2024 INTERNATIONAL CONFERENCE ON CONVERGENT AND SMART SYSTEMS (ICCSS 2024)

PIONEER INTERNATIONAL UNIVERSITY, NAIROBI, KENYA, JULY 1 - 5, 2024

Proceeding

SPONSORED BY

CHOSUN UNIVERSITY

사단법인 한국차세대컴퓨팅학회
Korean Institute of Next Generation Computing

PIONEER INTERNATIONAL UNIVERSITY

Taxonomy Construction of Anti-Tampering Techniques from a System Designer's Perspective

Ki-Woong Park*
Sejong University
Republic of Korea
woongbak@sejong.ac.kr

Sehan Lee
Sejong University
Republic of Korea
sehanlee141@gmail.com

ABSTRACT

This paper presents a taxonomy construction of anti-tampering techniques from a system designer's perspective. We have constructed a taxonomy matrix and introduce a specialized classification framework for anti-tampering techniques. The proposed taxonomy matrix makes it possible to correlate an identification number with the detailed techniques embedded in each anti-tampering solutions based on the 'sensing & reactions' perspective and their 'stackable position.' This approach enables the creation of a roadmap for anti-tampering techniques and facilitates anti-tampering orchestration to build secure systems requiring anti-tampering techniques. Finally, we introduce 'software-defined orchestration for the anti-tampering techniques for enabling an automated catalog for selecting the most suitable anti-tampering technology for a given system.

KEYWORDS

Anti-Tampering Techniques, Software-Defined System, Taxonomy Construction

1 INTRODUCTION

Over the past few decades, a wide range of anti-tampering techniques have been proposed to prevent the leakage of intellectual property embedded within systems [1]. Each anti-tampering technology comes with its own unique advantages and limitations. The applicability and suitability of a specific anti-tampering technique can vary based on the physical characteristics and security requirements of the target system [2]. In many cases, it is necessary to apply multiple anti-tampering techniques rather than relying on a single anti-tampering method. This is due to the diversity of anti-tampering technologies, each with its distinct strengths and weaknesses.

As a remedy to this problem, we focus on developing a comprehensive taxonomy of anti-tampering techniques from the perspective of system designers. We have created a taxonomy matrix and introduced a specialized classification framework designed for these techniques. This framework allows us to correlate identification numbers with the detailed methods embedded in each anti-tampering solution, considering both the 'sensing & reactions' perspective and their 'stackable position.' The organization of this paper is as follows: In Section 2, we propose a taxonomy design and a classification criterion for anti-tampering technologies derived from our study. Section 3 presents the classification matrix based on the proposed taxonomy for anti-tampering technologies and an application scenario utilizing the proposed taxonomy and classification matrix. Finally, Section 4 discusses the lessons learned from this study and suggests directions for future work.

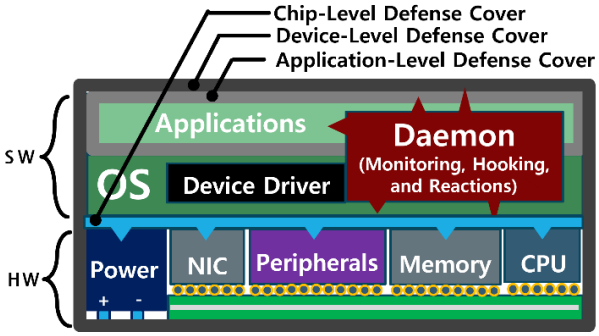

Figure 1: Classification of anti-tempering technologies and how they are driven by abstraction of system architecture.

