Hw7 TLS Vulnerabilities

Jackson Mowry

Thu Oct 23 13:52:08 2025

Summary

In 2015, researchers from INRIA, Microsoft Research, and IMDEA found a vulnerability in certain SSL clients (specifically OpenSSL and Apple's SecureTransport) that allowed requests to be rewritten to utilize less secure crypto keys. This attack is known as FREAK, which stands for Factoring RSA Export Keys Attack, which, as the name implies, means that these less secure RSA keys were then factored to break the encryption. This attack was discovered as the researchers fuzzed various software implementations of TLS/SSL suites. Fuzzing is a process in which an external program feeds input into the program being fuzzed, with the goal of enumerating all possible combinations of state within the fuzzed program. Through the process, the researchers discovered the vulnerable implementations.

The attack works by man-in-the-middling a connection between a vulnerable client device and an insecurely configured server. For this particular attack, the server has to support $\text{RSA}_{\text{EXPORT}}$ keys, which are 512-bit RSA keys that are a holdover required from the crypto export restrictions in the US. The MITM takes in a client connection, rewrites it to request $\text{RSA}_{\text{EXPORT}}$ class keys, stores the returned keys for factoring, and replies to the client. When the client then goes to encrypt the pre-master secret, the attacker decrypts it and has the master secret. The key can then be factored, which took approximately an hour in 2015, though this can likely be done much faster with modern hardware. One crucial vulnerability also exists on the target server once these $\text{RSA}_{\text{EXPORT}}$ keys are generated, they are used until the server restarts, which could be days or even weeks. Once the RSA key has been factored, the MITHM can funnel future client's traffic through themselves, allowing it to be viewed in the clear. Additionally, they can rewrite the contents of the website to say whatever they would like.

Back in 2015, the attack was originally thought to be a small concern, but as the researchers dug further, they realized that many more client devices and servers were vulnerable to the attack. A surprising 36.7% of all websites (utilizing TLS/SSL at the time) were shown to support $\text{RSA}_{\text{EXPORT}}$ quality keys. Client devices were mostly limited to mobile devices, such as iOS and Android mobile browsers.

Moving forward, it is important to think about how the open-source nature of security can help security move forward. It is incredible that most of our software is open source now and that these researchers were easily able to verify the implementation and discover where any potential bugs are hidden. Part of the reason this entire attack happened in the first place was that the US put crypto export rules into place, disallowing "strong" cryptography to be used when communicating outside the US. As we have seen over and over again in software, removing support for legacy systems is often hard, especially when users still rely on them for their daily function. Additionally, we should take this as a motivation to fuzz more open-source software.

Sources

https://web.archive.org/web/20250311154256/https://www.smacktls.com/
https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/
https://freakattack.com/