Side-channel attacks on mobile and IoT devices for Cyber–Physical systems

Conti, Mauro; Losiouk, Eleonora; Poovendran, Radha; Spolaor, Riccardo

DOI
10.1016/j.comnet.2022.108858

Publication date
2022

Document Version
Final published version

Published in
Computer Networks

Citation (APA)
Conti, M., Losiouk, E., Poovendran, R., & Spolaor, R. (2022). Side-channel attacks on mobile and IoT devices for Cyber–Physical systems. *Computer Networks*, *207*, Article 108858. https://doi.org/10.1016/j.comnet.2022.108858

Computer Networks 207 (2022) 108858

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Editorial

Side-channel attacks on mobile and IoT devices for Cyber–Physical systems

Mauro Conti [a,b], Eleonora Losiouk [a,*], Radha Poovendran [c], Riccardo Spolaor [d]

[a] Department of Mathematics, University of Padua, Via Trieste 63, Padua, 35121, Italy
[b] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Mekelweg 4, Delft, 2628 CD, The Netherlands
[c] Department of Electrical and Computer Engineering, University of Washington, Seattle, 98195, WA, United States
[d] School of Computer Science and Technology, Shandong University, Binhai road 72, Qingdao, 266237, China

ABSTRACT

The attacks that leverage the side-channels produced by processes running on mobile and IoT devices are a concrete threat for cyber–physical systems. This special issue is focused on the most recent research work that investigates novel aspects of this topic. This editorial summarizes the contributions of the seven accepted papers for this special issue.

1. Introduction

The advancements in networking and communication systems, as well as in software and hardware technologies, have paved the way for a revolution in the interaction among humans, smart devices, and engineered systems. Mobile devices and Internet of Things (IoT) devices are the main contributors to a fully interconnected world made of Cyber-Physical Systems (CPS). The success of this revolution strongly depends on the security and privacy guaranteed by such technologies and used to protect the sensitive data they store and exchange. In particular, attackers have been recently exploiting a novel approach to steal sensitive data from mobile and IoT devices: side channels. The impact of such attacks is reflected not only on the single device, but also on fully interconnected CPS, with significant consequences on industrial, environmental, and health issues.

The first instances of side-channels attacks required physical access to the target device and expensive equipment. Nowadays, even a mobile application without privileges and malicious code running on mobile and IoT devices can exploit the information leakage to extract sensitive data. Thus, there is the need to focus on the evolving field of side-channel attacks, by identifying technical challenges and recent results that could help to defend against them.

The seven accepted papers in this special issue investigate the most recent developments and research on the side-channel attacks on mobile and IoT devices for Cyber-Physical systems. The papers report theoretical and experimental studies related to these types of attacks. The contributions of these papers are outlined below.

2. Content of the issue

Attackers can use Side-channel Analysis (SCA) to profile and extract sensitive information from embedded devices. To assess the security of such devices, certification authorities test them against multiple SCA techniques, which can require a high level of complexity. In “Auto-tune POIs: Estimation of distribution algorithms for efficient side-channel analysis” [1], Rioja et al. ease this tedious task by solving the problem of identifying the Points Of Interest (POI) from a side-channel trace. In particular, the authors use Estimation of Distribution Algorithms (EDAs) to select the POI. In their experiments, the authors consider a use case involving AES implementations. They also address the portability issue raised by other state-of-the-art works by running their analyses on different devices of the same model.

Unfortunately, the noisy and high-dimensional nature of signals hinders classifiers training for SCA-based profiling attacks, which leads to false positives. To mitigate these problems, Paguada et al. in “Toward Practical Autoencoder-based Side-Channel Analysis Evaluations” [2] investigate the effectiveness of feature reduction and propose two feature reduction methods based on autoencoders. The evaluation results of the proposed methods on the ASCAD random key database outperform other state-of-the-art techniques.

In the paper “Enhanced Cache Attack on AES Applicable on ARM-based Devices with New Operating Systems” [3], Esfahani et al. present an Evict+Reload attack on the last round of the T-table of AES on ARM platforms that overcomes the limiting factor of the ARMageddon attack [4] in Linux and newer versions of Android operating systems. In those OSes, the main challenge is the restricted access to the mapping of virtual to physical addresses. The attack aims at retrieving all the key bits by extracting the 12 least significant bit (LSB) physical addresses of AES T-table elements. The attack can achieve this without requiring root privileges and without sharing the binary file with the victim.

