Beyond one server: Decentralizing secure group messaging

November 24 2021, by Daniel Tkacik

Credit: CC0 Public Domain

In May, WhatsApp made some controversial changes to its terms of service, leaving WhatsApp users with a choice: agree to the terms, or be forced to leave.

Similarly, journalists and activists who are worried about their messages being intercepted or spied on—especially in countries with weaker free speech guarantees—are faced with a choice regarding how the app handles their messages: agree to the terms, or leave the app.

"Right now, messaging app companies are in charge of users, when really it should be the other way around," says Matthew Weidner, a Ph.D. student advised by CyLab's Heather Miller in Carnegie Mellon University's Computer Science Department. "Users should have the freedom to choose how their messages are handled."

That's why Weidner argues that the services that group messaging apps use—such as end-to-end encryption or group management—should be de-centralized. That is, users shouldn't be tethered to a single company's server, which leaves them at the mercy of the company.

In a new study presented at last week's ACM Conference on Computer and Communications Security, Weidner defined a new security protocol that could bring this idea of decentralization to fruition.

"The idea of our work is to give users the same security, but support a more flexible network, thus giving more power to users," says Weidner, who served as the study's lead author. "If your message thread is routed through one server and the company raises the prices or shuts down, you could switch to another server seamlessly."

Core to Weidner's work is what's called continuous group key agreement (CGKA)—a previously-developed security protocol that allows a group of individuals to join and leave a group message thread after it's been created and not have to rely on a message group manager. CGKA also prevents the need to worry about when or how long members of the group are online. Typically, group messages are routed through a single server that applies CGKA, but Weidner and his colleagues aimed to

study the extent to which secure messaging was possible for more flexible, decentralized networks. Thus, they define decentralized CGKA, or DCGKA.

"What makes our paper different is we work in a decentralized setting, where we don't necessarily assume there's a central server to route messages and help out maintaining the group," Weidner says. "Instead, users can send messages to each other however they'd like."

A decentralized model introduces several challenges, Weidner says. Messages could be delayed or delivered in an inconsistent order, and with no central authority, there is no single source of truth. To solve this, messages are carefully designed so they have the same effect no matter what order they are received in. That way, even if something rare but unusual happens—like two users removing each other from the group simultaneously—the whole group eventually sees the same outcome.

How, then, does this play into the lives of journalists or activists trying to securely communicate in countries with weaker free speech rights? Weidner says DCGKA provides a solution.

"If the journalists are using a central server run by a company to communicate, but it gets blocked or shut down, they could switch to a 'self-hosted' server that's physically in one of their homes," Weidner says. "If that's blocked too, or if the whole Internet is shut down, they could switch to using a mesh network in which nearby devices connect over Bluetooth. Even if some messages get delayed or reordered during the transition, DCGKA will continue working and providing security."

More information: Matthew Weidner et al, Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees, *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (2021). DOI: 10.1145/3460120.3484542

Provided by Carnegie Mellon University