Researchers develop method to protect privacy and safety in encrypted messaging

September 12 2022, by Tom Fleischman

Credit: CC0 Public Domain

Cornell Tech researchers have developed a mechanism for preserving anonymity in encrypted messaging—which conceals message content but might not cloak the sender's identity—while simultaneously blocking unwanted or abusive messages.

Doctoral student and co-lead author Nirvan Tyagi presented the group's paper, "Orca: Blocklisting in Sender-Anonymous Messaging," at the 31st USENIX (Advanced Computing Systems Association) Symposium, held Aug. 10-12 in Boston.

Co-authors included Tom Ristenpart, professor of computer science at Cornell Tech and in the Cornell Ann S. Bowers College of Computing and Information Science; Julia Len, doctoral student in computer science; and Ian Miers, associate professor of computer science at the University of Maryland and a former postdoctoral associate at Cornell Tech.

This work is a continuation of research whose goal is to take significant steps toward safer online communication. Ristenpart is principal investigator of the project, "Privacy-Preserving Abuse Prevention for Encrypted Communications Platforms."

Platforms such as Signal, WhatsApp and Facebook Messenger rely on end-to-end encrypted (E2EE) messaging to preserve the confidentiality of the message, but user anonymity is not guaranteed. Signal recently introduced an anonymity-preserving feature, but it has been found to be susceptible to attack.

"While they prevent content from being leaked to the platform," Tyagi said, "this doesn't prevent other types of leakage of metadata."

While E2EE messaging provides strong confidentiality of the messages being sent, the platform can learn the identities of both the sender and recipient of every message sent over the network. Signal, a messaging app released in 2014 that now boasts more than 40 million users, has recently introduced a "sealed sender" protocol that ensures the sender's identity is never revealed to the platform.

This highlights a key tension in sender-anonymous systems: sender anonymity, while mitigating potentially abusive messages. E2E encryption by itself makes certain types of abuse mitigation more challenging, and sender anonymity only complicates those efforts. One example of abuse mitigation that is complicated by sender anonymity is blocklisting.

"That (sender-anonymous sender blocklisting) is a bit of an oxymoron," Tyagi said, "because we want the platform to be able to filter based on sender identities, but we also want sender anonymity from the platform."

With Orca, message recipients would register an anonymized blocklist with the platform. Senders construct messages that can be verified by the platform as being attributable to someone not on the blocklist.

Verification is achieved through group signatures, which allow users to sign messages anonymously on behalf of a group. The platform registers individual users, and the group's opening authority—the recipient—can trace the identity of each individual user.

If the sender is on the blocklist, or if the message is malformed, the platform rejects the message. But if the message is delivered, the recipient is guaranteed to be able to identify the sender.

Orca takes this efficiency one step further: Instead of creating and verifying a group signature for every message sent, the group signature will only be used periodically to mint new batches of one-time-use sender tokens from the platform. Messages can be sent by including a valid token for a recipient; these tokens, or access keys, are much more efficient for the platform to verify and require only a check against a list of used or blocked tokens.

"The sender sends a message, using cryptography they prove to the

platform that they're an authorized sender for the recipient and not on the recipient's blocklist," Tyagi said. "And they can do that in a way where they can still hide their identity from the platform."

Tyagi said this type of safeguard could be useful in a number of scenarios.

"Perhaps you're a whistleblower at a company, and you contact a journalist, which for most people is not a common occurrence," Tyagi said. "Then a big story appears; just the fact that someone from that company has been in recent contact with the journalist could raise a red flag.

"Or in the medical realm," he said, "just by the fact that you're communicating with, say, a cardiologist, could reveal confidential information about your health."

Future work will address the computational challenge of making sure a single cryptographic identity corresponds to a single human. It's one of many problems facing computer scientists as they address the tension between anonymity and abuse mitigation.

"Increased privacy can harm the ability to do certain types of abuse mitigation and accountability," Tyagi said. "The question is, can we make that tradeoff a little less costly with even better cryptography? And in some cases, we can."

More information: Nirvan Tyagi et al, Orca: Blocklisting in Sender-Anonymous Messaging (2022)

Provided by Cornell University