Transport Layer Security (TLS)

Certificate

Legacy Certificates

By legacy we mean distrusted certificates. An example from the past is the distrust of the Symantec PKI [1]. The best solution to date is, to replace the existing distrusted certificate with a new one from any Certificate Authority trusted by Google, Mozilla, Apple and Microsoft (and probably other browser vendors).

- [1] Google Blog Article

Misconfigured Chain

A correctly configured webserver should provide clients with the whole certificate chain up to the root certificate. If the server delivers a misconfigured certificate chain (e.g. incomplete or wrongly sorted) most browsers recover by verifying the certificate via AIA. [1]

This process, however, slows down page loading and browsers that do not support AIA may show the user a security warning.

- [1] Autority Information Access

Revoked Certificate

A Certificate may be revoked for various reasons (e.g. (possible) loss of the private key, domain closed, etc...). This means that the certificate is not valid anymore and users are shown a warning page in most browsers.

Protocol

TLS (Transport Layer Security) or SSL (Secure Socket Layer) is a protocol used to securely transmit encrypted data. Since SSL v3 the protocol is known as TLS, where TLS 1.0 corresponds to SSL v3.1. The currently recommended versions are TLS 1.2 and TLS 1.3. All the other versions are considered weak or contain vulnerabilities.

SSL v3/SSL v3.1/TLS 1.0

Those versions have also considerable security vulnerabilities. A well known attack is the Chained Initialization Vector CBC Mode MiTM Weakness (BEAST) attack. The attack is based on the usage of the CBC mode for encrypting the block ciphers and enables Man-in-The-Middle attacks which can be used to obtain plaintext HTTP header data. [1] Additionally, the key derivation function for the master key depends on a MD5 hash function. The possibility of collision based attacks let the protocol be considered as insecure in general. In October 2014 the POODLE attack has been published. This attack targets all implementations of SSL v3/TLS 1.0 which leads to the point that this protocol is not recommended to use any more. Using a Man-in-The-Middle attack, encrypted data can be decrypted and an attacker can gain access to plain text data. [2]

- [1] CVE-2011-3389
- [2] CVE-2014-3566

TLS 1.1 deprecation

The Internet Engineering Task Force (IETF) no longer recommends the use of TLS versions older than TLS 1.2. According to the following draft document (https://datatracker.ietf.org/doc/draft-ietf-tls-oldversions-deprecate/) TLS 1.0 and TLS 1.1 are deprecated. Negotiation of TLS 1.0 or 1.1 from any version of TLS MUST NOT be permitted. All major browser vendors are deprecating support for these versions of TLS by March 2020.

- [1] Google: https://blog.chromium.org/2019/10/chrome-ui-for-deprecating-legacy-tls.html
- [2] Mozilla: https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
- [3] Apple: https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/
- [4] Microsoft: https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/

Ciphers

DES

The recommended key length for TLS is at least 128 bits. [1] Keys with a shorter length could be broken and would allow the decryption of communications. The Data Encryption Standard (DES) is using only 56 bits. Therefore, DES based cipher suites should not be used.

- [1] SSL/TLS Deployment Best Practices

3DES

3DES or Triple-DES is a cryptographic block cipher algorithm which uses 64-bit blocks for data encryption between a client and server. Mostly used for establishing HTTPS connections, this cipher is known to be weak due to his short block size (in comparison, AES uses 128-bit blocks). With the emergence of the Sweet32 attack, there is a documented way of exploiting this trait. [1] The security measures of 3DES start to crumble whenever the birthday bound is reached. The point, at which a collision between the encrypted blocks is expected. Under certain circumstances, the attacker can then retrieve sensible data like session cookies.

- [1] Sweet32: Birthday attacks on 64-bit block ciphers in TLS

Export

Export Cipher Suites are weak by design. They are encrypted but only with weak key material. This leads to the fact that the encryption can be broken very easily as there are used 40 bit or 56 bit algorithms.

IDEA

IDEA uses 64-bit blocks for encryption which is considered as weak. Per RFC5469 this cipher is deprecated. It has been completely removed in TLS 1.2.

LOW

LOW are low strength encryption cipher suites, using 64 or 56 bit encryption algorithms but excluding export cipher suites. As of OpenSSL 1.0.2g, this is disabled in default builds. Src:

OpenSSL

Null

Using Null ciphers mean that no encryption for the data is used at all. They do not offer any privacy or security for the user of a web service. For this reason it is urgently recommended not to use Null ciphers.

RC2

It is advised not to use RC2 for encryption as it has an insufficient key size and is therefore seen as untrustworthy.

- [1] On the Design and Security of RC2

RC4

It has been known that RC4 has a weakness in its encryption and should therefore be avoided. On the other hand, there is no secure alternative as many clients still require RC4 support. However, since March 2013, RC4 is demonstrably broken and is classified as insecure in combination with TLS (Transport Layer Security). [1] The attack demonstrates that parts of the plain text can be recovered. For this reason, it is recommended that the support for this cipher should be removed in the near future.

- [1] RC4 Attack

SEED

SEED is an older South Korean cipher. OWASP recommends to not use this (and other older) cipher anymore.

Hash Functions

MD5

The use of the MD5 hash algorithm should be avoided in general as this algorithm is prone for collision attacks. [1]

- [1] How to Break MD5 and Other Hash Functions

SHA1

Known for its cryptographic and mathematical weaknesses, the SHA-1 hash algorithm was already replaced by the SHA-2 ciphers family as the recommended standard in 2002. As of begin of 2017, popular browser vendors like Microsoft, Mozilla or Google will stop accepting SHA-1 signed TLS certificates. Instead, the browsers will start displaying a warning sign if any certificate in the trust chain uses the outdated algorithm. Therefore, the upgrade of the web server's and of all intermediate certificates to the SHA-2 family should be considered as soon as possible.

- [1] Moving to SHA2
- [2] A further update on SHA-1 certificates in Chrome

Key Exchange Algorithms

Anonymous Diffie-Hellmann

Anonymous Diffie-Hellman Cipher Suites are used for anonymous Diffie-Hellman communications in which neither party is authenticated. Therefore this mode is vulnerable to Man-in-The-Middle attacks. [1]

- [1] RFC: The TLS Protocol Version 1.0

Revision #2
Created 2021-08-02 07:26:57 UTC by Patrick Wall
Updated 2021-08-02 08:07:39 UTC by Patrick Wall