International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 119-127, January-2024

https://doi.org/10.47001/IRJIET/2024.801016

Hardware Security and Trust: Trends, Challenges, and Design Tools

S.M.D.N.Siriwardana

Fellow, IEEE, Undergraduate in Cyber Security, Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka
E-mail: deemanthanayanajith1@gmail.com

***Abstract* - Hardware security in the cyber security domain had become a more of a controversial topic over the past decade due to the introduction of new design technologies in semiconductors and expansion of global supplier chains. In proportion to the technological advancement of hardware production, the success rate of the existing hardware attacks had also evolved over the time with a significantly high rate of emergence of new attacking techniques and methods. Computing hardware is becoming a more and more attractive attack surface due to several reasons. The technology of analyzing the hardware components is becoming more and more affordable and accessible to the general public than before. Also due to the influx of IoT devices in the market, trend of simplifying the design structure to decrease the power consumption and maximizing the processing speed has become the theme of modern hardware implementations rather than the security of the devices. When considering the market demand and user requirements, it is more obvious for the computer manufacturers to give priority to user requirements rather than stressing more on the security aspects of their designs and devices. But there could be some catastrophic outcomes if the security aspects of these hardware tends to fail in a critical infrastructure, because these semiconductors are used in devices ranging from simple IoT devices to more complex systems like SCADA systems. Therefore, it is always a better approach to find a balance ground between the user requirement as well as the security of the hardware, without compromising either of both in the design and development. In this article, it presents an overall insight to trends in Hardware Security domain, specifically related to modern computer hardware design and manufacturing processes, distribution, usage, their disposal and recycling. These various stages are analyzed under Three main objectives of exposing the threats to computer hardware, suggesting countermeasures to minimize or eliminate those threats and discussing about the utilization of various design tools that can assist in the way to securing these computer hardware systems in their day-to-day applications.**

Keywords: Hardware Security, Threats, Countermeasures, Design Tools, Hardware Attacks, Root of Trust.

I. INTRODUCTION

The design and development stages, but not limited to those Ardware security threats are mostly inherited at the stages as well. Security flows can arise at any of the phases in the life cycle of semiconductors, which starts from the requirement analysis, requirement elicitation, designing, prototyping, development, testing, fabrication, distribution, application, disposal and recycling. The awareness about the possibility of a successful large-scale catastrophic hardware attack was taken for granted up until the Stuxnet malware triggered on Programmable Logic Controllers (PLCs) in Supervisory Control and Data Acquisition (SCADA) systems used in the Iranian Nuclear Program by exploiting a hardware vulnerability which was inherited by the manufacturer's at the design stages of these specific PLCs [1], [2]. Following the Stuxnet malware, Mirai Botnet was the next major catastrophic occurrence of a hardware security breach, which was calculated for having a botnet capable of generating 1 Tbps traffic with use of over 150 000 infected IP cameras [3], [4], [5].

There can be a misconception among the people that these attacks are only applicable to outdated hardware systems. But the reality is that most of the modern hardware systems are more vulnerable and highly likely to leak confidential data than the older ones due to the manufactures' are keen on focusing the functionality and forgetting about the security verifications of their products. The best example is that the RISC-V processor – BOOM v3 (Berkeley Out-of-Order Machine) which claims to have mitigated the Meltdown vulnerability in their product was found to be still vulnerable and could be exploited under 3.9 milliseconds [6].

With the booming market for IoT devices in the today's world, key theme of IoT hardware manufacturers is to reduce the size of the hardware components while increasing the interoperability factor of the IoT components with other hardware consoles. Due to these two major focus point, the security of the hardware components has to be sacrificed to certain extends at most of the times. Even though there are IoT security standards like ISO/IEC JTC, IEEE-SA, ITU-T, IETF, oneM2M and OCF, the device manufactures and developers

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 1, pp 119-127, January-2024
https://doi.org/10.47001/IRJIET/2024.801016

tend to deviate from these guidelines due to several reasons like inability for producing fully automated IoT systems with selfadaptive capabilities while adhering to the standards and also due to constriction and hindrances to data accessibility and data transmissibility by these standards' guidelines [7]. The most disturbing factor is that even if these IoT hardware systems are manufactured with the certified standards, the vulnerabilities inherited by them due to their design simplicity cannot be avoided. Studies conducted on the side-channel information leakage on Arm Platform Security Architecture (PSA) Level 2 certified chips also revealed that these IoT chips are leaking electromagnetic traces of AES encryption process with the accuracy of 8-bits out of a 16-bit encryption key [8]. Due to these reasons, the present domain of hardware security is searching for more comprehensive, relatable and practical approaches in addressing the security of hardware devices while still maintaining their usability and performance.

