OpenPGP 2-4-1: Merging two messages in one ciphertext

Jonas Magazinius Nadim Kobeissi

Assured
jonas.magazinius@assured.se

Abstract. ASD

Keywords: OpenPGP

1 Introduction

This is intro!

2 Background

3 OpenPGP

3.1 CFB mode

OpenPGP CFB mode OpenPGP implements CFB mode slightly differently compared to standard CFB mode. Instead of encrypting an IV and XOR it with the first block of plaintext a block of zeroes is encrypted and XORed with a random number, acting as an IV.

$C_1 = E(0) \oplus R$
$|C_2|_a$

Properties of CFB mode To start out, let us note some important properties concerning modification of a ciphertext encrypted in CFB mode. It is important to note that neither of these properties depend on the encryption key, which implies that knowing the key is not required to abuse them. The properties have historically been abused, and will again be abused in Section X, to attack the PGP message format.

Property 1 The ciphertext will have the exact length of the ciphertext and vice versa. A modification of the length of the ciphertext will cause the same effect on the plaintext. Any number of bytes cut off the end of the ciphertext will cut the same amount of bytes from the plaintext.

Property 2 The decryption of a block depends only on the preceding block, regardless of where in the ciphertext it appears. Blocks can also be injected amidst two blocks, affecting only the first and last block of the injected sequence. As a result, any sequence of ciphertext blocks can be cut, duplicated or moved between blocks in the ciphertext, and still produce the same plaintext. The decrypted output of the first block of the two and the block following the second will however be garbled. This means an attacker can inject these two blocks amidst blocks in the ciphertext and the decrypted output will be one block of random data and one with arbitrary attacker chosen text.

Property 3 When decrypting, the plaintext stands in direct relation to the ciphertext. A flipped bit in the ciphertext causes the same bit to be flipped in the plaintext. By extension, if the plaintext of a block, or part of a block is known, that part of the plaintext can be arbitrarily and reliably modified to produce any text. Of course, modifying the ciphertext will cause the plaintext of the following block to be scrambled. If the modified block is the last block of the sequence, there will be no block to scramble.

3.2 The PGP message format

A PGP message consists of a set of packets. Each packet has a header consisting of a one byte tag and a variable number of bytes describing the total size of the packet. Five kinds of packets are of particular interest for this article, Literal, Compressed, Symmetrically Encrypted (SE), Symmetrically Encrypted Integrity Protected (SEIP), and Modification Detection Code (MDC) packets. For a complete description of the PGP message format the reader is referred to the PGP standard documentation, RFC4880.

The OpenPGP message format is specified and refined in RFCs 1991, 2440, and finally standardised in RFC 4880 [**?**,**?**].

Of particular interest are symmetrically encrypted packets, both with and without integrity protection.

4 Two for one

The "Two for One" attack merges two messages, encrypted with different keys, into a single ciphertext.

Steps: Find two key

5 Conclusion

Well, wasn't this awesome!

Acknowledgments