATTACK	19
4.1. OVERVIEW	19
4.2. TYPES OF FAULT INJECTION ATTACKS	20
4.2.1. OVERVIEW	20
4.2.2. PHYSICAL FAULT INJECTION	20

4.2.3.	SOFTWARE FAULT INJECTION	21
4.3.	COUNTERMEASURES.....	21
4.3.1.	OVERVIEW	21
4.3.2.	HARDWARE-BASED COUNTERMEASURES.....	21
4.3.3.	SOFTWARE-BASED COUNTERMEASURES	22
4.3.4.	HYBRID APPROACHES.....	22
5.	MANIPULATIVE ATTACKS AND HARDWARE REVERSE ENGINEERING: THREATS AND COUNTERMEASURES	23
5.1.	OVERVIEW	23
5.2.	MANIPULATIVE ATTACKS	23
5.2.1.	OVERVIEW	23
5.2.2.	TECHNIQUES.....	23
5.2.3.	EXAMPLE SCENARIOS	24
5.3.	HARDWARE REVERSE ENGINEERING.....	24
5.3.1.	OVERVIEW	24
FIGURE 1	IC IMAGE ANALYSIS IS THE KEY STEP OF IC CIRCUIT EXTRACTION	24
5.3.2.	TECHNIQUES.....	24
5.3.3.	NETLIST GENERATION	24
5.4.	COUNTERMEASURES AGAINST SCAS AND HRE.....	25
6.	SECURITY RATING	26
6.1.	OVERVIEW	26
6.2.	METHODOLOGY OF SECURITY RATING	26
FIGURE 2	SPIDER DIAGRAM FOR SECURITY RATING	27
6.3.	ILLUSTRATIVE EXAMPLE AND OUTLOOK	27
TABLE 2	SECURITY RATING	28
7.	REFERENCES.....	29

HARDWARE SECURITY ATTACK LANDSCAPE AND COUNTERMEASURES

ABSTRACT

An overview is given of attacks on hardware security by introducing the four attack classes: logical attacks, physical observative attacks, physical fault injection attacks, and physical manipulative attacks. Descriptions and examples are given for each class of attack. Additionally, typical countermeasures for products to prevent successful attacks are listed and explained. Thereby, an introduction to hardware security is given as well as information shared for advanced readers. A methodology is suggested for a rating scheme on the countermeasures to allow easier product selection for given use cases and applications. Finally, the definitions of related rating tables are identified.

1. INTRODUCTION

1.1. THE IMPORTANCE OF HARDWARE SECURITY

Hardware security is not new and has long been a concern for mitigating security risks in electric/electronic (E/E) systems. *E/E systems* are generally defined as systems with one or more E/E components/devices/building blocks, including all E/E elements such as power supplies, interface circuits, control circuits, processing units, memories, sensors, etc. *Security risks of E/E systems* generally refer to the concerns surrounding *security and privacy threats*, which are unauthorized access to hardware information/specification/database, intellectual property (IP), or any confidential information (e.g., proprietary product information or users' information). The undesirable results of these threats could be the risk of IP theft (e.g., tangible IP assets are stolen), reduced reputation (e.g., reputation damage due to the system failure or security leakage), counterfeiting (e.g., unguaranteed quality of the hardware), and overbuilding (e.g., unfair competition due to the hardware reproduction without any rightful permission). In the worst case, these threats could jeopardize national security, disrupt critical infrastructures, or lead to safety/life-threatening issues. With the advancement of semiconductor technology such that E/E systems often embody complex integrated circuits (ICs)/system-on-chips (SoCs) having millions (if not billions) of transistors, the detection of the security risks (i.e., hardware attacks) and the associated evaluation of the hardware attack countermeasures are becoming increasingly challenging. In short, it becomes important to rank/qualify hardware security under various hardware attacks and the influence of various hardware attack countermeasures.

1.2. TYPES OF HARDWARE ATTACKS

In this white paper, the types of hardware attacks are categorized according to the nature of how the attacks are handled and observed from the hardware. These attacks are logical attacks, observative attacks, fault-injection attacks, and manipulative attacks. TABLE 1 briefly summarizes these attacks. In general, logical attacks are the least invasive to the hardware, followed by observative attacks, fault-injection attacks, and manipulative attacks are the most invasive. In terms of hardware tempering, logical attacks require the least tampering effort, whereas manipulating attacks require the most tampering effort. Regarding software configuration, logical attacks require the most effort, whereas manipulating attacks require the least effort. Combining attacks by collectively adopting more than one type of attack is possible and increases the likelihood of a successful attack on hardware.

TABLE 1 TYPES OF HARDWARE ATTACKS

Attacks	Definition	Hardware treatment	Hardware-tamper	Software-config
Logical	Attacks on logical data by exploiting algorithmic/computational/data flow weaknesses through communication interfaces/remote protocols, as well as protocol misuse such as buffer overflow, rowhammer, denial of service, unauthorized debugging, etc.	Non-invasive	Less tampering	More config
Observative	Attacks on parametric variations by observing/leveraging side-channel leakages such as power consumption and emissions (electromagnetic, thermal, photonic, radio frequency [RF], and radiation) to glean sensitive information.			
Fault-injection	Attacks by injecting faults/errors/noises to analyze the abnormal characteristics/operations to decipher the sensitive information.			
Manipulative	Attacks by directly manipulating the hardware such as micro-probing, sample-preparation, reverse-engineering, etc.			

