References

[1] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the adoption of secure communication tools. In *IEEE Symposium on Security and Privacy*, 2017.

[2] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[3] A. Afanasyev, J. Halderman, S. Ruoti, K. Seamons, Y. Yu, D. Zappala, and L. Zhang. Content-based security for the web. In *New Security Paradigms Workshop (NSPW 2016)*. ACM, 2016.

[4] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *USENIX Annual Technical Conference*, pages 181–194, 2016.

[5] E. Atwater, C. Bocovich, U. Hengartner, E. Lank, and I. Goldberg. Leading Johnny to water: Designing for usability and trust. In *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, 2015.

[6] W. Bai, M. Namara, Y. Qian, P. G. Kelley, M. L. Mazurek, and D. Kim. An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 113–130, Denver, CO, 2016. USENIX Association.

[7] A. Bangor, P. Kortum, and J. Miller. An empirical evaluation of the System Usability Scale. *International Journal of Human–Computer Interaction*, 24(6):574–594, 2008.

[8] A. Bangor, P. Kortum, and J. Miller. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 4(3):114–123, 2009.

[9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

[10] N. Borisov, I. Goldberg, and E. Brewer. Off-the-record communication, or, why not to use pgp. In *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 77–84. ACM, 2004.

[11] J. Brooke. SUS — a quick and dirty usability scale. In *Usability Evaluation in Industry*. CRC Press, 1996.

[12] I. Brown, A. Back, and B. Laurie. Forward secrecy extensions for OpenPGP. `https://tools.ietf.org/html/draft-brown-pgp-pfs-03`, 2001. IETF Draft (work in progress).

[13] I. Brown and B. Laurie. Security against compelled disclosure. In *Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference*, pages 2–10. IEEE, 2000.

[14] R. Buck, R. Lee, P. Lundrigan, and D. Zappala. WiFu: A composable toolkit for experimental wireless transport protocols. In *Proceedings of 9th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 299–307, 2012.

[15] BYU Internet Research Lab. WiFu: A composable toolkit for experimental wireless transport protocols. `https://github.com/zappala/wifu`. Accessed: September 23, 2015.

[16] L. J. Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3), 2009.

[17] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. *Journal of Cryptology*, 20(3):265–294, Jul 2007.

[18] R. Chandramouli, S. Garfinkel, S. Nightingale, and S. Rose. NIST special publication 800-177: Trustworthy email. http://dx.doi.org/10.6028/NIST.SP.800-177, 2016. Accessed November 15, 2016.

[19] S. Dechand, D. Schürmann, T. IBR, K. Busse, Y. Acar, S. Fahl, and M. Smith. An empirical study of textual key-fingerprint representations. In *Twenty-Fifth USENIX Security Symposium (USENIX Security 2016)*. USENIX Association, 2016.

[20] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. Halderman. Neither snow nor rain nor mitm... an empirical analysis of mail delivery security. In *Proceedings of the 2015 Internet Measurement Conference (IMC)*, 2015.

[21] I. Foster, J. Larson, M. Masich, A. C. Snoeren, S. Savage, and K. Levchenko. Security by any other name: On the effectiveness of provider based email security. In *Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.

[22] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller. How to make secure email easier to use. In *ACM CHI*, 2005.

[23] S. L. Garfinkel and R. C. Miller. Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In *Proceedings of the First Symposium on Usable Privacy and Security*, pages 13–24. ACM, 2005.

[24] M. D. Green and I. Miers. Forward secure asynchronous messaging from puncturable encryption. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 305–320. IEEE, 2015.

[25] R. Holz, J. Amann, O. Mehani, M. Wachs, and M. A. Kaafar. TLS in the wild: An internet-wide analysis of TLS-based protocols for electronic communication. In *NDSS*, 2015.

[26] R. Holz, J. Amann, O. Mehani, M. Wachs, and M. A. Kaafar. TLS in the wild: An internet-wide analysis of TLS-based protocols for electronic communication. In *Twenty-Fourth Network and Distributed System Security Symposium (NDSS 2016)*, San Diego, CA, 2016. The Internet Society.

[27] H.-F. Hsieh and S. E. Shannon. Three approaches to qualitative content analysis. *Qualitative health research*, 15(9):1277–1288, 2005.

[28] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan. An empirical study of namecoin and lessons for decentralized namespace design. In *WEIS*, 2015.

[29] A. Lerner, E. Zeng, and F. Roesner. Confidante: Usable encrypted email: A case study with lawyers and journalists. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*, pages 385–400. IEEE, 2017.

[30] E. K. Maloney, M. K. Lapinski, and K. Witte. Fear appeals and persuasion: A review and update of the extended parallel process model. *Social and Personality Psychology Compass*, 5(4):206–219, 2011.

[31] M. Marlinspike. Advanced cryptographic ratcheting. `https://whispersystems.org/blog/advanced-ratcheting/`, 2013. Accessed: November 10, 2016.

[32] W. Mayer, A. Zauner, M. Schmiedecker, and M. Huber. No need for black chambers: Testing TLS in the e-mail ecosystem at large. In *IEEE ARES*, 2016.

[33] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman. Coniks: Bringing key transparency to end users. In *Proceedings of the 24th USENIX Security Symposium*, 2015.

[34] T. Monson. Usable secure email through short-lived keys. Master's thesis, Brigham Young University, Provo, UT, 2017.

[35] M. O'Neill, S. Heidbrink, S. Ruoti, J. Whitehead, D. Bunker, L. Dickinson, T. Hendershot, J. Reynolds, K. Seamons, and D. Zappala. TrustBase: An architecture to repair and strengthen certificate-based authentication. In *Proceedings of the 26th USENIX Security Symposium*, 2017.

