Job Offer: Cache Attacks - Improve, Detect, Defend!

Motivation
Server, desktop, and embedded processors implement sophisticated hierarchies of data and instruction caches to speed up code execution. These caches are shared across all users and privilege levels, which enables powerful attacks. Stealing cryptographic keys from Amazon EC2 cloud systems, spying on Android users without App permissions, and inferring information from ARM TrustZone applications are just some examples that illustrate how capable cache attacks have become. To assess the impact of cache attacks it is therefore essential to investigate new attack scenarios, detect vulnerabilities in software at design time, and defend against attacks during runtime.

Job Description
For the development of improvements, detection techniques, and defense mechanisms, we are continuously looking for motivated students with an interest in IT security. The monthly working time is 40 hours and can be extended upon request. We value an independent work style and offer plenty of room for creativity and own ideas. There is also the possibility to continue the work in the course of a Master’s thesis.

If you are interested in joining our team, feel free to contact us!

Requirements
- Strong programing skills in assembly, C, and Python
- Experience with the Linux kernel and operating system
- Basic knowledge in cryptography
- Experience with ARM-based embedded systems preferred
- Creativity and independent work style
- Good English or German skills (written and spoken)

Contact
Andreas Zankl
E-Mail: andreas.zankl@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Hardware Security Group
Parkring 4, 85748 Garching (near Munich), Germany
http://www.aisec.fraunhofer.de

Date of publication: 21. Februar 2017