FREAK ATTACK IN OPENSSL (CVE-2015-0204)

Rodion Krjutškov
UNIVERSITY OF TARTU
2015
SSL and TLS

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocols designed to provide communications security over a computer network. Original SSL protocols were developed by Netscape with first release in 1995. SSL and TLS use asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to negotiate a symmetric key for further encryption of data transferred between the parties.[7]

RSA_EXPORT in SSL

According to some sources, National Security Agency (NSA) of United States was interested in being able to read secured web traffic by foreign nationals.[2] Due to strict export of cryptography from the United States regulations, Netscape had to develop two versions of its web browser. The US edition supported full size (1024-bit or larger) RSA public keys in combination with full size symmetric keys (128-bit RC4 or 3DES in SSL 3.0 and TLS 1.0). The international edition had its key lengths reduced to 512 bits and 40 bits respectively (RSA_EXPORT with 40-bit RC2 or RC4 in SSL 3.0 and TLS 1.0). This weak 40-bit encryption could be broken in a matter of days using a single personal computer.[8]

These restrictions were lifted in the late 1990s, but the weaker encryption is built into software that is being used around the world (including United States), apparently unnoticed until this year.[9]

OpenSSL

OpenSSL is the most popular open-source cryptographic library and SSL/TLS implementation in the internet. According to some experts, up to two thirds of all webservers use it.[3] A number of notable vulnerabilities were discovered in OpenSSL over the course of time, such as “catastrophic” Heartbleed bug.[4]

FREAK attack

FREAK stands for “Factoring RSA Export Keys”. The vulnerability was discovered by researchers at INRIA (French Institute for Research in Computer Science and Automation).[5] The attack is possible because some modern TLS clients, including Apple's Secure Transport and OpenSSL, have a bug in them. This bug causes them to accept RSA “export-grade” keys even when the client didn't ask for “export-grade” RSA. The vulnerability allows a 'man in the middle attacker' to intercept HTTPS connections between clients and servers and force them to downgrade connections from “strong” RSA to “export-grade” RSA.[1]
**Man-in-the-middle (MITM) attack**

1. In the client’s Hello message, it asks for a standard RSA ciphersuite.
2. The MITM attacker changes this message to ask for “export” RSA.
3. The server responds with a 512-bit “export” RSA key, signed with its long-term key.
4. The client accepts this weak key due to the OpenSSL/Secure Transport bug.
5. The attacker factors the RSA modulus to recover the corresponding RSA decryption key.
6. When the client encrypts the “pre-master secret” to the server, the attacker can now decrypt it to recover the TLS “master secret”.
7. From here on out, the attacker sees plaintext and can inject anything it wants.[1]

**Fixes**

The FREAK attack is possible when a vulnerable browser connects to a susceptible web server, so the vulnerability has to be fixed both on server and client sides. CVE-2015-0204 refers to OpenSSL bug, but other TLS libraries have similar problems (Microsoft SChannel CVE-2015-1637, Apple Secure Transport CVE-2015-1067).

The OpenSSL vulnerability was fixed by abandoning the handshake in case the client receives an “export” RSA key that the client was not asking for.[10] The vulnerability was first classified as “low severity”, because it was originally thought that server RSA export ciphersuite support was rare.[11] Later it was reclassified as “high severity”, because studies have shown that RSA export ciphersuite support is far more common.[12]

**Sources**

All the following sources have been retrieved on 31 of May 2015.

1. [Attack of the week: FREAK (or 'factoring the NSA for fun and profit')](#).
2. [FREAK: Another day, another serious SSL security hole](#).
3. [Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping](#).
4. [Critical crypto bug exposes Yahoo Mail, other passwords Russian roulette-style](#).
5. [Tracking the FREAK Attack](#).
6. [FREAK](#).
7. [Transport Layer Security](#).
8. [Export of cryptography from the United States](#).
9. ['FREAK' flaw undermines security for Apple and Google users, researchers discover](#).
10. [Only allow ephemeral RSA keys in export ciphersuites](#).
11. [OpenSSL Security Advisory [08 Jan 2015]](#).
12. [OpenSSL Security Advisory [19 Mar 2015]](#).