[36] M. O'Neill, S. Ruoti, K. Seamons, and D. Zappala. TLS proxies: Friend or foe? In *Internet Measurement Conference*. ACM, 2016.

[37] M. O'Neill, S. Ruoti, K. Seamons, and D. Zappala. Tls inspection: How often and who cares? *IEEE Internet Computing*, 21(3):22–29, 2017.

[38] H. Orman. *Encrypted Email: The History and Technology of Message Privacy.* Springer, 2015.

[39] T. Perrin and M. Marlinspike. Double ratchet algorithm. `https://github.com/trevp/double_ratchet/wiki`, 2016. Accessed: November 12, 2016.

[40] K. Renaud, M. Volkamer, and A. Renkema-Padmos. Why doesn't Jane protect her privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2014.

[41] D. Ripplinger, S. Warnick, and D. Zappala. First-principles modeling of wireless networks for rate control. In *Proceedings of 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, pages 3794–3799, 2011.

[42] C. Robison, S. Ruoti, T. W. van der Horst, and K. E. Seamons. Private Facebook chat. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, pages 451–460. IEEE, 2012.

[43] S. Ruoti, J. Andersen, S. Heidbrink, M. ONeill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons. were on the same page: A usability study of secure email using pairs of novice users. In *34th Annual ACM Conference on Human Facors and Computing Systems (CHI 2016).* CHI, 2016.

[44] S. Ruoti, J. Andersen, T. Hendershot, D. Zappala, and K. Seamons. Private webmail 2.0: Simple and easy-to-use secure email. In *29th ACM Symposium on User Interface Software and technology (UIST 2016).* ACM, 2016.

[45] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client, 2015. arXiv preprint arXiv:1510.08555.

[46] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. *arXiv preprint arXiv:1510.08555*, 2015.

[47] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, and K. Seamons. Confused Johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 5. ACM, 2013.

[48] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. Seamons. Weighing context and trade-offs: How suburban adults selected their online security posture. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 211–228, Santa Clara, CA, 2017. USENIX Association.

[49] S. Ruoti, M. O'Neill, D. Zappala, and K. Seamons. User attitudes toward the inspection of encrypted traffic. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[50] S. Ruoti, K. Seamons, and D. Zappala. Layering security at global control points to secure unmodified software. In *IEEE Secure Development Conference (SecDev 2017)*, pages 42–49. IEEE, 2017.

[51] S. Ruoti, D. Zappala, and K. Seamons. Messageguard: Retrofitting the web with user-to-user encryption. *arXiv preprint arXiv:1510.08943*, 2015.

[52] J. Sauro. *A practical guide to the system usability scale: Background, benchmarks & best practices*. Measuring Usability LLC, 2011.

[53] B. Schneier and C. Hall. An improved e-mail security protocol. In *Proceedings of the 13th Annual Computer Security Applications Conference*, pages 227–230. IEEE, 1997.

[54] S. Schröder, M. Huber, D. Wind, and C. Rottermanner. When SIGNAL hits the fan: On the usability and security of state-of-the-art secure mobile messaging. In *First European Workshop on Usable Security (EuroUSEC 2016)*, 2016.

[55] S. Sheng, L. Broderick, C. Koranda, and J. Hyland. Why Johnny still can't encrypt: evaluating the usability of email encryption software. In *Proceedings of the Second Symposium On Usable Privacy and Security - Poster Session*, 2006.

[56] G. Stewart and D. Lacey. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1):29–38, 2012.

[57] J. Tan, L. Bauer, J. Bonneau, L. F. Cranor, J. Thomas, and B. Ur. Can unicorns help users compare crypto key fingerprints? In *Thirty-Fifth ACM Conference on Human Factors and Computing Systems (CHI 2017)*, pages 3787–3798. ACM, 2017.

[58] T. S. Tullis and J. N. Stetson. A comparison of questionnaires for assessing website usability. In *Usability Professional Association Conference*, pages 1–12, 2004.

[59] M. Tungare and M. Pérez-Quiñones. best if used by: Expiration dates for email. In *Proceedings of the 2009 CHI Workshop on Interacting with Temporal Data*, 2009.

[60] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. Sok: Secure messaging. In *2015 IEEE Symposium on Security and Privacy*, pages 232–249. IEEE, 2015.

[61] E. Vaziripour, M. ONeill, J. Wu, S. Heidbrink, K. Seamons, and D. Zappala. Social authentication for end-to-end encryption. In *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[62] E. Vaziripour, J. Wu, M. O'Neill, J. Whitehead, S. Heidbrink, K. Seamons, and D. Zappala. Is that you, alice? a usability study of the authentication ceremony of secure messaging applications. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 29–47, Santa Clara, CA, 2017. USENIX Association.

[63] L. Wang, D. Ripplinger, A. Rai, S. Warnick, and D. Zappala. A convex optimization approach to decentralized rate control in wireless networks with partial interference. In *Proceedings of 49th IEEE Conference on Decision and Control (CDC)*, pages 639–646, 2010.

[64] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium*, 1999.

[65] K. Witte. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4):329–349, 1992.

[66] K. Witte. Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, 61(2):113–134, 1994.

[67] J. Yan, A. Blackwell, R. Anderson, and A. Grant. The memorability and security of passwords-some empirical results. *Technical Report-University Of Cambridge Computer Laboratory*, page 1, 2000.

[68] X. Zhang, R. Buck, and D. Zappala. Experimental performance evaluation of ATP in a wireless mesh network. In *Proceedings of 8th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 122–131, 2011.