Encryption Protocols [1]

Recommendations for SSL/TLS

In the world of certificate-based encryption protocols, only TLSv1.2 remains standing today. Previous versions of TLS (and all versions of SSL) now suffer from vulnerabilities and problems that make them untenable in 2018. In addition to the problems with earlier protocols, the big Internet players have signaled that it's time to move on: Microsoft recently announced that they'll be disabling all protocols prior to TLSv1.2 for Office 365 beginning on March 1. Google has removed TLSv1.0 fallback from Chrome and has plans to do the same for TLSv1.1 in the near future. And, finally, the PCI DSS standard no longer accepts TLSv1.0 as passable after June of this year.

With this in mind, the University IT Security Office recommends that web servers offering encrypted content via TLS do so ONLY via TLSv1.2 or higher going forward. Existing server configurations should also be updated for strict TLSv1.2 compatibility.

In regard to the cipher suites used within TLSv1.2, we still follow the Mozilla Foundation's recommendations [2]. However, in prior recommendations we suggested that their Intermediate compatibility group of cipher suites should be used. We are updating our recommendation to suggest that only the Modern compatibility group [3] now be used.

It is crucial that their recommended general purpose ciphersuite be implemented exactly as-is in order achieve proper cipher prioritization, as well as to be sure that Perfect Forward Secrecy is enabled. Perfect Forward Secrecy is important to protect any TLS encrypted data that may be captured and stored by third parties with access to the transit networks that data travels on. Without PFS, the likelihood of a Man in the Middle-style attack during transit, or the eventual decryption of captured encrypted data, is significantly increased.

To recap:

- Allow only the TLSv1.2 protocol. All others should be explicitly disabled.
- Use the Modern compatibility cipher list provided Mozilla exactly as it is written.
- Where applicable, make sure your OS supports the latest and greatest version of OpenSSL.

Source URL: https://security.duke.edu/encryption-protocols

Links
[1] https://security.duke.edu/encryption-protocols