Balancing Privacy and Accountability on Encrypted Messaging Platforms

Alistair Pattison and Nick Hopper

Encrypted messaging services like WhatsApp, Facebook Messenger, and Signal provide secure and deniable communication for billions across the world, but these exact properties prevent holding users accountable for sending messages that are abusive, misinformative, or otherwise harmful to society. This work introduces a protocol in which **the sender of an abusive message can be identified if there is sufficient agreement among a group of moderators**. The protocol **retains all security properties of the messaging service for unreported messages**.

The Protocol

This work extends a protocol by Issa, Alhaddad, and Varia called Hecate. In the Hecate protocol, every message requires a token

$$x_1 \coloneqq \textsc{Enc}(id_{src},\ pk_{mod}),$$

and an ephemeral key pair (pk_{eph}, sk_{eph}). When a user sends a message, she attaches the signature

$$\sigma_{src} = \textsc{Sign}_{sk_{eph}}(x_2)$$
$$x_2 \coloneqq x_1 \oplus H(m)$$

The signature binds x_1 to the sent message, and if the message is ever reported, the moderator decrypts x_1 with his private key to obtain the original sender's identity.

function $\textsc{CreateToken}(id_{usr})$
- Compute $x_1 \coloneqq \langle g^r,\ id_{usr} \oplus H(pk_{mod}^r)\rangle$ where $r \leftarrow_{\$} \mathbb{Z}_q$
- Package x_1 into a token and send a signature request to each moderator along with the randomness r.
- Each moderator verifies verifies x_1 and returns their signature share on the token.
- Once sufficient responces are recieved, combine the signature shares into into a valid signature.

function $\textsc{HandleReport}(m,\ x_1)$
- A coordinator sends a request to all n moderators containing the reported message m and the encrypted id, $x_1 = \langle c_1, c_2\rangle$.
- If the moderator believes that the message is worth acting upon, she responds with the decrption share $d_i \coloneqq c_1^{s_i}$.
- If enough decryption shares are received, the moderator recovers x_1.

Opinion: WhatsApp skewed Brazilian election, showing social media's danger to democracy

Dec 5, 2018 5:27 PM EDT

How WhatsApp Leads Mobs to Murder in India

By Vindu Goel, Suhasini Raj and Priyadarshini Ravichandran

July 18, 2018

Signal app warns it will quit UK if law weakens end-to-end encryption

Boss of messaging app says users' trust at risk from powers in online safety bill to impose monitoring

Dan Milmo *Global technology editor*

Fri 24 Feb 2023 12.28 EST

On WhatsApp, fake news is fast — and can be fatal

By Elizabeth Dwoskin and Annie Gowen

July 23, 2018 at 8:20 p.m. EDT

Benchmarks

We implement the protocol in Rust where each party runs in a separate Docker container and communicates over HTTP.

TO BE COMPLETED FOR FINAL POSTER

← Download the extended abstract!

University of Minnesota
Driven to Discover℠