Cryptology ePrint Archive: Report 2011/633

Practical realisation and elimination of an ECC-related software bug attack

B.B. Brumley and M. Barbosa and D. Page and F. Vercauteren

Abstract: We analyse and exploit implementation features in OpenSSL version 0.9.8g which permit an attack against ECDH-based functionality. The attack, although more general, can recover the entire (static) private key from an associated SSL server via 633 adaptive queries when the NIST curve P-256 is used. One can view it as a software-oriented analogue of the bug attack concept due to Biham et al. and, consequently, as the first bug attack to be successfully applied against a real-world system. In addition to the attack and a posteriori countermeasures, we show that formal verification, while rarely used at present, is a viable means of detecting the features which the attack hinges on. Based on the security implications of the attack and the extra justification posed by the possibility of intentionally incorrect implementations in collaborative software development, we conclude that applying and extending the coverage of formal verification to augment existing test strategies for OpenSSL-like software should be deemed a worthwhile, long-term challenge.

Category / Keywords: cryptographic protocols / elliptic curve, OpenSSL, NIST, fault attack, bug attack

Publication Info: This is the full version of a shorter paper to appear at CT-RSA 2012

Date: received 24 Nov 2011, last revised 6 Mar 2012

Contact author: page at cs bris ac uk