In this article, above efforts are evaluated under 4 major sections as hardware security properties in Section II, hardware security threats in Section III, countermeasures in Section IV and hardware security tools in Section V. Section VI summarizes the potential future research areas. Finally, conclusion about the article is presented in Section VII.

II. HARDWARE SECURITY PROPERTIES

Hardware based security threats are carried out by violating the hardware security properties. Therefore implementing the unused security properties and enforcing them in more strict ways can provide a level of assurance about the security of the hardware component. Since it is hard to define specific security properties in single, for each and every hardware component of circuitry and also obviously impossible, it is more practical to define a common set of security properties which can be adhered by all types of hardware components according to their use-cases.

A) Confidentiality, Integrity and Availability

These are the three fundamental security properties in the computer security domain and it remains trues and same for hardware security domain as well. In hardware context, these terms are defined to be more cleared according to the context. Confidentiality is the state of inability to obtain, infer or predict the secret information by observing or analyzing a public output or a memory location. Even though it is more easy to identify the direct leakages of sensitive information, the indirect leakage of information from side channels cannot be spotted directly or easily. This can be taken in advantage in covert side channel attacks such as thermal side-channel attacks [9], electromagnetic side-channel analysis [10] targeting the cryptographic cores, processors, microprocessors [11] and cache registers [12].

Integrity is the inability to overwrite a trusted data object by an untrusted entity. Integrity violations by exploiting memory corruption vulnerabilities in the system components can facilitate VTable reuse attacks which can be the first step of performing further malicious outcomes [13].

Availability is defined as maximum time period that a system is capable of operating and serving its intended function. Fault injection attacks specifically targeted on smart grids in order to induce sequential power outages in the main grid or trip selected branches of a grid [14] is an example of a denial of service (DOS) attack which affects the availability property in a system.

B) Reliability

Reliability is defined as the ability to output the desired functional results under normal operations and also under slight fluctuations in the operational environment for a specific period of time. Reliability is one of the most important properties in computer hardware manufacturing for critical systems such as military grade versions of electronic components [15], firefighting equipment [16] and space command control platforms [17] to ensure that they operate in harsh environmental conditions and circumstances.

C) Isolation

Isolation for computer hardware component can be defined as the separation or avoidance of two individual hardware components with different levels of security being directly communicating with each other. This is considered as one of the most common security properties that should be implemented specially on processors embedded in IoT devices in order to prevent information leakage when they are communicating with nearby devices [18].

D) Constant Time

This property suggests that a certain hardware component taking an invariant time for processing an input and producing an output, irrelevant of the input combinations provided to it. This is most important in preventing timing channel attacks. But in practicality, this is very hard to achieve due to performance optimization reasons and also due to technologies like On-Demand Branch Prediction (ODBP) and Path-based On-Demand Branch Prediction (ODBP-PATH) technologies [19]. and fast path calculations in arithmetic units.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 119-127, January-2024

https://doi.org/10.47001/IRJIET/2024.801016

E) Safety

Safety of the hardware components is defined from the perspective of the user. That means the ability of the hardware components to avoid catastrophic incidents and consequences and incident to the user and the surrounding environment is considered as the safety property of the computer hardware devices. Since this is a subjective and relative attribute, the measurement of this parameter also varies depending on the situation, industry and expectations of the provided output by the systems [20], [21], [22].

III. HARDWARE SECURITY THREATS

A) Architectural and System Threats

These are the threats that are inherent due to the design and implementation of the hardware component within the system architecture. These threats can be minimized at the designing and fabrication phases of the hardware lifecycle, but sometimes it can be inevitable to eliminate them completely due to the functionality expected by the hardware components and also due to some performance enhancing mechanisms used within the components. Secure boot attacks [23], [24], firmware attacks [25], [26], dynamic random access memory threats such as Row hammering attacks [27], [28], [29], cache attacks [30], [31], speculative execution attacks [32], [33], [34], [35] and code reuse attacks [36] are some examples for these types.

B) Covert and Side-Channel Threats

Covert channel is created between two parties to hide the traces of information exchange without other parties having clues about the information exchange happening between them. The channels used as covert channels are generally not meant for communications. Covert channel on Intel CPU-iGPU platform [34], cross-component covert channels on integrated CPU-GPU systems identified using the ring bus connecting CPU and GPU to the Last Level Cache (LLC) [35], conflict based cache covert channel exposed by reverse engineering cache behavior of PREFETCHNTA in Intel processors [36], covert channels created by exploiting vulnerabilities in current management mechanism in latest Intel processors [37] and covert channel exploitation of CVA6 RSC-V open-source CPU with the help of baremetal simulations [38] are some example works.

