PEACH
FUZZER

SSL Peach Pit
Data Sheet

- Peach Pit: SSL
- Target: Client (with and without certificate request), Server
- Supported Platforms: Windows, Linux, OS X

The SSL/TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Variations

Protocol	Server	Server Verify	Client	Client Verify
TLS 1.0	X	X	X	X
TLS 1.1	X	X	X	X
TLS 1.2	X	X	X	X

Specifications

Specification	Title
RFC 2246	The TLS Protocol Version 1.0
RFC 4346	The Transport Layer Security (TLS) Protocol Version 1.1
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 6520	Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension

Use Cases

Messages	Specification
Client Hello	RFC 2246, RFC 4346, RFC 5246
Server Hello	RFC 2246, RFC 4346, RFC 5246
Server Certificate	RFC 2246, RFC 4346, RFC 5246
Server Key Exchange	RFC 2246, RFC 4346, RFC 5246

Messages	Specification
Certificate Request	RFC 2246, RFC 4346, RFC 5246
Server Hello Done	RFC 2246, RFC 4346, RFC 5246
Client Certificate	RFC 2246, RFC 4346, RFC 5246
Client Key Exchange	RFC 2246, RFC 4346, RFC 5246
Change Cipher	RFC 2246, RFC 4346, RFC 5246
Certificate Verify	RFC 2246, RFC 4346, RFC 5246
Finished	RFC 2246, RFC 4346, RFC 5246
Alert	RFC 2246, RFC 4346, RFC 5246
Encrypted Data	RFC 2246, RFC 4346, RFC 5246
Heartbeat Hello	RFC 6520
Heartbeat Request	RFC 6520
Heartbeat Response	RFC 6520

Cipher Suites

Cipher Suite
RSA-SHA-AES128