Ubiquitous Metadata Private Communication

Alexandre Pauwels
University of Cambridge
ap2453@cam.ac.uk

In 2016, WhatsApp completed the integration of Signal's double-ratchet end-to-end encryption protocol into its app. [3] In 2017, it announced it had over one billion daily active users, and in 2020, over two billion total registered users. [4, 5] Combining its massive scale and familiar interface with strong cryptography allowed WhatsApp to bring forth what PGP had failed to do before it: ubiquitous data confidentiality. This is not the case for metadata privacy.

Signal, WhatsApp, and the various other encrypted messaging contenders may differ in the implementation details of their encryption protocols, but they are alike in one sense: they know who is talking to whom, how much, and when. No existing large-scale messaging system provides metadata-private communications.

Metadata-private systems exist, but at a scale orders of magnitude below that of a service like WhatsApp. Not only do they require users to download special applications that are often difficult to configure, but a subset of these users must be willing to donate their time, money, and expertise to running nodes in the network through which requests can be routed. [1] This creates a divide between users and operators, and means networks cannot rapidly scale: a massive increase in users does not lead to a proportional increase in operators. [6]

Mobile devices and reusing existing communications infrastructure are key to closing the gap between scale and metadata privacy. Rather than making devices users of a metadata-private communications network, we achieve ubiquitous metadata-privacy once each device is both a user and an operator of the network. To test this concept, this work uses email as the transport layer of a metadata-private communications protocol. Each inbox, and therefore mobile device, becomes a mix node in the network. We use the Sphinx packet format modified to use puncturable encryption along with Poisson-distributed delays and cover traffic inspired by modern anonymity systems like Loopix [2]. We show that using this construct achieves sender anonymity, receiver anonymity, and sender/receiver unlinkability while maintaining perfect forward secrecy in the asynchronous communications setting.

Building such a protocol within the constraints of mobile systems presents a unique set of challenges. Mobile devices guarantee no availability, and existing messaging systems are built with spam and abuse prevention tactics that rely on metadata to work. The prevailing view is that it is difficult or impossible to correctly build data security on top of existing insecure systems. The email-based protocol is therefore evaluated across the following categories to test feasibility:

1. User interface - Are non-technical users able to use this system with no additional input?
2. Availability - Endpoints cannot guarantee availability or synchronicity, how does this affect our routing and cryptographic protocols?
3. Spam and abuse prevention - Existing messaging systems rely on metadata for spam and abuse prevention, is this still possible in our construct?
4. Integration - Can metadata-anonymous protocols run on top of existing systems, do they require cooperation from the systems' developers, and what extra resources do they require?
5. Security - Do we achieve sender anonymity, receiver anonymity, third-party unlinkability, and perfect forward secrecy?

Finally, we generalize requirements for expanding this protocol to non-email transport layers.

References

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153, San Jose, CA, USA, May 2017. IEEE.

[2] Ania Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The Loopix Anonymity System, March 2017. arXiv:1703.00536 [cs].

[3] WhatsApp. End-to-end encryption, 2016.

[4] WhatsApp. Connecting One Billion Users Every Day, 2017.

[5] WhatsApp. Two Billion Users – Connecting the World Privately, 2020.

[6] Tsuen-Wan "Johnny" Ngan, Roger Dingledine, and Dan S. Wallach. Building Incentives into Tor. In *Financial Cryptography and Data Security*, volume 6052, pages 238–256. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. Series Title: Lecture Notes in Computer Science.