Side channel is more likely a backdoor to a system in which an attacker gains the chance of extracting secret information belonging to the victim, without the knowledge of the victim. Side channels exposed using electromagnetic emanations in power management unit of modern computers [39], physical side-channel attacks on Field Programmable Gate Arrays (FPGAs) [40] and cross-core cache side-channel vulnerability exploited in x86 Intel processor by exploiting the implementation weakness in PREFETCHW instruction [41] are some of the proven researches done in the side-channel attack domain.

C) Intellectual property Theft

There are several types of Intellectual Property (IP) rights granted to SoC and IC designs including patents, Register Transfer-Level (RTL), design (soft IP), physical layout (hard IP) and gate-level netlist (firm IP). For fabrication or mass production requirements of silicon microchips and Integrated Circuits (ICs), these IP rights are granted to third parties most of the times for manufacturers who are located at off shores. There is a risk involved in this process. That is, there could be a chance for IP counterfeiting, production and selling of the counterfeit versions of these microchips and ICs under the brand names of the original manufacturers and suppliers. These are called cloning attacks and they can endanger the security of critical infrastructure which uses these hardware items in their systems. In addition to the revenue loss and sabotage of the genuine vendor's reputation, these cloned hardware could affect the expected reliability, performance and security of critical systems such as health, military, aviation, transportation etc. and also could create backdoors and logics to violate confidentiality, integrity and availability of the information processed within these components as well.

D) Hardware Trojans

Hardware trojan (HT) is an intentionally and maliciously modified circuitry in a hardware component. Earlier versions of these hardware trojans used a single rare event in process execution to trigger the payload. But modern HTs uses multiple signals as their triggering event to ensure their execution within the system. There are several types of HTs depending on their intended malicious activity. Some of them are Classical digital trojans, HTs exploiting don't care conditions, Analog HTs and HTs inducing aging and performance degradation are some examples.

These HTs could be introduced to the legitimate circuits at their fabrication phases intentionally by rogue employees, rogue manufacturers or due to reasons like outsourcing electronic components from untrusted vendors and suppliers in the circuit fabrication phase. These HTs are most likely to easily infiltrate into secure infrastructure of government organizations, or critical systems when hardware accessories and components are ordered and purchased from untrusted suppliers. After infiltration, these HTs could act as backdoors to the systems used within the protected infrastructure and cause leakage of confidential information and sometimes

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 119-127, January-2024

https://doi.org/10.47001/IRJIET/2024.801016

causing destruction to the system components at extreme cases.

IV. COUNTERMEASURES

A) Hardware Security Primitives

True Random Number Generators (TRNGs) and Physical Unclonable Functions (PUFs) are most widely used hardware security primitives to withstand most of the vulnerabilities and threats targeting intrinsic hardware security. TRNG can be of two types as software or hardware-based components, in which the main functionality is to generate a sequence of unpredictable random numbers. TRNGs can be implemented by using various random parameters such as using perturbed states of NOR flash memory cells [45] and electrical noise [46]. Since the predictability of the generated output of TRNGs are extremely low and due to its true randomness, TRNGs can be used in cryptographic algorithms to increase the unpredictability and randomness in secure key generation. PUFs on the other hand, uses intrinsic fabrication process variations to generate unique unforgeable device fingerprints [47]. PUFs are of 3 types as User-device PUFs, Data-device PUFs and Event-driven PUFs. User-device PUFs perform use and device authentication using a message exchange function [48], [49]. Data-device PUFs perform data and device independent authentication mainly in the domain of digital forensics [50]. Event-driven PUFs are triggered by server provided challenges [51], [52].

B) Architectural and System Threat Countermeasures

For defense against architectural and system design flaws various protection techniques such as usage of trusted execution environments for local [53], remote [54] and IoT systems [55], cache side-channel mitigation techniques such as runtime detection [56] and concurrent randomization of processor frequency and prefetcher operation [57], memory protection techniques such as Combined Tag and Data Parity (CTDP) schemes [58] and control flow integrity verification techniques such as selective and random verification [59] can be used.

C) Side-channel Protection techniques

Side-channel attacks being the one of the most effective against extracting the encryption keys of RSA and AES like algorithms because these ciphers rely on heavy mathematical functions in key generation which cannot be cracked in feasible amount of time and resources under normal conditions. Since these ciphers are used in critical systems, these side-channel data leakages pose a huge threat to their operational security.

To minimize this risk, a technique which uses 3D CPU design is incorporated. In here caches and main memory are stacked vertically on top of the processor with the help of Through-Silicon Vias (TSVs) [60].

Power side-channel attacks can be minimized by using special power monitors (PwrMons) which separate the switching activity signals used in computing power estimations by eliminating the use of functions related to secret key, ciphertext and plaintext [61].

