Drown Attack

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) is a security attack that exploits vulnerabilities in SSLv2 to decrypt RSA encrypted connections. It targets servers that still support the obsolete and insecure SSLv2 protocol, even if they primarily use newer TLS versions. Many servers have SSLv2 enabled for backwards compatibility.

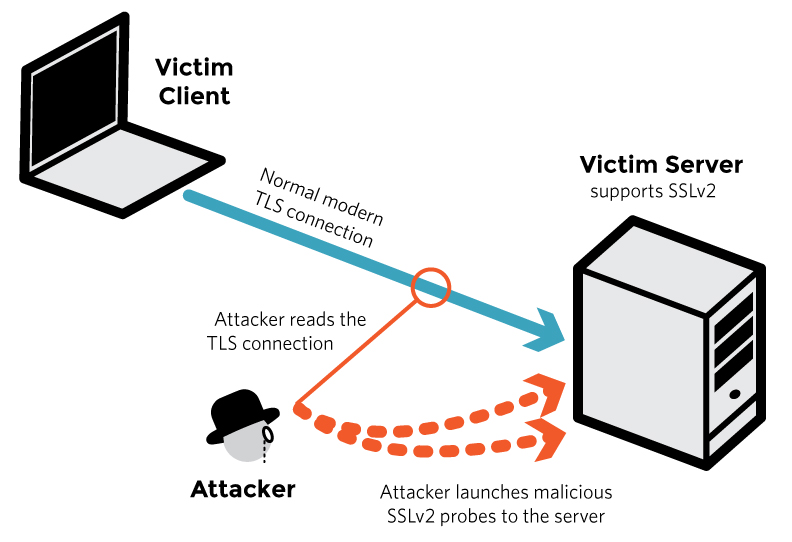
Overview:

These days most modern servers don't support SSLv2 and use other protocols like TLS. Yet in

2016, out of 36 million HTTPS servers, 6 million support SSLv2 [1].

In the Drown attack, the attacker uses the SSLv2 protocol in order to break the TLS connection.

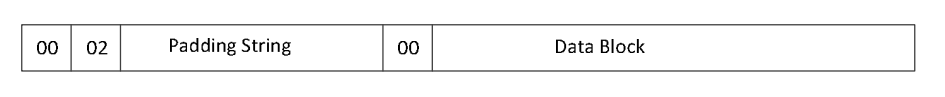
As shown in the figure below, the client that doesn't support SSLv2 sends a request to a server using TLS protocol. Although this connection is through TLS, the server might support SSLv2 too. Or in some cases, there might be another server supporting SSLv2 that shares the same key with the former server. In this case, the attacker intercepts and captures the traffic between the client and the server. Then it sends the traffic to the SSLv2 server multiple times, each time with a little modification in order to collect some information. Using this information it can then decrypt the RSA ciphertext. The decryption step is done using the Bleichenbacher attack.



Details of decryption using Bleichenbacher:

Bleichenbacher's padding oracle attack is an adaptive chosen ciphertext attack against PKCS#1 v1.5, the RSA padding standard used in SSL and TLS. It enables the decryption of RSA ciphertexts if a server distinguishes between correctly and incorrectly padded RSA plaintexts, and was termed the “million-message attack”.

As shown in Figure below, in PKCS#1 v1.5 encryption padding data being encrypted has a specific format. When data is being sent to the server, it decrypts the data and validates the format. If the format has a problem the server returns 1, in case of proper format it returns 0.



Despite bleichenbacher that attacks TLS directly with key length of 384 bit, Drown attacks deals with short secret for export grade crypto which means the key length is 40 bits. Also in TLS, the server chooses type of cipher suites, so we don't have information about exact length of the key.

Morph TLS connection : The connection captured is not compatible with SSLv2 oracel and it can not decrypt it. So it is needed to find SSLv2 format for the ciphertext.

decrypyt the key using bleichenbacher: send modified ciphertext multiple times in order to narrow down the possible answers and continue till only one solution remains.

References:

[1] Aviram, N., Schinzel, S., Somorovsky, J., Heninger, N., Dankel, M., Steube, J., Valenta, L., Adrian, D., Halderman, J.A., Dukhovni, V. and Käsper, E., 2016. {DROWN}: Breaking {TLS} Using {SSLv2}. In *25th USENIX Security Symposium (USENIX Security 16)* (pp. 689-706).