SCADD: Side Channel Attacks, Detection Defenses

Special Track along with the 5th International Conference on Cyber-Technologies and Cyber-Systems (CYBER) 2020
October 25-29, 2020, Nice-France
https://www.iaria.org/conferences2020/filesCYBER20/SCADD.pdf

Maria Mushtaq

LIRMM-CNRS, Univ Montpellier, France
Email: maria.mushtaq@lirmm.fr

Muhammad Khurram Bhatti

ECLab, Information Technology University, Pakistan
Email: khurram.bhatti@itu.edu.pk

***Abstract*—Timing-based side-channels play an important role in exposing the state of a process execution on underlying hardware by revealing information about timing and access patterns. *Side-channel attacks (SCAs)* are powerful cryptanalysis techniques that focus on the underlying *implementation* of cryptographic ciphers during execution rather than attacking the structure of cryptographic functions. This track reviews cache-based software side-channel attacks, mitigation and detection techniques that target various cryptosystems. It provides a detailed taxonomy of attacks and cryptosystems. The track also discusses the mitigation and detection techniques proposed against side-channel attacks and classifies them based on their effectiveness at various levels in caching hardware and leveraged features. Finally, the track discusses recent trends in attacks, the challenges involved in their mitigation, and future research directions needed to deal with side-channel information leakage.**

***Keywords*–Side-Channel Attacks (SCAs), Cryptography, Detection, Mitigation, Machine Learning, Security, Privacy.**

I. INTRODUCTION

With the development of computing and storage infrastructure, information security has become one of the paramount concerns. In the past decade or so, there has been an explosion in the amount of digital data. For instance, according to IBM Big Data research, 2.5 quintillion bytes of data are created worldwide every day; so much that 90% of data in the world today was created in the last two years alone. The information buried in these data is valuable to society, be it commercial, economic, environmental, government statistics, or concern the health and privacy of individuals. Faced with this deluge of data, information processing infrastructure have evolved to increase their performance, energy efficiency, reliability, and safety. These platforms are now increasingly shifting from the end-user to centralized computing facilities (the cloud computing concept) in order to free end-user terminals from excessively high computational loads. Cloud computing is the delivery of on-demand computing resources including everything from applications to data centers over the Internet. The issue of *trust* between end-users and cloud computing platforms is, however, a major concern that is currently preventing universal acceptance of this new technological solution.

Modern-day cloud computing solutions offer Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) for both public and private cloud [1]. These services provide virtualized system resources to end-users that offer high utilization through resource sharing. Such systems usually co-host multiple virtual machines (VMs) on the same hardware platform, which is managed by a virtual machine monitor (VMM) to insulate VMs and system resources.

While virtualization is supposed to provide insulation and exclusive access to resources, in practice the VMs are designed to share the same physical resources thereby creating a loophole for potential interventions. The co-resident VMs that share physical resources are mutually distrusting. For instance, a malicious VM co-residing with a victim's VM can discover the information of other VM [2], [3], [4] through resource sharing and can cause serious damage by conducting side-channel attacks (SCA) on the victim's VMs [5], [6], thus exposing the system to the conventional challenges of information security represented by the classical CIA (confidentiality, integrity, and availability) triad. Absolute system confidentiality, integrity, and availability cannot be achieved simultaneously. Therefore, all systems have design trade-offs resulting in inherent vulnerabilities and rendering the system vulnerable to attacks.

SCAs are powerful techniques used to retrieve sensitive information by observing the system behavior through side-channels including power consumption, timing variation, acoustic emanation. Although SCAs can be used in many contexts (user spying, data extraction, etc.), this paper focuses on SCAs of cryptosystem implementations and more specifically on RSA cryptosystems. Rather than attacking the underlying structure of cryptographic functions, SCAs focus on the implementations of cryptographic ciphers [7]. SCAs use variations in physical parameters (e.g. power consumption [8], electromagnetic radiation [9], acoustic emanation [10], memory accesses or fault occurrence [5], [11], [12], [13], [14], [15], [16]) generated by the execution of specific implementation of a cipher to extract secret information. In general, SCAs can be classified in two types: hardware-based SCAs in which the attacker requires measurement equipment to get physical parameters and software-based SCAs in which the attacker uses software instead of measurement equipment to steal information such as memory access or fault occurrence that help retrieve cryptographic information [7], [17].
For this special session we focus on the following topics related to side-channel attacks: attacks and exploitations, secure implementations, implementation attack-resilient architectures and schemes, secure design and evaluation, practical attacks, test platforms and open benchmarks, detection and countermeasure techniques.

