CS 427, Final Project
POODLE
Padding Oracle on Downgraded Legacy Encryption

Cody Malick
malickc@oregonstate.edu

March 13, 2017

Abstract

This paper outlines the POODLE exploit. It gives details on how it allows an adversary to repeatedly query a server, and eventually decrypt a block one byte at a time. The exploit was first published by the Google Security Team on October 14, 2014 by Bodo Moller, Thai Duong, and Kryzsztof Kotowicz. While SSL version 3.0 is quite old, it is still in use today for browser backward compatibility.

Introduction

POODLE is an attack on Secure Socket Layer version 3.0 that was made public in 2014. It was announced on Google's Security Blog, co-published by Bodo Moller, Thai Duong, and Kryzsztof Kotowicz. POODLE allows an attacker targeting SSL 3.0 to decrypt one byte of an encrypted SSL block one out of two-hundred fifty-six attempts. While this is an average, being able to decrypt a byte of an encrypted block that quickly is quite a security flaw.[1]

The Attack

Context

To completely understand the attack, the context should first be made clear. SSL version 3.0 is quite dated, and should for all intents and purposes be completely retired. Modern browsers, however, use SSLv3 as a fall back for compatibility purposes. The browser will first try to connect to the web server using TLS version 1.2, the de facto standard for web communication. If that fails, it is default behavior in browsers to fall back to earlier standards, such as SSLv3.[1]

While browsers continue to support SSLv3, this attack will continue to be an issue. A savvy attacker with the proper resources could catch web requests with a man in the middle attack, and prevent all non-SSLv3 requests from going through. This would force the use of SSLv3 if it is supported by the web server.

Padding

AES CBC Mode

Exploit

Exploit Publication by Google

The Fix

Bibliography

References

[1] K. K. Bodo MOller, Thai Duong. (2014, Octoboer) This poodle bites: Exploiting the ssl 3.0 fallback. [Online]. Available: https://www.openssl.org/ bodo/ssl-poodle.pdf