Side-channel attacks exploit leakage from cryptographic devices to extract secret keys. However, such attacks are effective for small-size

[*] Corresponding editor.
E-mail address: eleonora.losiouk@unipd.it (E. Losiouk).

https://doi.org/10.1016/j.comnet.2022.108858

Available online 15 February 2022

keys but they cannot directly extract long keys (e.g., 128 bits in AES 128). To infer long keys, attackers apply a divide-and-conquer strategy to split a key into subkeys and analyze the subkeys separately. Jin et al. in "Efficient Side-Channel Attacks beyond Divide-and-Conquer Strategy" [5] effectively address the two main shortcomings of such strategy: (1) the inaccuracy of power leakage models due to noise; (2) the unsuccessful key recovery due to errors in combining its recovered subkeys. In the experiments, the authors show how their method correctly recovers a secret key of AES 128.

Nemesis [6] is a timing side-channel attack that aims to infer information flow dependences by counting the number of cycles of specific opcodes. In the paper entitled "NemesisGuard: Mitigating Interrupt Latency Side-Channel Attacks With Static Binary Rewriting" [7], Salehi et al. analyze the components of Nemesis attack and propose a simple but effective mitigation technique against such attack. In particular, this mitigation technique consists of rewriting a binary file and injecting padding opcodes to balance the number of cycles for each branch. In this way, Nemesis cannot distinguish between the traversed branches. The authors implement their countermeasure for ARM architectures of IoT devices and it does not require hardware or compiler modifications. In the experimental evaluation, they show that NemesisGuard is efficient and effective.

Network operators often analyze the traffic to obtain insights into the ongoing activity in their networks. Many methods collect the network traffic via a "man in the middle" approach. However, such an approach is made more challenging by the presence of mobile and remote traffic passing through VPN or relay networks. To cope with this limitation, Shusterman et al. in "Cache-Based Characterization: a Low-Infrastructure, Distributed Alternative to Network-Based Traffic and Application Characterization" [8] presents an edge computing-oriented lightweight traffic characterization method based on the last level CPU cache side-channel carried out directly on the end-point device. Such a side-channel can be accessed using an unprivileged JavaScript-based webpage. In the experimental evaluation, the proposed method is tested against VPN and non-VPN networks, and it achieves comparable results with other MITM methods.

Wireless Sensor Networks (WSN) involve battery-constrained devices that acquire data from their surrounding environment. The security focus in WSN is to ensure sensor data integrity. In "Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs" [9], Velasco et al. first briefly survey the data integrity measures in WSN. The authors then propose a novel method to guarantee data integrity that offers medium-level security while maintaining a low energy cost. In particular, such a method overlaps shuffled blocks in WSNs which makes sensor data tampering from an attacker more challenging. Moreover, the receiver can detect whether a data packet has been compromised and it can request data retransmissions. The authors evaluate their proposed method via experiments on TelosB nodes running TinyOS 2.1 in terms of energy consumption, memory, and packet size overheads.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We would like to express our deep thanks to the Editors-in-Chief for providing us with the opportunity to host this special issue in Computer Networks. We also thank all the authors who submitted their papers. Last but not least, we thank the thoughtful work of the many reviewers who have provided invaluable evaluations and recommendations.

References

[1] U. Rioja, L. Batina, J.L. Flores, I. Armendariz, Auto-tune POIs: Estimation of distribution algorithms for efficient side-channel analysis, Comput. Netw. 198 (2021) 108405.

[2] S. Paguada, L. Batina, I. Armendariz, Toward practical autoencoder-based side-channel analysis evaluations, Comput. Netw. 196 (2021) 108230.

[3] M. Esfahani, H. Soleimany, M.R. Aref, Enhanced cache attack on AES applicable on ARM-based devices with new operating systems, Comput. Netw. 198 (2021) 108407.

[4] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice, S. Mangard, Armageddon: Cache attacks on mobile devices, in: 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 549–564.

[5] S. Jin, R. Bettati, Efficient side-channel attacks beyond divide-and-conquer strategy, Comput. Netw. 198 (2021) 108409.

[6] J. Van Bulck, F. Piessens, R. Strackx, Nemesis: Studying microarchitectural timing leaks in rudimentary cpu interrupt logic, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 178–195.

[7] M. Salehi, G. De Borger, D. Hughes, B. Crispo, NemesisGuard: Mitigating interrupt latency side channel attacks with static binary rewriting, Comput. Netw. 205 (2022) 108744.

[8] A. Shusterman, C. Finkelstein, O. Gruner, Y. Shani, Y. Oren, Cache-based characterization: A low-infrastructure, distributed alternative to network-based traffic and application characterization, Comput. Netw. 200 (2021) 108550.

[9] F. Alcaraz Velasco, J.M. Palomares, J. Olivares, Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs, Comput. Netw. 199 (2021) 108470.