Cryptology ePrint Archive: Report 2013/172

On the Applicability of Time-Driven Cache Attacks on Mobile Devices (Extended Version)

Raphael Spreitzer and Thomas Plos

Abstract: Cache attacks are known to be sophisticated attacks against cryptographic implementations on desktop computers. Recently, also investigations of such attacks on testbeds with processors that are employed in mobile devices have been done. In this work we investigate the applicability of Bernstein's timing attack and the cache-collision attack by Bogdanov et al. in real environments on three state-of-the-art mobile devices. These devices are: an Acer Iconia A510, a Google Nexus S, and a Samsung Galaxy SIII. We show that T-table based implementations of the Advanced Encryption Standard (AES) leak enough timing information on these devices in order to recover parts of the used secret key using Bernstein's timing attack. We also show that systems with a cache-line size larger than 32 bytes exacerbate the cache-collision attack by Bogdanov et al.

Category / Keywords: applications / AES, ARM Cortex-A series processors, time-driven cache attacks, cache-collision attacks

Publication Info: Extended version of a short paper accepted at NSS 2013

Date: received 26 Mar 2013

Contact author: raphael spreitzer at iaik tugraz at