20 years of Bleichenbacher attacks

Gage Boyle

Technical Report

RHUL–ISG–2019–1

27 March 2019

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

A secure implementation of SSL/TLS is a critical part of modern internet security. Consequently, one would hope that a 20-year-old side-channel attack against the protocol would be easy to defend against. In this project, we establish that this is not the case, illustrate how to exploit such side-channel information, and provide a detailed investigation into how Bleichenbacher's attack has evolved since 1998. Our example, which we build upon throughout, demonstrates the improvements to the attack in both a technical and non-technical way. Furthermore, our research into optimising the algorithm provides tangible evidence regarding its most efficient implementation.

The main findings of this project revolve around the security concerns brought about by known padding schemes, and that the exploitation of side-channel leakage during an SSL/TLS handshake severely damages the security of hybrid encryption that utilises RSA. We found that many high-profile websites and implementations are or have been vulnerable, including Facebook, PayPal, Java Secure Socket Extension and OpenSSL. As such, the pervasiveness of this attack warrants careful consideration by all those who are responsible for implementing SSL/TLS – including TLS 1.3 and its deprecation of RSA encryption. The attack exists in many forms, and this is something that we highlight as we analyse literature from the last 20 years. Its application is also not restricted to the SSL/TLS protocol, and our overview of its ability to exploit the XML standard and the QUIC protocol is testament to this. Furthermore, we discovered a mathematical error in the original algorithm, and our research and experimentation towards the end of the project provides both insight and improvements to the available literature.

With this in mind, the purpose of this project is to present a comprehensive understanding of the attack and ultimately provide evidence regarding its cause. Although we seek the most optimised version of the attack algorithm, this project was written in an attempt to gain and provide awareness of poor SSL/TLS implementations. Subsequently, our intention is to uncover what must be done to successfully defend against an adversary with the knowledge to invoke such an attack.