# DATA – Differential Address Trace Analysis

Samuel Weiser*, Andreas Zankl⋆, Raphael Spreitzer*,
Katja Miller⋆, Stefan Mangard*, and Georg Sigl⋆†

* Graz University of Technology ⋆ Fraunhofer AISEC † Technical University of Munich
www.iaik.tugraz.at www.aisec.fraunhofer.de www.sec.ei.tum.de

*Side-channel attacks* infer sensitive information from computing devices by monitoring supposedly benign properties like execution time or power consumption. Similar side-information can also be obtained from memory hierarchies and microarchitectures of modern processors. DRAM, caches, and branch prediction units, for instance, have all been targets to so-called *microarchitectural attacks*. These attacks typically exploit the persistent state of shared resources and can be launched without having physical access to a target device. Microarchitectural attacks bypass important isolation mechanisms employed by operating systems or hypervisors and consequently put critical applications at risk. Dedicated countermeasures, however, are only slowly deployed or often completely omitted in practice. We therefore present DATA, an analysis tool for detecting data and code accesses that can potentially be exploited by microarchitectural attacks. More precisely, DATA is a differential address trace analysis framework that reveals address-based side-channel leaks in program binaries. This type of leaks accounts for cache attacks [1], DRAM attacks [2], branch prediction attacks [3], controlled-channel attacks [4], and likewise. The detection of address-based side-channel leaks works in three phases. First, the program under test is executed to record several address traces. Second, a generic leakage test filters execution differences caused by statistically independent program behavior, e.g., randomization, and reveals true information leaks. The third phase classifies these leaks according to the information that can be obtained from them. This provides further insight for security analysts about the risk the leaks pose in practice. To demonstrate the effectiveness of DATA, we showcase information leaks in widely used implementations of symmetric and asymmetric ciphers. The results indicate that even rigorously tested software may offer a significant attack surface to microarchitectural side-channel attacks. Frameworks like DATA help to improve code quality by detecting information leaks early in the development process. Given the modest deployment of countermeasures in practice and the increasing arsenal of attacks, they constitute an important part of the defense strategy of security and privacy critical applications.

## References

[1] Tromer, E., Osvik, D. A., and Shamir, A. Efficient Cache Attacks on AES, and Countermeasures. *J. Cryptology 23* (2010), 37–71.

[2] Pessl, P., Gruss, D., Maurice, C., Schwarz, M., and Mangard, S. DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks. In *USENIX Security Symposium 2016*

[3] Aciiçmez, O., Koç, Ç. K., and Seifert, J. Predicting Secret Keys Via Branch Prediction. In *Topics in Cryptology – CT-RSA 2007* (2007), vol. 4377 of *LNCS*, Springer, pp. 225–242.

[4] Xu, Y., Cui, W., and Peinado, M. Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems. In *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*, pp. 640–656.

**crypto day matters 28** (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-14