For mitigating electro-magnetic side-channel leakages, techniques such as on-chip clock network adjustments [62], using metal layers aided with higher-order multipoles in integrated Circuit (IC) designs [63], usage of Randomized Switching Successive Approximation Register (RS-SAR) with Analog to Digital Converters (ADCs) [64] and amplitude modulation of the load signal by converter capacitance acting as a carrier in Switched-capacitor (SC) dc-dc converters [65] are used.

Fault injection attacks are also a serious threat to cryptographic ICs. Hardware redundancy and signature analysis technique [66] is used in mitigating fault injection attacks in Trivium stream ciphers. To mitigate this vulnerability, Detection of fault injection attacks as compressed sensing problem as a result of sparsity of soft errors [67] is another technique used by other cryptographic ICs to eliminate the chances existence of fault injection vulnerabilities in them.

D) IP protection techniques

Hardware watermarking, hardware steganography and logic obfuscation like techniques are the most common industrial solutions in protecting IP rights in hardware designs. But modern IP violations can bypass this general IP protection mechanisms and therefore more complicated and secure solutions are introduced to the hardware designers and developers. Example for such techniques are LeGO framework [68], selective weight obfuscation with non-malicious backdoors [69], embedding the IP vendor's fingerprints (biometric data) into the hardware accelerator as a secret security constraint [70], dynamic digital compression coding [71], combining Split Manufacturing (SM) and Layout Camouflaging (LC) [72] and WATERMARCH technology which operates on authenticated obfuscation utilizing hash based message authentication code (HMAC) [73].

E) Hardware Trojan Detection and Prevention

Hardware Trojan (HT) detection countermeasures are categorized into several categories depending on at which stage these techniques is being enforced. These include Pre-

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 119-127, January-2024
https://doi.org/10.47001/IRJIET/2024.801016

silicon countermeasures, Post-silicon countermeasures, Design-for Security (DFS) techniques, Runtime monitoring techniques and HT prevention techniques. The most recent hardware trojan detection and prevention methods include techniques such as combination of thermal maps with inception neural networks [74], applying information theory technology and density based clustering algorithms called Density-Based Spatial Clustering of Applications with Noise (DBSCAN) for detecting trojan logics in the circuit [75], using chaos theory in hardware based runtime detection of HTs [76] and utilizing reconfigurable assertion checkers (RAC) for HT detection in System-On-Chip (SoC) [77].

V. HARDWARE SECURITY TOOLS

Hardware security tools can be categorized into 2 types as Security verification tools and Security driven hardware design tools. Security verification tools are used for verifying the security of hardware components which are already fabricated and available in the consumer market or to check the security aspect of a design before its fabrication. These tools can be either Academic tools of Commercial tools. Valkyrie [78] and BitMine [79] are examples for these types of tools. Security driven hardware design tools are the ones used in designing the hardware components. These include Computer-

Aided Designing (CAD) tools used for PCB and logic designing. In a research conducted by H. Ma, J. He, Y. Liu, L. Liu, Y. Zhao and Y. Jin [80] a novel approach in such automated CAD tool was developed in order to enhance the security of hardware components to withstand against electromagnetic side-channel attacks. Similar commercial tools are also available in the market and also these technologies are being constantly tested and researched to improve the flaw detection mechanisms and to minimize the error in order to increase the accuracy of vulnerability predictions.

VI. CONCLUSION

The hardware security domain is a constantly evolving and rapidly growing domain. With the expansion of consumer electronics markets along with IoT, cloud services, machine learning and artificial intelligent related products, the hardware production to run these services are also rapidly evolving. In this rapid production phase, most of the vendors tend to neglect the security aspects of these components since they focus more on increasing the capabilities and performance of these components. The hardware market trends in the current society are cramming dozens of capabilities and functionalities into a small compact hardware designs, making hardware components rich in wireless or physical connectivity or adding “Smartness” to these components. It’s rare that vendors consider about the security because the consumers itself are also not likely to worry too much on the security aspects, but they focus more on getting as much as performance, capabilities and connectivity features in their gadgets for the money they spend. Because of these reasons, the computer hardware market has become highly vulnerable to security threats like never before. In this paper, the current trends in hardware security threats, design tools, challenges and countermeasures are discussed in order to make a contribution to raise the awareness of the general public as well as the designers and the vendors to focus more on the security aspects of their hardware products as much as they are stressing about their capabilities and performances.

ACKNOWLEDGMENT

A thankful mentioning to my lecturer Dr. Pradeep Abeygunawardhana, Mr. Jaliya and Mrs. Nishadhi De Silva for continuously encouraging and providing support throughout preparing this article.

REFERENCES

[1] A.N. a. S. Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 2-13, 2018.