II. Submissions

The first contribution in SCADD track is entitled "Challenges of Using Performance Counters in Security Against Side-Channel Leakage". It presents that over the past few years, high resolution and stealthy attacks and their variants such as Flush+Reload, Flush+Flush, Prime+Probe, Spectre and Meltdown have completely exposed the vulnerabilities in modern computing architectures. Many effective mitigation techniques against such attacks are also being proposed that use system's behavioral parameters at run-time using Performance Counters (PCs) coupled with machine learning models. Although PCs, both in hardware and software, have shown promising results when used in the context of security, this paper provides experimental evaluation and analysis of the potential challenges, perils and pitfalls of using these counters in security.

The second contribution in the track is entitled "Side Channel Attacks on RISC-V Processors: Current Progress, Challenges, and Opportunities". Authors presented side channel attacks on microprocessors, like the RISC-V, exhibit security vulnerabilities that lead to several design challenges. Hence, it is imperative to study and analyze these security vulnerabilities comprehensively. In this paper, we present a brief yet comprehensive study of the security vulnerabilities in modern microprocessors with respect to side channel attacks and their respective mitigation techniques. Moreover, we also perform an in-depth analysis of the applicability and practical implications of cache attacks on RISC-V microprocessors and their associated challenges. Finally, based on the comparative study and our analysis, we highlight some key research directions to develop robust RISC-V microprocessors that are resilient to side channel attacks.

Third contribution in SCADD is entitled "Efficient AES Implementation for Better Resource Usage and Performance of IoTs". The paper presents that the research on Internet of Things (IoT) devices has advanced tremendously over the past few years. IoT-based systems have their applications in almost every sphere of human life. Modern IoT devices are of quite heterogeneous nature and they are going to be involved in every thing from turning home lights ON/OFF to handling life critical data of a patient in smart health system. Because of the amount and nature of the data handled by IoT devices, they are a lucrative target for various kinds of security attacks. Among the many countermeasures against the security threats, Advanced Encryption Standard (AES) is a popular cryptographic scheme as it offers robust and platform independent implementation. In this work, keeping in view of the heterogeneous nature of target IoT devices, we explore five different implementations of AES algorithm. These implementations use different algorithmic and architecture optimizations. The results obtained through these implementation reveal that some of them are very suitable for resource constrained edge IoT devices while others are useful for performance hungry middle layer gateways of an IoT-based system. Experimental results reveal that in an IoT-based system, a uniform cryptographic implementation should not be considered and that the implementations should be altered as per the nature of target device.

Fouth contribution is entitled "Exploiting Vulnerabilities in Deep Neural Networks: Adversarial and Fault-Injection Attacks". This contribution presents that from tiny pacemaker chips to aircraft collision avoidance systems, the state-of-the-art Cyber-Physical Systems (CPS) have increasingly started to rely on Deep Neural Networks (DNNs). However, as concluded in various studies, DNNs are highly susceptible to security threats, including adversarial attacks. In this paper, we first discuss different vulnerabilities that can be exploited for generating security attacks for neural network-based systems. We then provide an overview of existing adversarial and fault-injection-based attacks on DNNs.We also present a brief analysis to highlight different challenges in the practical implementation of the adversarial attacks. Finally, we also discuss various prospective ways to develop robust DNN-based systems that are resilient to adversarial and fault-injection attacks.

