

CipherShed - Bug #110

Open Crypto Audit Project TrueCrypt CS-TC-4 - Unauthenticated ciphertext in volume headers

04/05/2015 02:49 AM - Jason Pyeron

| | | | |
|--|------|------------------------|------------|
| Status: | New | Start date: | 04/05/2015 |
| Priority: | High | Due date: | |
| Assignee: | | % Done: | 0% |
| Category: | | Estimated time: | 0.00 hour |
| Target version: | | Spent time: | 0.00 hour |
| Description | | | |
| <p>TARGETS: TrueCrypt volume metadata stored in encrypted headers</p> <p>DESCRIPTION: The TrueCrypt volume format consists of a small header containing metadata followed by the contents of the volume. The header and volume contents are encrypted separately: the header with a key derived from a user-supplied password, and the contents with a master key stored in the encrypted header.</p> <p>Cryptographic integrity and authenticity guarantees are beyond the scope of full-disk encryption. This is because providing these checks would necessarily incur unacceptable storage and performance penalties. Volume contents are accordingly encrypted without authentication.</p> <p>In contrast, guaranteeing the integrity of the volume header is a tractable problem. Indeed, TrueCrypt attempts to provide integrity by several means, including:</p> <ul style="list-style-type: none">• A magic string ``TRUE" at the beginning of the volume header.• A CRC32 calculated over the master key material.• A CRC32 calculated over the remainder of the volume header. <p>These checks do not constitute a true message authentication code (MAC). In a plaintext-only scenario, it would be trivial for an attacker to forge a valid header. In practice, an attacker does not have such fine-grained control due to the message-scrambling properties of the available encryption algorithms. Nevertheless, existential forgeries are possible with approximately 2³² queries.</p> <p>The consequences of a successful header forgery are unclear. Because the header contains many fields that drive program behavior, tampering with them may cause TrueCrypt to enter unexpected or invalid states.</p> <p>Recommendation: Design a new system that uses the passphrase-derived user key to derive both an encryption and an authentication key. Verify a MAC of header ciphertext before attempting decryption.</p> <p>March</p> | | | |