Bibliography

[1] Pavitra Bhade et al. "Lightweight Hardware-Based Cache Side-Channel Attack Detection for Edge Devices (Edge-CaSCADe)". en. In: *ACM Transactions on Embedded Computing Systems* 23.4 (July 2024), pp. 1–27. ISSN: 1539-9087, 1558-3465. DOI: 10.1145/3663673. URL: https://dl.acm.org/doi/10.1145/3663673 (visited on 06/24/2024).

[2] Shing Hing William Cheng et al. *Evict+Spec+Time: Exploiting Out-of-Order Execution to Improve Cache-Timing Attacks*. Publication info: Preprint. 2024. URL: https://eprint.iacr.org/2024/149 (visited on 06/28/2024).

[3] Md Hafizul Islam Chowdhuryy, Hao Zheng, and Fan Yao. "MetaLeak: Uncovering Side Channels in Secure Processor Architectures Exploiting Metadata". en. In: *2024 ACM/IEEE 51st Annual International Symposium on Computer Architecture (ISCA)*. Buenos Aires, Argentina: IEEE, June 2024, pp. 693–707. ISBN: 9798350326581. DOI: 10.1109/ISCA59077.2024.00056. URL: https://ieeexplore.ieee.org/document/10609616/ (visited on 09/09/2024).

[4] Qian Ge et al. "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware". en. In: *Journal of Cryptographic Engineering* 8.1 (Apr. 2018), pp. 1–27. ISSN: 2190-8508, 2190-8516. DOI: 10.1007/s13389-016-0141-6. URL: http://link.springer.com/10.1007/s13389-016-0141-6 (visited on 05/05/2024).

[5] Hodong Kim et al. "Deep Learning-Based Detection for Multiple Cache Side-Channel Attacks". en. In: *IEEE Transactions on Information Forensics and Security* 19 (2024), pp. 1672–1686. ISSN: 1556-6013, 1556-6021. DOI: 10.1109/TIFS.2023.3340088. URL: https://ieeexplore.ieee.org/document/10345632/ (visited on 06/28/2024).

[6] Paul Kocher et al. "Spectre Attacks: Exploiting Speculative Execution". en. In: ().

[7] Mulong Luo et al. "AutoCAT: Reinforcement Learning for Automated Exploration of Cache-Timing Attacks". In: *2023 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. ISSN: 2378-203X. Feb. 2023, pp. 317–332. DOI: 10.1109/HPCA56546.2023.10070947. URL: https://ieeexplore.ieee.org/document/10070947/?arnumber=10070947&tag=1 (visited on 07/18/2024).

[8] Maria Mushtaq et al. "Winter is here! A decade of cache-based side-channel attacks, detection & mitigation for RSA". en. In: *Information Systems* 92 (Sept. 2020), p. 101524. ISSN: 03064379. DOI: 10.1016/j.is.2020.101524. URL: https://linkinghub.elsevier.com/retrieve/pii/S0306437920300338 (visited on 05/05/2024).

[9] Omais Pandith, Rafail Psiakis, and Johanna Toivanen. "EMAClave: An Efficient Memory Authentication for RISCV Enclaves". In: *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. ISSN: 1558-1101. Mar. 2024, pp. 1–6. DOI: 10.23919/DATE58400.2024.10546597. URL: https://ieeexplore.ieee.org/document/10546597/?arnumber=10546597 (visited on 09/09/2024).

[10] Jakub Szefer. "Survey of Microarchitectural Side and Covert Channels, Attacks, and Defenses". en. In: *Journal of Hardware and Systems Security* 3.3 (Sept. 2019), pp. 219–234. ISSN: 2509-3428, 2509-3436. DOI: 10.1007/s41635-018-0046-1. URL: http://link.springer.com/10.1007/s41635-018-0046-1 (visited on 05/05/2024).

[11] Fabian Thomas et al. "RISCVuzz: Discovering Architectural CPU Vulnerabilities via Differential Hardware Fuzzing". en. In: ().

[12] Yuval Yarom and Katrina Falkner. "FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack". en. In: ().