The fifth and last contribution is entitled "PCache: Permutation based Cache to Counter Eviction-based Cache-Side Channel Attacks". Authors present that eviction-based cache-based side-channel attacks (SCAs) are continuously increasing confidentiality issues in computing systems. To mitigate these attacks, randomization based countermeasures have raised interest because these have the potential to achieve strong security and high performance while retaining the cache features such as high-associativity and operate without the involvement of system software. However, existing countermeasures are proved to be less secure because of the small eviction set size or weak indexing functions used in them. To cope with this issue, we propose a novel randomization based architecture, called PCache, which introduces hidden members in the eviction sets to enlarge their size, which makes it difficult for an attacker to launch eviction-based cache-based SCAs. PCache replaces cache lines in multiple steps by passing through different permutation functions, which consider bits of tag and index part of the memory address in the replacement process and result in strong indexing function. Experimental evaluations show that PCache provides high security. For a 10MB cache, an attacker needs 2 years to find the eviction set and can launch eviction-based cache-based SCAs with only 28confidence level. Moreover, PCache performance overhead is only 1.6% at maximum as compared to classical set-associative caches.

III. Conclusion

The SCADD special track includes a broad range of topics related to side-channel attacks, detection and mitigation mechanisms. It contains both academic research papers introducing interesting ideas for future work in this thriving research domain.

IV. Acknowledgements

I would like to thank the organizers of CYBER2020 for their tireless efforts and for accepting SCADD as a special track in the conference. I also thank the members of the program committee for their hard work with the reviews and feedback. I am also very thankful to the authors for their very interesting contributions.

References

[1] B. P. Rimal, E. Choi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems," in 2009 Fifth International Joint Conference on INC, IMS and IDC, Aug 2009, pp. 44–51.

[2] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in ACM CCS, 2009.

[3] Z. Wu, Z. Xu, and H. Wang, "Whispers in the Hyper-space: High-speed Covert Channel Attacks in the Cloud," in USENIX Conference on Security Symposium, 2012.

[4] Y. Xu, M. Bailey, F. Jahanian, K. Joshi, M. Hiltunen, and R. Schlichting, "An Exploration of L2 Cache Covert Channels in Virtualized Environments," in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, 2011.

[5] Y. Yarom and K. Falkner, "FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack," in 23rd USENIX Conference on Security Symposium, 2014.

[6] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," in ACM CCS, NY, USA, 2012.

[7] Y. Yarom, D. Genkin, and N. Heninger, "CacheBleed: a timing attack on OpenSSL constant-time RSA," Journal of Cryptographic Engineering, vol. 7, no. 2, 2017, pp. 99–112.

[8] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '99. London, UK, UK: Springer-Verlag, 1999, pp. 388–397. [Online]. Available: http://dl.acm.org/citation.cfm?id=646764.703989

[9] J.-J. Quisquater and D. Samyde, ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 200–210.

[10] D. Genkin, A. Shamir, and E. Tromer, RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 444–461.

[11] D. Gullasch, E. Bangerter, and S. Krenn, "Cache Games – Bringing Access-Based Cache Attacks on AES to Practice," in IEEE S&P, 2011.

[12] E. Tromer, D. A. Osvik, and A. Shamir, "Efficient Cache Attacks on AES, and Countermeasures," Journal of Cryptology, vol. 23, no. 1, 2010, pp. 37–71.

[13] Q. Ge, Y. Yarom, D. Cock, and G. Heiser, "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware," Journal of Cryptographic Engineering, 2016, pp. 1–27.

[14] D. Gruss, C. Maurice, K. Wagner, and S. Mangard, "Flush+Flush: A Fast and Stealthy Cache Attack," in Proceedings of the 13th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment - Volume 9721, ser. DIMVA 2016, 2016.

[15] D. Gruss, R. Spreitzer, and S. Mangard, "Cache template attacks: Automating attacks on inclusive last-level caches," in Proc. of 24th USENIX Conf. on Security Symp. Berkeley, CA, USA: USENIX Assoc., 2015, pp. 897–912.

[16] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-Tenant Side-Channel Attacks in PaaS Clouds," in ACM SIGSAC, NY, USA, 2014.

[17] D. J. Bernstein, "Cache-timing attacks on aes," in Technical Report, 2005.