2 TAXONOMY OVERVIEW

This section presents the abstraction of a system architecture for a construction of the taxonomy for anti-tampering technologies, which regarding the illustration for the applicable anti-tampering techniques and their core principles at each system layer. Fig. 1 depicts the key components of a typical computer system and the positions of possible anti-tampering technologies designed to protect the targeting systems. For example, components such as the CPU, memory, NIC (Network Interface Card), and peripherals on a PCB board are powered by the power supplier. To safeguard the internal structure of semiconductors mounted on the PCB, a chip-level defense cover can be employed as an anti-tampering measure. Additionally, above the hardware, there exist the OS layer and the application layer. The OS contains device drivers acting as intermediaries between the devices and applications. The anti-tampering technologies can be applied at the application level to protect the information within applications. The anti-tampering

*: First Author & Corresponding Author

technologies as a device-level defense can also be utilized to protect the overall system, both hardware and software. Each anti-tampering technology must take appropriate action in response to external intrusion attempts, a concept we define as ‘sensing & reactions’ in this study. We have established the classification criteria such as the target of protection, the technology’s position within the system, and the operating principles for each anti-tampering technology, thus forming the taxonomy metrics. The classification matrix based on this framework is detailed in Section 3.

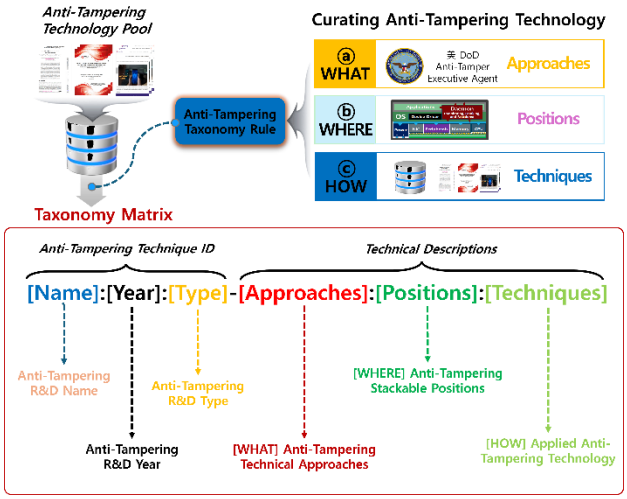

Figure 2: Overall research flow for constructing taxonomy for anti-tampering technologies and the proposed taxonomy matrix.

3 PROPOSED CLASSIFICATION MATRIX

This section outlines the classification matrix of anti-tampering techniques, constructed based on the system abstraction and taxonomy metrics described in Section 2. As illustrated in Fig. 2, our research collected outstanding research results [3–4, 6–20, 23] and commercial-off-the-shelf solutions [5, 21] from both research and industry era into the anti-Tampering technology pool. As a next step, each technology was classified according to the defined classification matrix so that each technology can be assigned a unique ID corresponding sub-techniques.

The taxonomy matrix and detailed classification task for each technology are shown at the bottom of Fig. 2. The classification matrix is divided into two main parts: the left side contains the anti-tampering IDs, and the right side displays the criteria used to classify the technologies corresponding to the unique IDs. The classification is approached from three main perspectives: ‘[WHAT] Anti-Tamper Approaches,’ ‘[WHERE] Positions of Anti-Tampering Techniques,’ and ‘[HOW] Techniques for Anti-Tampering.’ We propose a structured classification matrix that systematically categorizes these technologies, making it easier for system programmers to interpret.

Fig. 3 illustrates an example of an analyzed anti-tampering technique from research era, classified according to the proposed matrix. The study to be analyzed titled ‘6thSense,’ presented at the Usenix Conference held in 2017, is assigned a unique anti-tampering technology ID. The right side of the figure details the principles of its operation (`Where & How=Approaches`), the deployment position (`Where=Positions`), and the required technical elements (`How=Techniques`) for this technology. The ‘6thSense’ study monitors events, situations, and anomalies (`MONI-EVET, MONI-SITU, MONI-ANOM`) in the target system, and detects these through monitoring actions (`DETC-EVET, DETC-SITU, DETC-ANOM`). This technology operates at the system software layer as a daemon (`DEMN`), with necessary sub-techniques (`EVDT, SIAW, MONI`) identified. This classification system allows for understanding the operational position, principles, and necessary sub-techniques of each Anti-Tampering technology through its unique identification code.

