Cryptology ePrint Archive

Paper 2006/136

A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL

Gregory V. Bard

Abstract

This paper introduces a chosen-plaintext vulnerability in the Secure
Sockets Layer (SSL) and Trasport Layer Security (TLS) protocols which
enables recovery of low entropy strings such as can be guessed from a
likely set of 2--1000 options. SSL and TLS are widely used for securing communication over the Internet. When utilizing block ciphers
for encryption, the SSL and TLS standards mandate the use of the
cipher block chaining (CBC) mode of encryption which requires an
initialization vector (IV) in order to encrypt. Although the first IV
used by SSL is a (pseudo)random string which is generated and shared
during the initial handshake phase, subsequent IVs used by SSL are
chosen in a deterministic, predictable pattern; in particular, the IV
of a message is taken to be the final ciphertext block of the immediately-preceding message, and is therefore known to the adversary.

traveling over the same SSL channel. We show this provides a feasible
``point of entry'' for this attack. Moreover, we show that the location of target data among block boundaries can have a profound
impact on the number of guesses required to recover that data,
especially in the low-entropy case.

The attack in this paper is an application of the blockwise-adaptive
chosen-plaintext attack paradigm, and is the only feasible attack to
use this paradigm with a reasonable probability of success. The
attack will work for all versions of SSL, and TLS version 1.0. This
vulnerability and others are closed in TLS 1.1 (which is still in draft status) and OpenSSL after 0.9.6d. It is hoped this paper will
encourage the deprecation of SSL and speed the adoption of OpenSSL
or TLS 1.1/1.2 when they are finially released.

Note: Changes relating to the directions of traffic of the adversary and target. Also some formatting changes.

Metadata

Available format(s)

PDF

Category

Implementation

Publication info

Keywords

Blockwise Adaptive | Chosen Plaintext Attack (CPA) | Secure Sockets Layer (SSL) | Transport Layer Security (TLS) | Cryptanalysis | HTTP-proxy | Initialization Vectors (IV) | Cipher Block Chaining (CBC) | Virtual Private Networks (VPN).

Contact author(s)

gregory bard @ ieee org

History

2006-04-18: last of 2 revisions

2006-04-09: received

See all versions

Short URL

https://ia.cr/2006/136

License

CC BY

BibTeX Copy to clipboard

```
@misc{cryptoeprint:2006/136,
      author = {Gregory V.  Bard},
      title = {A Challenging but Feasible Blockwise-Adaptive
      howpublished = {Cryptology {ePrint} Archive, Paper 200
      year = {2006},
      url = {https://eprint.iacr.org/2006/136}
}
```

Cryptology ePrint Archive