Quantifying Side-Channels in RSA and AES

Boris Köpf
IMDEA Software Institute
Madrid, Spain
boris.koepf@imdea.org

Quantitative information-flow analysis (QIF) offers methods for reasoning about information-theoretic confidentiality properties of programs. The measures used by QIF are associated with operational security guarantees such as lower bounds for the effort required to determine a secret by exhaustive search. Moreover, they can be concisely expressed in terms of programming language semantics, which enables one to leverage existing program analysis techniques for their computation.

This talk reports on a line of work on techniques for the QIF analysis of cache and timing side-channels in implementations of cryptographic algorithms. Attacks exploiting these side-channels are highly effective [2, 3, 7], and most countermeasures against them are only heuristic (i.e. they defeat particular attacks, but are not backed up by a formal security guarantee). The talk will show how QIF techniques can be used for establishing upper bounds for the side-channel leakage of implementations of the RSA and AES cryptosystems, based on formal models of the underlying platforms.

For RSA, I will present work [4, 6] on the QIF analysis of input blinding, the state-of-the-art countermeasure against timing attacks. The analysis reveals that blinding offers strong guarantees whenever the range of possible timing measurements is small. Based on this insight, we propose the combination of blinding and discretization of execution times as the first countermeasure (beyond constant-time implementations) against RSA timing attacks that is backed up by a formal security guarantee. Our experiments on a 1024-bit RSA implementation demonstrate the cost-efficiency of this countermeasure.

For AES, I will report on ongoing work [5] on a method for the automatic QIF analysis of side-channels due to observable cache behavior. At the heart of this method is a novel technique for efficient counting of concretizations of abstract cache-states that enables connecting techniques for static cache-analysis and QIF. We implement this counting procedure on top of the AbsInt TimingExplorer [1], the most advanced engine for static cache-analysis and perform a study where we derive upper bounds on the cache leakage of a 128-bit AES executable. Our results demonstrate the feasibility of automating QIF analyses for cache side-channels of real systems.

References

[1] *AbsInt aiT Worst-Case Execution Time Analyzers*. http://www.absint.com/a3/.

[2] Daniel J. Bernstein (2005): *Cache-timing attacks on AES*. Technical Report.

[3] Paul Kocher: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. In: *Proc. CRYPTO 2006*.

[4] Boris Köpf & Markus Dürmuth: *A Provably Secure And Efficient Countermeasure Against Timing Attacks*. In: *Proc IEEE CSF 2009*.

[5] Boris Köpf, Laurent Mauborgne & Martin Ochoa: *Automatic Quantification of Cache Side-Channels*. Cryptology ePrint Archive, Report 2012/034. http://eprint.iacr.org/.

[6] Boris Köpf & Geoffrey Smith: *Vulnerability Bounds and Leakage Resilience of Blinded Cryptography under Timing Attacks*. In: *Proc. IEEE CSF 2010*.

[7] Dag Arne Osvik, Adi Shamir & Eran Tromer: *Cache Attacks and Countermeasures: the Case of AES*. In: *Proc. CT-RSA 2006*.

Submitted to:
QAPL 2012