Additionally, this approach enables the creation of a roadmap for anti-tampering techniques and facilitates anti-tampering orchestration to build secure systems requiring anti-tampering techniques [22]. Finally, this matrix makes it possible to act as a ‘software-defined orchestration engines for an automated catalog for selecting the most suitable anti-tampering technology for a given system.

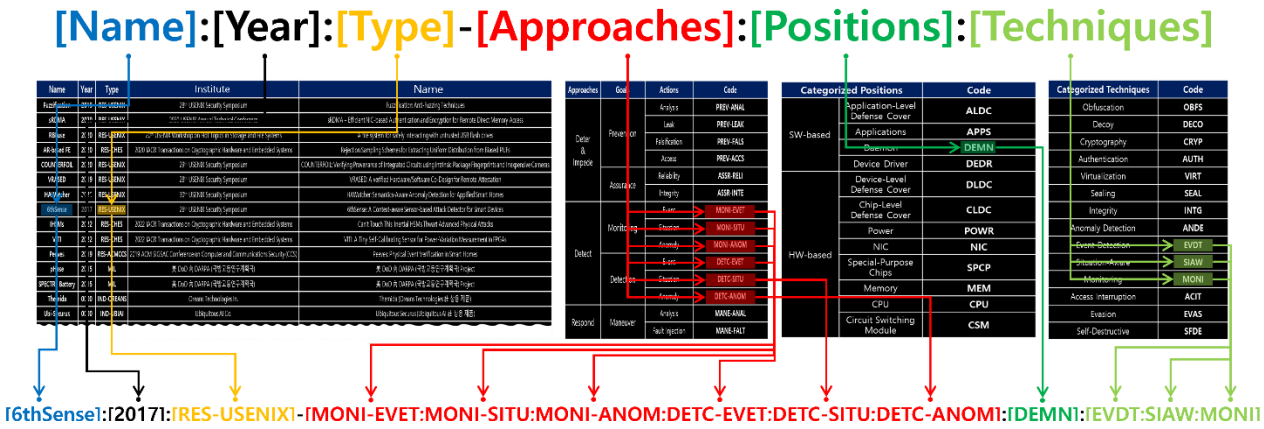

Figure 3: Case Study: an analyzed anti-tampering technique from research era, classified according to the proposed matrix.

4 CONCLUSIONS & FURTHER WORK

In conclusion, we have presented a taxonomy construction of anti-tampering techniques from a system designer's perspective. By constructing a taxonomy matrix and introducing a specialized classification framework, we have made it possible to correlate identification numbers with the detailed techniques embedded in each anti-tampering solution based on the 'sensing & reactions' perspective and their 'stackable position.' This approach enables the creation of a roadmap for anti-tampering techniques and facilitates the orchestration of anti-tampering solutions to build systems requiring advanced protection technology. Moreover, we have introduced 'software-defined orchestration' for anti-tampering techniques, enabling an automated catalog for selecting the most suitable anti-tampering technology for a given system.

For future research, we suggest exploring the application of our proposed taxonomy and classification framework in real-world scenarios to validate its effectiveness and adaptability. Further studies could focus on enhancing the automated catalog by integrating machine learning algorithms to improve the selection process of the most suitable anti-tampering technologies. Additionally, investigating the potential for expanding the taxonomy to include emerging anti-tampering techniques and their impact on system security would be valuable. Collaborative efforts with industry professionals could also provide practical insights and help refine the framework for broader applicability.

ACKNOWLEDGMENTS

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) ,(Project No. RS-2022-00165794, Development of a Multi-Faceted Collection-Analysis-Response Platform for Proactive Response to Ransomware Incidents, 30%), (Project No.2022-0-00701, 10%, Project No.RS-2023-00228996, 10%), the ICT R&D Program of MSIT/IITP, (Project No. 2021-0-01816, A Research on Core Technology of Autonomous Twins for Metaverse, South Korea, 10%), and a National Research Foundation of Korea (NRF), South Korea grant funded by the Korean government (Project No. RS-2023-00208460, 40%).

