Software implementations of block ciphers are widely used to perform critical operations such as disk encryption or TLS traffic protection. To speed up cipher execution, many implementations rely on pre-computed lookup tables, which makes them vulnerable to cachetiming attacks on modern processors. For time-driven attacks, the overall execution time of a cipher is sufficient to recover the secret key. Testing cryptographic software on actual hardware is consequently essential for vulnerability and risk assessment. In this work, we investigate the efficient and robust evaluation of cryptographic software on modern processors under a time-driven attack. Using a practical case study, we discuss necessary adaptations to the original attack and identify promising new micro-architectural side-channels for it. To leverage the leakage of multiple side-channels, we propose a simple, heuristic way to combine their corresponding attacks. As an additional benefit, combined attacks simplify a comprehensive evaluation of cryptographic software across multiple different processors. We finally formulate practical
evaluation suggestions based on the results of our case study.

Stichworte: ARM, new side-channels, efficient evaluation, vulnerability testing, exploiting performance events, rank estimation, AES

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
21th European Symposium on Research in Computer Security (ESORICS)

Kongress / Zusatzinformationen:
Heraklion, Creete, Greece

Datum der Konferenz:
26.-30.09.2016

Jahr:
2016

Quartal:
3. Quartal

Jahr / Monat:
2016-09

Monat:
Sep

Revied:
ja

Sprache:
en

WWW:
http://www.ics.forth.gr/esorics2016/

Occurences:
- Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016

entries: