Cryptology ePrint Archive: Report 2013/157

The fragility of AES-GCM authentication algorithm

Shay Gueron and Vlad Krasnov

Abstract: A new implementation of the GHASH function has been recently committed to a Git version of OpenSSL, to speed up AES-GCM. We identified a bug in that implementation, and made sure it was quickly fixed before trickling into an official OpenSSL trunk. Here, we use this (already fixed) bug as a real example that demonstrates the fragility of AES-GCM's authentication algorithm (GHASH). One might expect that incorrect MAC tag generation would only cause legitimate message-tag pairs to fail authentication (which is already a serious problem). However, since GHASH is a "polynomial evaluation" MAC, the bug can be exploited for actual message forgery.

Category / Keywords: AES-GCM, GHASH, polynomial evaluation MAC, message forgery, OpenSSL

Date: received 15 Mar 2013, last revised 15 Mar 2013

Contact author: shay at math haifa ac il

Available formats: PDF | BibTeX Citation

Version: 20130326:134653 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]