[2] R. T. X. G. Z. X. a. T. L. J. Tian, "Moving Target Defense Approach to Detecting Stuxnet-Like Attacks," IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 291-300, 2020.

[3] A.K. H. N. T. J. C. B. M. L. A. a. K. T. A. Borys, "An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet," in 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022.

[4] H. k. Idriss, "Mirai Botnet In Lebanon," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020.

[5] B. R. M. F. a. B. S. G. Gallopeni, "A Practical Analysis on Mirai Botnet Traffic," in 2020 IFIP Networking Conference (Networking), Paris, France.

[6] Y. -P. S. Y. -R. C. Y. -T. C. a. S. -J. C. C. -H. Lin, "Empirical Study of Proposed Meltdown Attack Implementation on BOOM v3," in 2022 IEEE 65th International Midwest Symposium on Circuits and Systems (MWSCAS), Fukuoka, Japan, 2022.

[7] Y. -D. S. S. -R. O. a. Y. -G. K. E. Lee, "A Survey on Standards for Interoperability and Security in the Internet of Things," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1020-1047, 2021.

[8] D. L. J. L. V. C. M. L. S. L. a. J. F. F. Chen, "Arm PSA-Certified IoT Chip Security: A Case Study,"

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 119-127, January-2024
https://doi.org/10.47001/IRJIET/2024.801016

Tsinghua Science and Technology, vol. 28, no. 2, pp. 244-257, 2022.

[9] T. K. a. Y. Shin, "Thermal Bleed: A Practical Thermal Side-Channel Attack," IEEE Access, vol. 10, no. 1, pp. 25718-25731, 2022.

[10] M. P. a. A. Z. B. B. Yilmaz, "Electromagnetic Side Channel Information Leakage Created by Execution of Series of Instructions in a Computer Processor," IEEE Transactions on Information Forensics and Security, vol. 15, no. 1, pp. 776-789, 2020.

[11] V. F. P. A. K. C. a. E. S. K. Dhananjay, "High Bandwidth Thermal Covert Channel in 3-D-Integrated Multicore Processors," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 11, pp. 1654-1667, 2022.

[12] N. M. W. X. S. K. a. J. S. S. Deng, "Evaluation of Cache Attacks on Arm Processors and Secure Caches," IEEE Transactions on Computers, vol. 71, no. 9, pp. 2248-2262, 2022.

[13] B. C. Y. L. a. H. W. C. Wang, "Layered Object-Oriented Programming: Advanced VTable Reuse Attacks on Binary-Level Defense," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 693-708, 2019.

[14] X. L. Z. L. a. Y. W. L. Che, "False Data Injection Attacks Induced Sequential Outages in Power Systems," IEEE Transactions on Power Systems, vol. 34, no. 2, pp. 1513-1523, 2019.

[15] H. U. A. K. a. N. C. S. N. B. Gaikwad, "The Internet-of-Battlefield Things (IoBT)-Based Enemy Localization Using Soldiers Location and Gunshot Direction," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11725-11734, 2020.

[16] F. S. B. P. D. G.-C. A. V. D. B. T. V. R. D. J. S. Q. Vey, "POUCET: A Multi-Technology Indoor Positioning Solution for Firefighters and Soldiers," in 2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Lloret de Mar, Spain, 2021.

[17] L. X. F. Z. J. Z. M. L. Y. L. K. H. Y. L. N. Xiao, "An Architecture of Cross-Domain Support System for Multiple Space Command and Control Platforms," in 2021 IEEE Aerospace Conference (50100), Big Sky, MT, USA, 2021.

[18] M. Y. a. S. W. N. Hu, "Surviving Information Leakage Hardware Trojan Attacks Using Hardware Isolation," IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, pp. 253-261, 2019.

[19] S. H. E. A. A. B. T. M. A. a. W. J. D. M. Mohammadi, "Energy Efficient On-Demand Dynamic Branch Prediction Models," IEEE Transactions on Computers, vol. 69, no. 3, pp. 453-465, 2020.

[20] P. S. a. L. K. Singh, "Reliability and Safety Engineering for Safety Critical Systems: An Interview Study With Industry Practitioners," IEEE Transactions on Reliability, vol. 70, no. 2, pp. 643-653, 2021.

[21] F. A. Y. I. O. A. Y. S. O. A. a. O. O. H. Ahangari, "Analysis of Design Parameters in Safety-Critical Computers," IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 3, pp. 712-723, 2020.

[22] C. -Y. C. M. H. S. L. S. M. a. M. C. F. Abdi, "Preserving Physical Safety Under Cyber Attacks," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6285-6300, 2019.

[23] H. T. Q. M. A. M. a. S. E. A. Vasselle, "Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot-Extended Version," IEEE Transactions on Computers, vol. 69, no. 10, pp. 1449-1459, 2020.

