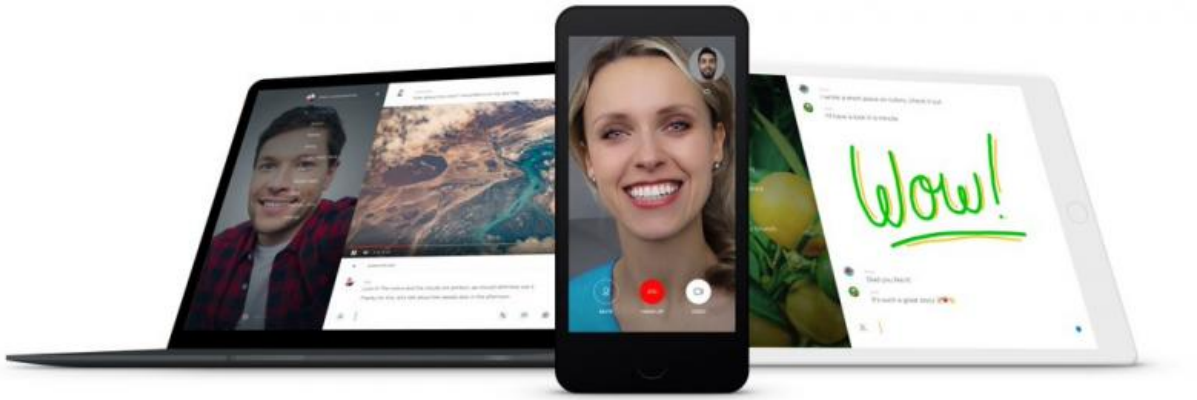
Switzerland-based Wire adds video call encryption

March 13 2016, by Nancy Owano



Switzerland-based Wire is a package of private communications services which this month took on newer capabilities. It is an encrypted messaging app that first launched in December 2014 but it has been given additional secure messaging capabilities. It not only has end-to-end encryption for messaging traffic but end-to-end encrypted video.

As such, for those concerned about privacy, it is an attractive way to experience an on-screen communication. Clear voice, video, group chat or text. No ads. No profiling to go up for sale. The real plus. Data—your

data—encrypted, always. Text, voice, video and media, on Wire, are always end-to-end encrypted 1:1 and in groups.

Conversation content is encrypted with encryption on the sender's device. It is decrypted on the recipient's device.

Wire doesn't hold the decryption keys and the software has no backdoor. Wire relays communications through its network of cloud computers but user communications are stored, in encrypted form, on their own devices, said Reuters.

The Wire team looked around and they did not like what they saw. "The data collected is vast, detailed, and often very personal. Vast resources are being spent to refine the profiles, all without transparency, policy or oversight." In their words, "we should be able to communicate directly without passing our private communications through these corporate data mines."

They are not fans of user profiles. We in a sense value our freedom to step on and off the world's stage when we want. The information people share on social networks, via email, and messaging services, however, when used to build profiles in turn is used to sell products and services through targeted advertising and suggestions. That is what motivated them to offer their own communication approach.

Wire's technical features include text messages and pictures using Off-the-Record (OTR) end-to-end encryption. Wire uses the Axolotl ratchet and pre-keys optimized for mobile messaging.

Voice calls use the WebRTC standard. DTLS is for key negotiation and authentication and SRTP is for encrypted media transport.

The source code for data handling is available to the public under the

GPL License.

Eric Auchard in Reuters reported on another interesting aspect of the story, the faces behind Wire. They are technologists who worked with Skype and they are backed by Skype co-founder Janus Friis. This is a new version of its own messaging service, said Auchard. The 50-person start-up is mostly made up of engineers, he added. "We believe Wire is unique in the industry with always-on encryption for all conversation(s), in groups or 1:1, with simultaneous support for multiple devices," Wire Chief Technology Officer Alan Duric said.

"Everything is end-to-end encrypted: That means voice and video calls, texts, pictures, graphics - all the content you can send," Wire Executive Chairman Janus Friis told Reuters. Quoted in Bloomberg, Friis said, "Everything you do, especially when it's your private, personal, professional communication, does not have to be tracked."

What about the business model of Wire? Jeremy Kahn, reporting in Bloomberg: "Friis said Wire would never create an advertising-based business model. Instead, he said, the platform might charge for certain premium services in the future."

More information: wire.com/

© 2016 Tech Xplore

Citation: Switzerland-based Wire adds video call encryption (2016, March 13) retrieved 23 April 2024 from https://techxplore.com/news/2016-03-switzerland-based-wire-video-encryption.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.