Cryptology ePrint Archive: Report 2011/643

Some Words About Cryptographic Key Recognition In Data Streams

Alexey Chilikov and Evgeny Alekseev

Abstract: Search for cryptographic keys in RAM is a new and prospective technology which can be used, primarily, in the computer forensics. In order to use it, a cryptanalyst must solve, at least, two problems: to create a memory dump from target machine and to distinguish target cryptographic keys from other data. The latter leads to a new mathematical task: <<recognition of cryptographic keys in the (random) data stream>>. The complexity of this task significantly depends on target cryptoalgorithm. For some algorithms (i.e. AES or Serpent) this task is trivial but for other ones it may be very hard. In this work we present effective algorithms of expanded key recognition for Blowfish and Twofish. As far as we know this task for these algorithms has never been considered before.

Category / Keywords: side-channel attacks, live-memory analysis, digital forensics, blowfish, twofish

Date: received 29 Nov 2011

Contact author: chilikov at passware com