[24] J. -Y. P. D. -G. H. a. S. B. Y. -S. Won, "Practical Cold boot attack on IoT device - Case study on Raspberry Pi -," in 2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), Singapore, 2020.

[25] K. N. R. C. G. P. D. a. G. P. K. A. Adithyan, "Reverse Engineering and Backdooring Router Firmwares," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020.

[26] L. L. Y. Z. B. P. a. X. F. C. Gao, "Microcontroller Based IoT System Firmware Security: Case Studies," in 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 2019.

[27] O. M. a. J. S. Kim, "RowHammer: A Retrospective," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 8, pp. 1555-1571, 2020.

[28] Y. C. D. L. S. N. Z. W. a. Y. Y. Z. Zhang, "PThammer: Cross-UserKernel-Boundary Rowhammer through Implicit Accesses," in 2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), Athens, Greece, 2020.

[29] A.P. F. a. O. K. L. P. Fraile, "Revisiting Rowhammer Attacks in Embedded Systems," in 2019 14th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS), Mykonos, Greece, 2019.

[30] M. B. a. H. Yun, "Memory-Aware Denial-of-Service Attacks on Shared Cache in Multicore Real-Time Systems," IEEE Transactions on Computers, vol. 71, no. 9, pp. 2351-2357, 2022.

[31] C. S. Y. a. B. P. P. Kumar, "DAMARU: A Denial-of-Service Attack on Randomized Last-Level Caches," IEEE Computer Architecture Letters, vol. 20, no. 2, pp. 138-141, 2021.

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 119-127, January-2024
https://doi.org/10.47001/IRJIET/2024.801016

[32] A.J. a. R. Davies, "Speculative Execution Attack Methodologies (SEAM): An overview and component modelling of Spectre, Meltdown and Foreshadow attack methods," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019.

[33] H. L. a. F. Y. M. H. Islam Chowdhuryy, "BranchSpec: Information Leakage Attacks Exploiting Speculative Branch Instruction Executions," in 2020 IEEE 38th International Conference on Computer Design (ICCD), Hartford, CT, USA, 2020.

[34] C. S. M. S. a. S. K. P. Aimoniotis, "Reorder Buffer Contention: A Forward Speculative Interference Attack for Speculation Invariant Instructions," IEEE Computer Architecture Letters, vol. 20, no. 2, pp. 162-165, 2021.

[35] S. C. Y. X. Y. Z. Z. L. a. T. H. L. G. Chen, "SgxPectre: Stealing Intel Secrets from SGX Enclaves Via Speculative Execution," in 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 2019.

[36] S. R. H. H. a. S. M. P. D. A. Dhavlle, "CR-Spectre: Defense-Aware ROP Injected Code-Reuse Based Dynamic Spectre," in 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), Antwerp, Belgium, 2022.

[37] J. K. a. Y. S. T. Kim, "Constructing Covert Channel on Intel CPUiGPU platform," in 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea (South), 2021.

[38] H. N. N. A.-G. A. M. a. K. B. S. B. Dutta, "Leaky Buddies: Cross Component Covert Channels on Integrated CPU-GPU Systems," in 2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture (ISCA),, Valencia, Spain, 2021.

[39] X. X. Y. Z. a. J. Y. Y. Guo, "Leaky Way: A Conflict-Based Cache Covert Channel Bypassing Set Associativity," in 2022 55th IEEE/ACM International Symposium on Microarchitecture (MICRO), Chicago, IL, USA, 2022.

[40] L. O. J. S. K. J. G. L. A. G. Y. M. A. I. P. O. M. J. Haj-Yahya, "IChannels: Exploiting Current Management Mechanisms to Create Covert Channels in Modern Processors," in 2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture (ISCA), Valencia, Spain, 2021.

[41] Y. T. B. A. a. R. L. V. Martinoli, "Recovering Information on the CVA6 RISC-V CPU with a Baremetal Micro-Architectural Covert Channel," in 2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS), Torino, Italy, 2022.

[42] B. B. Y. A. Z. a. M. P. N. Sehatbakhsh, "A New Side-Channel Vulnerability on Modern Computers by Exploiting Electromagnetic Emanations from the Power Management Unit," in 2020 IEEE International Symposium on High Performance Computer Architecture (HPCA), San Diego, CA, USA, 2020.

[43] S. S. M. a. M. Stojilović, "Physical Side-Channel Attacks and Covert Communication on FPGAs: A Survey," in 2019 29th International Conference on Field Programmable Logic and Applications (FPL), Barcelona, Spain, 2019.

[44] A.Z. Y. Z. a. J. Y. Y. Guo, "Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks," in 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022.

