Literature Search

Yiwen Tang Jiayi Zhang Yawei Zhang Rui Zhang

February 14, 2020

1 Proposed and Established Standards

1. Dierks, T., & Allen, C. (1999). The TLS protocol version 1.0.
2. Kaliski, B. (1998). PKCS# 1: RSA encryption version 1.5. RFC 2313, March.
3. Simon, D., Aboba, B., & Hurst, R. (2008). The EAP-TLS authentication protocol. RFC 5216.
4. Rescorla, E. (2000). Http over TLS.
5. Dierks, T., & Rescorla, E. (2008). The transport layer security (TLS) protocol version 1.2.
6. Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., & Wright, T. (2003). Transport layer security (TLS) extensions.

2 Landmark Papers

1. Dolev, D., & Yao, A. (1983). On the security of public key protocols. IEEE Transactions on information theory, 29(2), 198-208.
2. Rescorla, E., & Modadugu, N. (2006). Datagram transport layer security.
3. Krawczyk, H., Paterson, K. G., & Wee, H. (2013, August). On the security of the TLS protocol: A systematic analysis. In Annual Cryptology Conference (pp. 429-448). Springer, Berlin, Heidelberg.
4. Hoffman, P., & Schlyter, J. (2012). The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA. RFC 6698, August.
5. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
6. Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol. In The Second USENIX Workshop on Electronic Commerce Proceedings (Vol. 1, No. 1, pp. 29-40).
7. Ray, M., & Dispensa, S. (2009). Renegotiating tls.
8. Danezis, G. (2009). Traffic Analysis of the HTTP Protocol over TLS.
9. Saito, T., Sekiguchi, K., & Hatsugai, R. (2008, September). Authentication Binding between TLS and HTTP. In International Conference on Network-Based Information Systems (pp. 252-262). Springer, Berlin, Heidelberg.

10. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, 61(3), 527-542.

11. Paulson, L. C. (1999). Inductive analysis of the Internet protocol TLS. ACM Transactions on Information and System Security (TISSEC), 2(3), 332-351.

3 Current Research

1. Rowan, S., Clear, M., Gerla, M., Huggard, M., & Goldrick, C. M. (2017). Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. arXiv preprint arXiv:1704.02553.

2. Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47-54.

3. "Merzdovnik, G., Falb, K., Schmiedecker, M., Voyiatzis, A. G., & Weippl, E. (2016, July). Whom you gonna trust? a longitudinal study on TLS notary services. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 331-346). Springer, Cham.

4. Onieva, J. A., & Zhou, J. (2008). Secure multi-party non-repudiation protocols and applications (Vol. 43). Springer Science & Business Media

5. Giesen, F., Kohlar, F., & Stebila, D. (2013, November). On the security of TLS renegotiation. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 387-398).

6. Szalachowski, P. (2018). Blockchain-based tls notary service. arXiv preprint arXiv:1804.00875.

7. Bhargavan, K., Fournet, C., Kohlweiss, M., Pironti, A., & Strub, P. Y. (2013, May). Implementing TLS with verified cryptographic security. In 2013 IEEE Symposium on Security and Privacy (pp. 445-459). IEEE.

8. Nykvist, C., Sjöström, L., Gustafsson, J., & Carlsson, N. (2018, March). Server-side adoption of certificate transparency. In International Conference on Passive and Active Network Measurement (pp. 186-199). Springer, Cham.

9. Moriarty, K., & Trammell, B. (2010). Transport of Real-time Inter-network Defense (RID) Messages. RFC 6046, November.

10. Szalachowski, P., Chuat, L., & Perrig, A. (2016, March). PKI safety net (PKISN): Addressing the too-big-to-be-revoked problem of the TLS ecosystem. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 407-422). IEEE.

11. Nofal, R. A., Tran, N., Garcia, C., Liu, Y., & Dezfouli, B. (2019, November). A Comprehensive Empirical Analysis of TLS Handshake and Record Layer on IoT Platforms. In Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (pp. 61-70).

12. Lerner, S. (2015). Renegotiation and TLSNotary. IETF TLS mailing list.

13. Heiss, J., Eberhardt, J., & Tai, S. (2019, July). From oracles to trustworthy data on-chaining systems. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 496-503). IEEE.

14. Ritzdorf, H., Wüst, K., Gervais, A., Felley, G., & Capkun, S. (2017). TLS-N: Non-repudiation over TLS Enabling-Ubiquitous Content Signing for Disintermediation. IACR Cryptology ePrint Archive, 2017, 578.

15. Zhang, J., Yang, L., Cao, W., & Wang, Q. (2020). Formal Analysis of 5G EAP-TLS Authentication Protocol Using ProVerif. IEEE Access.

16. Simos, D. E., Bozic, J., Garn, B., Leithner, M., Duan, F., Kleine, K., ... & Wotawa, F. (2019). Testing TLS using planning-based combinatorial methods and execution framework. Software quality journal, 27(2), 703-729. "

4 Academic and Industry Published Tutorials

1. Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016, October). Town crier: An authenticated data feed for smart contracts. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 270-282).

2. Ritzdorf, H. (2018). Advances in Designing Trustworthy Cloud Services (Doctoral dissertation, ETH Zurich