REFERENCES

[1] Indeed Co., "What is a Systems Designer? Duties, Skills, and Salary", https://www.indeed.com/career-advice/finding-a-job/what-is-systems-designer

[2] US DoD Anti-Tamper Executive Agent, "What is Anti-Tamper?", https://at.dod.mil/What-Is-Anti-Tamper/

[3] Dr. Mikhail J. Atallah et al., "A Survey of Anti-Tamper Technologies", The Journal of Defense Software Engineering, Nov., 2004

[4] Al-Wosabi et al., "Framework for Software Tampering Detection in Embedded System", The 5th International Conference on Electrical Engineering and Informatics, Aug., 2015.

[5] Rambus Co., "Understanding Anti-Tamper Technology", https://rambus.com/blogs/

[6] Jinho Jung et al., "Fuzzification: Anti-Fuzzing Techniques", The 28th USENIX Security Symposium, Aug., 2019.

[7] Konstantin Taranov et al., "sRDMA - Efficient NIC-based Authentication and Encryption for Remote Direct Memory Access", The 2020 USENIX Annual Technical Conference, July, 2020

[8] Ke Zhong et al., "RBFuse - A file system for safely interacting with untrusted USB flash drives", The 12th USENIX Workshop on Hot Topics in Storage and File Systems, July, 2020.

[9] Vincent Immler et al., "Secure Physical Enclosures from Covers with Tamper-Resistance", IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), Nov., 2018.

[10] Rei Ueno et al., "AR-based FE - Rejection Sampling Schemes for Extracting Uniform Distribution from Biased PUFs", IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), Aug., 2020

[11] S. N. Dhanuskodi et al., "COUNTERFOIL: Verifying Provenance of Integrated Circuits using Intrinsic Package Fingerprints and Inexpensive Cameras", The 19th USENIX Security Symposium, Aug., 2020.

[12] Ivan De Oliveira Nunes et al., "VRASED: A Verified Hardware/Software Co-Design for Remote Attestation", The 28th USENIX Security Symposium, Aug., 2019.

[13] Chenglong Fu et al., "HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes", The 30th USENIX Security Symposium, Aug., 2021.

[14] Amit Kumar Sikder et al., "6thSense: A Context-aware Sensor-based Attack Detector for Smart Devices", The 26th USENIX Security Symposium, Aug., 2017

[15] Jan Sebastian Götte and Björn Scheuermann, "IHSMs - Can't Touch This: Inertial HSMs Thwart Advanced Physical Attacks", IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), Nov., 2021.

[16] Brian Udugama et al., "VITI: A Tiny Self-Calibrating Sensor for Power-Variation Measurement in FPGAs", IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), Nov., 2021.

[17] Simon Birnbach et al., "Peeves: Physical Event Verification in Smart Homes", 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS), Nov., 2019.

[18] Shashank S. Pandey et al., "Self-Destructing Secured Microchips by On-Chip Triggered Energetic and Corrosive Attacks for Transient Electronics", Advanced Materials Technologies, June, 2018.

[19] Hyunwoo Heo et al., "Secure IC with Countermeasure to Unpowered Physical Attack using On-chip Photodiode and Charge Pump", International Conference on Electronics, Information, and Communication (ICEIC), Feb., 2021.

[20] Bogdan Groza et al., "CANARY - a reactive defense mechanism for Controller Area Networks based on Active Relays", The 30th USENIX Security Symposium, Aug., 2021.

[21] USA TODAY, "Pentagon seeks to build a disappearing battery", https://www.usatoday.com/story/nation/2013/12/27/vanishing-silicon-air-battery-darpa/4222327/

[22] MITRE ATT&CK, "Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle", http://www2.mitre.org/public/industry-perspective/lifecycle.html

[23] Park, J.-G. et al., "Ghost-MTD: Moving Target Defense via Protocol Mutation for Mission-Critical Cloud Systems", Energies 2020, 13, 1883.