[45] B. R. a. A. M. P. Poudel, "Microcontroller TRNGs Using Perturbed States of NOR Flash Memory Cells," IEEE Transactions on Computers, vol. 68, no. 2, pp. 307-313, 2019.

[46] J. Z. H. L. L. S. a. Y. W. L. Gong, "True Random Number Generators Using Electrical Noise," IEEE Access, vol. 7, no. 1, pp. 125796-125805, 2019.

[47] J. M. a. M. O'Neill, "Fast DRAM PUFs on Commodity Devices," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3566-3576, 2020.

[48] Z. L. a. Y. Guan, "RUDBA: Reusable User-Device Biometric Authentication Scheme for Multi-service Systems," in 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Tysons Corner, VA, USA, 2021.

[49] Y. C. a. C. -H. C. Y. Zheng, "UDhashing: Physical Unclonable Function-Based User-Device Hash for Endpoint Authentication," IEEE Transactions on Industrial Electronics, vol. 66, no. 12, pp. 9559-9570, 2019.

[50] Y. C. a. C. -H. C. Y. Zheng, "A PUF-Based Data-Device Hash for Tampered Image Detection and Source Camera Identification," IEEE Transactions on Information Forensics and Security, vol. 15, no. 1, pp. 620-634, 2019.

[51] Y. Z. a. C. -H. C. J. X. Soo, "Live Demonstration: Event-Driven Physical Unclonable Function for Proactive Monitoring System by Dynamic Vision Sensor," in 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 2021.

[52] X. Z. T. S. Y. C. a. C. -H. C. Y. Zheng, "Ed-PUF: Event-Driven Physical Unclonable Function for Camera Authentication in Reactive Monitoring System," IEEE Transactions on Information Forensics and Security, vol. 15, no. 1, pp. 2824-2839, 2020.

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 119-127, January-2024
https://doi.org/10.47001/IRJIET/2024.801016

[53] C. D. R. S. M. S. K. D. N. A. T. K. S. C. -K. P. T. -T. Hoang, "Trusted Execution Environment Hardware by Isolated Heterogeneous Architecture for Key Scheduling," IEEE Access, vol. 10, no. 1, pp. 46014-46027, 2022.

[54] K. N. S. J. Y. C. a. Y. P. H. Oh, "MeetGo: A Trusted Execution Environment for Remote Applications on FPGA," IEEE Access, vol. 9, no. 1, pp. 51313-51324, 2021.

[55] C. C. P. L. X. X. X. G. S. Z. M. Y. T. J. L. Guan, "Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 438-453, 2019.

[56] H. S. A. S. S. R. a. H. H. H. Wang, "Hybrid-Shield: Accurate and Efficient Cross-Layer Countermeasure for Run-Time Detection and Mitigation of Cache-Based Side-Channel Attacks," in 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD), San Diego, CA, USA, 2020.

[57] H. S. T. M. L. Z. A. S. S. R. H. H. H. Wang, "Mitigating CacheBased Side-Channel Attacks through Randomization: A Comprehensive System and Architecture Level Analysis," in 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 2020.

[58] P. R. a. F. L. S. Liu, "Protection of Associative Memories Using Combined Tag and Data Parity (CTDP)," IEEE Transactions on Nanotechnology, vol. 20, no. 1, pp. 1-9, 2021.

[59] M. C. P. a. D. H. Lee, "Random CFI (RCFI): Efficient Fine-Grained Control-Flow Integrity Through Random Verification," IEEE Transactions on Computers, vol. 70, no. 5, pp. 733-745, 2021.

[60] C. B. a. A. Srivastava, "Reducing Timing Side-Channel Information Leakage Using 3D Integration," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 4, pp. 665-678, 2019.

[61] L. C. a. W. F. D. Zoni, "Design of Side-Channel-Resistant Power Monitors," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 5, pp. 1249-1263, 2022.

[62] J. H. M. P. Y. J. a. Y. Z. H. Ma, "Automatic On-Chip Clock Network Optimization for Electromagnetic Side-Channel Protection," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 2, pp. 371-382, 2021.

[63] D. D. a. S. S. M. Nath, "A Multipole Approach Toward On-Chip Metal Routing for Reduced EM Side-Channel Leakage," IEEE Microwave and Wireless Components Letters, vol. 31, no. 6, pp. 685-688, 2021.

[64] E. V. L. a. A. P. C. M. Ashok, "Randomized Switching SAR (RSSAR) ADC for Power and EM Side-Channel Security," IEEE SolidState Circuits Letters, vol. 5, no. 1, pp. 247-250, 2022.

[65] M. Y. C. C. M. O. T. S. a. L. K. R. Jevtic, "EM Side-Channel Countermeasure for Switched-Capacitor DC–DC Converters Based on Amplitude Modulation," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 6, pp. 1061-1072, 2021.

