Overview TLS attacks

vrijdag 6 januari 2023 14:09

Attack	**Description**
SSLstrip	Intercept HTTP traffic & replace links/redirects to HTTPS with HTTP
BEAST *(Browser Exploit Against SSL/TLS)*	Working in CBC mode: given c_0 and c_1, we can check whether $p_1 = x$ by choosing $p_2 = x \oplus c_0 \oplus c_1$. Requires attacker to be able to make client send data (i.e. the chosen guess p_2).
CRIME *(Compression Ratio Info-leak Made Easy)*	Second occurrence of a character is encoded as a back reference in compressed plaintext, which leads to shorter ciphertext; allows for guessing secrets in ciphertext.
BREACH *(Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)*	Same as CRIME, but applied to HTTP compression instead of TLS compression.
Padding Oracle	Error message depends on correctness of padding in plaintext; allows for checking validity of plaintext by guessing based on crafted message.
Lucky 13	Padding oracle, but using timing of MAC computation as side channel.
POODLE *(Padding Oracle On Downgraded Legacy Encryption)*	Make client accept lower TLS version, then apply padding oracle attack.
RC4 attacks (RC4 is a stream cipher)	• Roos' biases • First byte of keystream is correlated to first three bytes of key. • Biased outputs of the RC4 • Second output byte of keystream is biased toward zero with probability $\frac{1}{128}$. • Fluhrer, Mantin and Shamir attack: • If nonce and long-term key are concatenated (as in WEP), long-term key can be discovered. • Klein's attack • Correlation between RC4 keystream and key • Royal Holloway attack • Even more correlations in keystream • Bar-mitzvah attack • Some keys are particularly weak in RC4 → could reveal hundreds of plaintext bytes • NOMORE RC4 (Numerous Occurrence MOnitoring & Recovery Exploit) • Even more biases
FREAK *(Factoring RSA Export Keys)*	Use MitM to downgrade key systems used for symmetric key exchange to export-grade cryptography, then factor weak RSA key.
Logjam	Similar to FREAK, but for Diffie-Hellman with standard primes.
Heartbleed	Buffer overflow in heartbeat message implementation of OpenSSL
Sweet32	Attack on 3DES-CBC → search for colliding ciphertext with known plaintext. *Alternative description: birthday attack on 64-bit block ciphers*
DROWN *(Decrypting RSA with Obsolete and Weakened eNcryption)*	Use of SSLv2 as a Bleichenbacher oracle to decrypt a TLS handshake