Cryptology ePrint Archive: Report 2011/221

Protecting Drive Encryption Systems Against Memory Attacks

Leo Dorrendorf

Abstract: Software drive encryption systems are vulnerable to memory attacks, in which an attacker gains physical accesses to the unattended computer, obtains the decryption keys from memory and consequently decrypts the drive. We reviewed the currently existing mitigations and have found that they provide only partial protection, and none of them protect against the full range of memory attacks. We propose a new method for protecting encryption systems against memory attacks, by converting them to use two tiers of keys, a single Master Key and a set of File or Sector keys. When the computer is unattended, the Master Key and part of the second-tier keys are erased from memory. The method is secure against any type of memory attack, including attackers who gain complete control of the unattended system. Compared to previous methods of protection, which erase keys and shut down the computer, our method allows to keep the computer operational by a combination of cryptographic and operating systems techniques. Applications may continue running, and can access any unencrypted data as well as a chosen subset of the encrypted data, at the cost of leaving that data unsecured against memory attacks. We first describe the application of the method to file-based encryption systems, where we have implemented and tested it in practice, and then describe a possible adaptation to disk-based encryption systems.

Category / Keywords: applications / key management

Date: received 6 May 2011

Contact author: leo dor at gmail com