[66] E. T.-S. J. M. M.-G. M. V.-B. a. C. J. J.-F. F. E. Potestad-Ordóñez, "Trivium Stream Cipher Countermeasures Against Fault Injection Attacks and DFA," IEEE Access, vol. 9, no. 1, pp. 168444-168454, 2021.

[67] C. S. a. Z. W. H. Li, "Detecting Fault Injection Attacks Based on Compressed Sensing and Integer Linear Programming," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 476-483, 2019.

[68] S. C. P. C. T. H. a. S. B. A. Alaql, "LeGO: A Learning-Guided Obfuscation Framework for Hardware IP Protection," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 4, pp. 854-867, 2022.

[69] U. R. M. L. a. T. N. M. Grailoo, "Hardware-assisted Neural Network IP Protection using Non-malicious Backdoor and Selective Weight Obfuscation," in 2022 IEEE 15th Dallas Circuit And System Conference (DCAS), Dallas, TX, USA, 2022.

[70] A.S. a. M. Rathor, "HLS Based IP Protection of Reusable Cores Using Biometric Fingerprint," IEEE Letters of the Computer Society, vol. 3, no. 2, pp. 42-45, 2020.

[71] W. H. H. D. a. W. X. L. Xiao, "A hardware intellectual property protection scheme based digital compression coding technology," in 2019 IEEE International Conference on Smart Cloud (SmartCloud), Tokyo, Japan, 2019.

[72] M. A. O. S. a. J. K. S. Patnaik, "A Modern Approach to IP Protection and Trojan Prevention: Split Manufacturing for 3D ICs and Obfuscation of Vertical Interconnects," IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1815-1834, 2021.

[73] B. Olney and R. Karam, "WATERMARCH: IP Protection through Authenticated Obfuscation in FPGA Bitstreams," IEEE Embedded Systems Letters, vol. 13, no. 3, pp. 81-84, 2021.

[74] Y. W. a. W. Yu, "Combining Thermal Maps With Inception Neural Networks for Hardware Trojan Detection," IEEE Embedded Systems Letters, vol. 13, no. 2, pp. 45-48, 2021.

[75] H. S. Z. F. H. L. W. Z. a. X. L. R. Lu, "HTDet: A clustering method using information entropy for

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 119-127, January-2024
https://doi.org/10.47001/IRJIET/2024.801016

hardware Trojan detection," Tsinghua Science and Technology, vol. 26, no. 1, pp. 48-61, 2021.

[76] L. K. K. A. K. C. A. K. a. L. N. H. Zhao, "Applying Chaos Theory for Runtime Hardware Trojan Monitoring and Detection," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 4, pp. 716-729, 2020.

[77] U. A. a. F. Gebali, "Hardware Trojan Detection Using Reconfigurable Assertion Checkers," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 7, pp. 15751586, 2019.

[78] S. P. a. O. S. N. Limaye, "Valkyrie: Vulnerability Assessment Tool and Attack for Provably-Secure Logic Locking Techniques," IEEE Transactions on Information Forensics and Security, vol. 17, no. 1, pp. 744-759, 20022.

[79] W. H. Y. C. W. W. Y. G. M. W. K. L. S. N. Y. X. Z. Zhang, "BitMine: An End-to-End Tool for Detecting Row hammer Vulnerability," IEEE Transactions on Information Forensics and Security, vol. 16, no. 1, pp. 5167-5181, 2021.

[80] J. H. Y. L. L. L. Y. Z. a. Y. J. H. Ma, "Security-Driven Placement and Routing Tools for Electromagnetic Side-Channel Protection," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 6, pp. 1077-1089, 2021.

[81] J. Moos, "Cyber Forensics in a Post Stuxnet World," ITNOW, vol. 57, no. 4, pp. 32-33, 2015.

AUTHOR'S BIOGRAPHY

S.M.D.N. Siriwardana,
(Fellow, IEEE) studying as an undergraduate in Cyber Security at Sri Lankan Institute of Information Technology (SLIIT), Malabe, Sri Lanka. Currently follows academics in final year in Cyber Security program related to Department of Computer Systems and Engineering at SLIIT, Malabe, Sri Lanka.
He joined SLIIT in the year 2019 and the degree was dated to be completed by the end of year 2022. He is currently following the academics in the fields of Hardware Security and Cyber Governance. Currently his research works focuses on Cryptographic algorithms and incorporating behavioral biometrics and anti-forensic techniques in mobile and IoT security.

Citation of this Article:

S.M.D.N.Siriwardana, "Hardware Security and Trust: Trends, Challenges, and Design Tools" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 1, pp 119-127, January 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.801016

****