1.3. OUTLOOK: IMPERATIVE FOR STANDARDS IN HARDWARE SECURITY—BRIDGING THE GAP

1.3.1. OVERVIEW

The hardware security domain is rapidly evolving, with an ever-expanding array of attack vectors and vulnerabilities emerging. While research communities and industry practitioners actively develop attacks and countermeasures, the current landscape of standards and evaluation methodologies lacks comprehensive protection. This gap poses a significant challenge to the widespread adoption of secure hardware practices, particularly with increasingly sophisticated and diverse threats. The classification of application type, environment, and adversarial abilities is crucial to defining such standards and methodologies per setting.

1.3.2. LOGICAL ATTACKS

While some existing standards like IEEE Std 1149.1™ [5]¹ provide guidelines for secure debug access, they may not comprehensively address vulnerabilities arising from protocol misuse, implementation flaws, and combinations with physical attacks. Developing standards that enforce secure coding practices, input validation, and access control mechanisms is imperative to mitigate these risks, considering hardware security as a whole and various attacker modalities and threat models.

¹The numbers in brackets correspond to those of the references in Section 7.

1.3.3. OBSERVATIVE ATTACKS

Observative attacks pose a serious threat to hardware security, as witnessed by NIST requirements for lightweight cryptography standardization for secure symmetric primitives and asymmetric post-quantum cryptography (PQC) designs with similar concerns (NIST IR 4813 [11]). While standards like ISO/IEC 17825 and FIPS 140-3 address some aspects of side-channel analysis, they often focus on specific cryptographic implementations and may not encompass the full spectrum of side-channel vulnerabilities, different primitives, architectural aspects, etc. Although standards like IEC 62132 and ISO/IEC 10373-1 (e.g., see Chacon et al. [3]) provide guidelines for electromagnetic compatibility (EMC) or EMI standards and testing, they primarily focus on ensuring functional integrity rather than protecting against information leakage.

1.3.4. FAULT-INJECTIVE/MANIPULATIVE ATTACKS

While standards like ISO/IEC 27001 and NIST SP 800-53 address physical security measures at the system level, they may not provide sufficient guidance on protecting individual hardware components from unauthorized access and modification. The development of standards for secure chip design, tamper-resistant packaging (Katz, Avital, and Levi [6]), and supply chain integrity is vital to counter these threats, along with protocol/mathematical-level solutions. These typically hold some assumption on the hardware and demands for hardware-level protection of some assets such as key readout, memory handling, flash handling, side-channel-attack (SCA), fault-injection protection of certain macros, etc. However, most requirements need to be better standardized.

1.3.5. COMBINED ATTACKS

The convergence of logical, observative, fault injection, and manipulative attacks necessitates the development of improved security practices and protocols. The underlying principles are to make the security practices and protocols more reliable, robust, and resilient. The reliability could be improved by implementing the design concepts of *roots of trust*, e.g., having reliable encryption and authentication processes, secure boot, secure memory, key generation, etc. The robustness could be improved by introducing good security attack countermeasures that are resistant to various attacks. The resiliency could be improved by introducing anti-tampering/redundancy measures that quickly respond to various attacks. The existing standards may not adequately address the interaction among logical vulnerabilities, side-channels, faults, and their interplay under active and manipulative adversaries. The development of standards that explicitly consider these combined

attacks and provide guidelines for designing and evaluating the improved security practices and protocols is crucial for hardware security—backed by reliability, robustness, and resiliency.

1.3.6. NEED FOR COMPREHENSIVE METRICS

To evaluate the effectiveness of security countermeasures and compare different solutions, robust and comprehensive metrics are essential. Existing metrics like side-channel leakage assessment and fault injection resistance evaluation offer valuable insights but may need to fully capture the interplay between various attack vectors, architectural aspects, SoC level, electromagnetic (EM), and RF interactions, etc. The development of new metrics that consider the full spectrum of hardware threats and provide a holistic assessment of security is a critical area for future research and advancement for secure hardware.

The ever-evolving landscape of hardware security demands a proactive approach to developing and updating standards and evaluation methodologies. This includes developing standards that explicitly consider the interplay between different attack vectors. We can strengthen the security of hardware systems and stay ahead in the ongoing battle against cyber threats by:

- Incorporating advanced testing and evaluation methods, including machine learning-based analysis
- Promoting collaboration between academia, industry, and standardization bodies to share knowledge and best practices
- Fostering the development of new metrics that provide a holistic assessment of hardware security

2. LOGICAL ATTACKS

2.1. OVERVIEW

The confidentiality, integrity, and availability (CIA) paradigm of data processing within electronic systems is challenged by various logical attacks, like unauthorized access to data through debug ports. Such attacks are conducted mainly at the software level and often exploit the interconnected nature of modern systems. There are also attacks on hardware design, such as reverse engineering (RE) and piracy of the chip design's intellectual property (IP). These threats arise due to the globalized nature of electronics supply chains. Note that these attacks can be considered logical attacks, as they target the data of the hardware internals.