Cryptology ePrint Archive: Report 2011/232

Remote Timing Attacks are Still Practical

Billy Bob Brumley and Nicola Tuveri

Abstract: For over two decades, timing attacks have been an active area of research within applied cryptography. These attacks exploit cryptosystem or protocol implementations that do not run in constant time. When implementing an elliptic curve cryptosystem with a goal to provide side-channel resistance, the scalar multiplication routine is a critical component. In such instances, one attractive method often suggested in the literature is Montgomery's ladder that performs a fixed sequence of curve and field operations. This paper describes a timing attack vulnerability in OpenSSL's ladder implementation for curves over binary fields. We use this vulnerability to steal the private key of a TLS server where the server authenticates with ECDSA signatures. Using the timing of the exchanged messages, the messages themselves, and the signatures, we mount a lattice attack that recovers the private key. Finally, we describe and implement an effective countermeasure.

Category / Keywords: public-key cryptography / side-channel attacks, timing attacks, elliptic curve cryptography, lattice attacks.

Date: received 11 May 2011, last revised 8 Jun 2011

Contact author: bbrumley at tcs hut fi

Available formats: PDF | BibTeX Citation

Version: 20110608:084003 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]