

Figure 6: Distribution of payload lengths by type for WhatsApp, Viber, and Telegram.

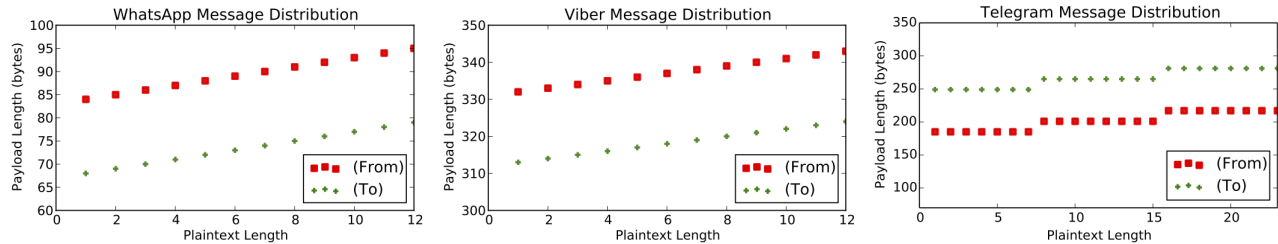


Figure 7: Scatterplot of plaintext message lengths versus payload lengths for WhatsApp, Viber, and Telegram.

6. REFERENCES

- [1] Spencer Ackerman and James Ball. Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ. <http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo>, February 2014.
- [2] Inc. Apple. iOS Security. http://images.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf, February 2014.
- [3] Agathe Battestini, Vidya Setlur, and Timothy Sohn. A Large Scale Study of Text-Messaging Use. In *Proceedings of the 12th Conference on Human Computer Interaction with Mobile Devices and Services*, pages 229–238, 2010.
- [4] Marjorie Cohn. NSA Metadata Collection: Fourth Amendment Violation. http://www.huffingtonpost.com/marjorie-cohn/nsa-metadata-collection-f_b_4611211.html, January 2014.
- [5] K.P. Dyer, S.E. Coull, T. Ristenpart, and T. Shrimpton. Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, pages 332–346, May 2012.
- [6] Michael Frister and Martin Kreichgauer. PushProxy: A Man-in-the-Middle Proxy for iOS and OS X Device Push Connections. <https://github.com/meeee/pushproxy>, May 2013.
- [7] Dan Goodin. Can Apple Read Your iMessages? Ars Deciphers End-to-End Crypto Claims. <http://arstechnica.com/security/2013/06/can-apple-read-your-imessages-ars-deciphers-end-to-end-crypto-claims/>, June 2013.
- [8] Matthew Green. Can Apple read your iMessages? <http://blog.cryptographyengineering.com/2013/06/can-apple-read-your-imessages.html>, June 2013.
- [9] Andy Greenberg. Apple Claims It Encrypts iMessages And Facetime So That Even It Can't Decipher Them. <http://www.forbes.com/sites/andygreenberg/2013/06/17/apple-claims-it-encrypts-imessages-and-facetime-so-that-even-it-cant-read-them>, June 2013.
- [10] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H. Witten. The WEKA Data Mining Software: An Update. *SIGKDD Explorations*, 11(1), 2009.
- [11] Dominik Herrmann, Rolf Wendolsky, and Hannes Federrath. Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naive-Bayes Classifier. In *Proceedings of the ACM Workshop on Cloud Computing Security*, pages 31–42, November 2009.
- [12] M. Liberatore and B. Levine. Inferring the Source of Encrypted HTTP Connections. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pages 255–263, October 2006.
- [13] Ben Lovejoy. Massive Growth in Apple's Cloud-Based Services Eclipsed by Debate on Financials. <http://www.macrumors.com/2013/01/24/massive-growth-in-apples-cloud-based-services-eclipsed-by-debate-on-financials>, January 2013.
- [14] Parmy Olson. Watch Out, Facebook: WhatsApp Climbs Past 400 Million Active Users. <http://www.forbes.com/sites/parmyolson/2013/12/19/watch-out-facebook-whatsapp-climbs-past-400-million-active-users/>, December 2013.
- [15] Andriy Panchenko, Lukas Niessen, Andreas Zinnen, and Thomas Engel. Website Fingerprinting in Onion Routing-based Anonymization Networks. In *Proceedings of the Workshop on Privacy in the Electronic Society*, pages 103–114, October 2011.
- [16] Q. Sun, D. R. Simon, Y. Wang, W. Russell, V. N. Padmanabhan, and L. Qiu. Statistical Identification of Encrypted Web Browsing Traffic. In *Proceedings of the 23rd Annual IEEE Symposium on Security and Privacy*, pages 19–31, May 2002.
- [17] Jörg Tiedemann. Parallel Data, Tools and Interfaces in OPUS. In *Proceedings of the 8th International Conference on Language Resources and Evaluation*, May 2012.
- [18] Andrew M. White, Austin R. Matthews, Kevin Z. Snow, and Fabian Monrose. Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on Fon-iks. In *Proceedings of the 32nd IEEE Symposium on Security and Privacy*, pages 3–18, May 2011.
- [19] C. Wright, L. Ballard, S. Coull, F. Monrose, and G. Masson. Spot Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, pages 35–49, May 2008.
- [20] Charles V. Wright, Scott E. Coull, and Fabian Monrose. Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis. In *Proceedings of the 16th Network and Distributed Systems Security Symposium*, pages 237–250, February 2009.