Transport Layer Security

TLS vs. SSL:

SSL connections begin with security and proceed directly to secured communications

TLS connections begin with an insecure “hello” to the server and only switch to secured communications after the handshake between the client and the server is successful.

TLS is an open community standard and is therefore more extensible.

TLS allows flexibility in choosing ciphers of varying complexities – hence is non-interoperable with SSL

TLS is no longer backward compatible with SSL – will never negotiate lower than SSL 3.0

Transport Layer Security

TLS Vulnerabilities:

Drown Attack – still affects high percentage of servers:

Configuration exploit – attacker forces a server to use SSL v.2 which is known to be badly insecure.

No modern clients use SSL v.2 – some servers have kept supporting SSL v.2 because it did not seem to matter
Configuration change would prevent this attack

SSL v.2 vulnerable to Ciphersuite rollback attack (MiM)
SSL v.2 allows DES encryption (cracking in a few days)
Signature Verification Failed vulnerability – client may continue with the connection without authentication
SSL v.1 doesn't block disabled ciphers
Divide and conquer session key recovery in SSL v.2
DH primes that are not safe are allowed – can be recovered if static DH is used

Transport Layer Security

TLS Vulnerabilities:

Key Compromise Impersonation vulnerability:

Attacker can impersonate trusted servers without being in possession of the servers' secret keys

Attacker spoofs server, forces client to use insecure TLS authentication options and a certificate for which attacker has the private key

Victim gets attacker's certificate through social engineering
e.g. attacker presents victim with certificate to use a service

Uses the fact that many operations manage certificates insecurely

Transport Layer Security

TLS Vulnerabilities:

Browser Exploit Against SSL/TLS (BEAST):

Attacker can determine an initialization vector

If IVs are known, an attacker can get information from ciphertext patterns, although not a lot

Requires another vulnerability such as XXS

Factoring RSA Keys (FREAK) & Logjam:

Reduce the security offered by SSL/TLS by forcing a connection to use “Export-grade” grade encryption

- which reduces the RSA strength to 512 bits

Numerous Occurrence Monitoring & Recovery Exploit:

Attack against RC4 which allows a HTTP cookie to be retrieved in a couple of days

Transport Layer Security

TLS Vulnerabilities:

Bar Mitzvah:

Small amounts of plaintext can be recovered from streams protected by RC4 encryption

Sweet32:

Capture a HTTP cookie after grabbing 785 GB of traffic

TLS Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability:

Possible when a block cipher is enabled utilizing the CBC cipher mode

Allows an attacker to decipher a chosen byte of cipher text in as few as 256 attempts.

Heartbleed:

Theft of credentials – buffer overrun

Transport Layer Security

TLS Certificates:

Self-Signed:

Attacker can create its own “forged” certificate
End user has no way of knowing the certificate is bogus
Attacker can capture all encrypted data and modify client requests and server responses.

Certificate with wrong hostname:

Certificates confirm the identity of a service
The identity is specified by the Common Name (CN)
CN != hostname raises security error in browsers
Attacker now has the means to place illegitimate cert on end user's machine – the end user clicks OK to accepting the certificate