REFERENCES

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., & Zimmermann, P. (2015). Imperfect forward secrecy: How diffie-hellman fails in practice. *Proceedings of the ACM Conference on Computer and Communications Security*, *2015-October*, 5–17. https://doi.org/10.1145/2810103.2813707

Beurdouche, B., Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., Strub, P. Y., & Zinzindohoue, J. K. (2017). A messy state of the union: Taming the composite state machines of TLS. *Communications of the ACM*, *60*(2), 99–107. https://doi.org/10.1145/3023357

Halderman, J. A., & Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9269*, 35–53. https://doi.org/10.1007/978-3-319-22270-7_3

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., Manthorne, C., Churchill, E. F., & Consolvo, S. (2017). *Stories from survivors: Privacy & security practices when coping with intimate partner abuse*. https://research.google/pubs/pub46080/

Specter, M. A., Koppel, J., Weitzner, D., Specter MIT, M. A., Koppel MIT, J., & Weitzner MIT, D. (2020). The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in {U.S}. Federal Elections. In *arXiv*. https://www.usenix.org/conference/usenixsecurity20/presentation/zhou-jie

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the estonian internet voting system. *Proceedings of the ACM Conference on Computer and Communications Security*, 703–715. https://doi.org/10.1145/2660267.2660315

Valenta, L., Cohney, S., Liao, A., Fried, J., Bodduluri, S., & Heninger, N. (2016). Factoring as a Service. *Financial Cryptography*, *9603 LNCS*, 321–338. https://doi.org/10.1007/978-3-662-54970-4_19

Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, & J. A. Halderman. (2015, March 3). *Tracking the FREAK Attack*. https://freakattack.com/