History of SSL/TLS

Kyu Doun Sim

kdsim@connect.ust.hk

Motivation

The following written report examines the history of SSL/TLS and the weakness or vulnerabilities that it overcame over its development. It would be interesting to see how the protocol responded to different vulnerabilities and its solution. Hopefully, users will be able to get a glimpse of where the development of the protocol will lead to.

Inception

Terminologies(Difference between TLS and SSL)

What is the difference between SSL and TLS? And why do they often come together? Are they referring to the same protocol?

Historical Version

Impactful Events

Future

Conclusion

References

<https://www.decalage.info/file_formats_security/pdf>

<http://www.malwaretracker.com/pdfthreat.php>

<https://www.investintech.com/resources/blog/archives/84-13-ways-the-pdf-is-vulnerable.html>

<https://www.welivesecurity.com/2018/05/15/tale-two-zero-days/>

<https://securityxploded.com/pdf_vuln_exploits.php>

<https://security.stackexchange.com/questions/64052/can-a-pdf-file-contain-a-virus>

<https://www.foxitsoftware.com/blog/understanding-security-vulnerabilities-in-pdfs/>

<http://pralab.diee.unica.it/sites/default/files/aisec09f-corona.pdf>

<https://www.zdnet.com/article/windows-10-or-mac-user-patch-adobe-reader-and-acrobat-now-to-fix-9-critical-security-flaws/>

<https://www.brightfort.com/pdffix.html>

<https://www.websecurity.digicert.com/en/hk/security-topics/what-is-ssl-tls-https>