Cryptology ePrint Archive

Paper 2004/111

The Vulnerability of SSL to Chosen Plaintext Attack

Gregory V. Bard

Abstract

The Secure Sockets Layer (SSL) protocol is widely used for securing communication over the Internet. When utilizing block ciphers for encryption, the SSL standard mandates the use of the cipher block chaining (CBC) mode of encryption which requires an initialization vector (IV) in order to encrypt. Although the initial 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. We show that this introduces a vulnerability in SSL which (potentially) enables easy recovery of low-entropy strings such as passwords or PINs that have been encrypted. Moreover, we argue that the open nature of web browsers provides a feasible ``point of entry'' for this attack via a corrupted plug-in; thus, implementing the attack is likely to be much easier than, say, installing a Trojan Horse for ``keyboard sniffing''. Finally, we suggest a number of modifications to the SSL standard which will prevent this attack.

Metadata

Available format(s)

PDF | PS

Cryptology ePrint Archive

Published elsewhere. Submitted to ESORICS 2004.

Keywords

Chosen Plaintext Attack | SSL | TLS | Cryptanalysis.

Contact author(s)

gregory bard @ ieee org

History

2004-05-12: revised

2004-05-11: received

See all versions

Short URL

https://ia.cr/2004/111

License

CC BY

BibTeX Copy to clipboard

```
@misc{cryptoeprint:2004/111,
      author = {Gregory V.  Bard},
      title = {The Vulnerability of {SSL} to Chosen Plaintext
      howpublished = {Cryptology {ePrint} Archive, Paper 200
      year = {2004},
      url = {https://eprint.iacr.org/2004/111}
}
```

Cryptology ePrint Archive