Zoom security: Here's what you need to know

May 4 2020, by Thomas Reisinger

Credit: AI-generated image (disclaimer)

The video conferencing app Zoom gained about 2 million new users in the first two months of 2020—and that was before the World Health Organization declared the coronavirus outbreak a pandemic. With so many people now relying on video conferencing for contact with their friends, family and colleagues, it's no wonder Zoom has seen a significant increase in its company stock price. But the firm has also attracted some negative press recently for issues related to its privacy

and security.

I worked in the video conferencing industry for 10 years. During this time, I started a Ph.D. on whether such systems meet the needs of organisations that have to communicate under adversarial circumstances, such as international NGOs and opposition groups under oppressive regimes. My near-finished research shows that Zoom has indeed had plenty of problems, but is far from the only platform with security and privacy issues.

A number of issues with Zoom have attracted public attention, most notably call hijacking or "Zoom-bombing." Calls that are not set to private or password-protected can be accessed by anyone who inputs the nine- to 11-digit meeting code, and researchers have shown how valid meeting codes could easily be identified (something Zoom now says it prevents).

Zoom has also recently had to make changes to its iPhone and iPad apps to stop Facebook being able to collect data about users. And last year it was forced to fix a problem that could have allowed websites to turn on Mac users' cameras without permission.

Another issue, recently highlighted by The Intercept, is that Zoom claims its calls can be encrypted, but doesn't use the kind of end-to-end encryption that many people have come to understand as standard for private communication services. Messages or calls sent with end-to-end encryption are effectively locked with the receiving user's public key that anyone can access, but can only be unlocked by the user's private key. This system is used by messaging apps such as WhatsApp to ensure only a message's recipient can read it—not even the app's provider has access.

Zoom instead uses the AES-256 ECB method of encryption, which

shares the key used to encrypt calls with Zoom's servers around the globe. This potentially gives them full access to the audio and video streams, although the company has stated no user content is available to its employees or servers once encrypted.

Researchers have also found that encryption keys even up on Zoom servers based in China (where the company has development sites) even when no Chinese participants are in the call. This opens the possibility that the Chinese government, famed for its control of internet communications in the country, could eavesdrop on calls. Zoom has now started offering paying customers the ability to opt out of having data routed through China or other regions.

While Zoom has developed measures or options to at least partly address all of the issues highlighted—and said it will freeze the development of new features for 90 days so it can focus on improving security—the litany of problems that have already been identified should provoke serious thought among its users. On top of this, Zoom's privacy policy is arguably not user-friendly. By downloading the app, you essentially grant the company permission to do with your personal data whatever they want.

The problem for anyone looking for a more private system is that many of Zoom's competitors have their own similar security issues. For example, Microsoft's Skype and Teams services also use forms of encryption that give the company control over the keys.

Alternatives

So what are the alternatives? The most secure options are arguably those that use end-to-end encryption and are built with open-source code because it can be publicly reviewed to check it doesn't have any hidden problems.

Signal is a messaging app that falls into this category and also provides video calling from smartphones, but not desktop video calls or video conferencing with multiple parties. Jitsi is also open source and provides end-to-end encrypted video calls via a web browser, and is working on doing the same for multi-party video conferencing.

If these options don't suit you, then there are things you can do when using Zoom or other video calling services that have potential security issues to maximise your privacy and safety.

- Enforce encryption by default and makes sure it's end-to-end if possible
- Lock and password-protect meetings
- Unauthenticated users should be held in a waiting room so the organiser can check their identity before admitting them to the call
- Make sure a meeting host monitors the participants list and ensures no unknown participant joins
- Be careful with meeting recordings and get consent from the participants
- Be aware that audio-only participants calling via a regular phone dial-in option will "break" the encryption
- Be careful with file and screen-sharing capabilities. They could accidentally disclose sensitive information or be used to spread malicious programs.

In response to the issues raised in this article, a Zoom spokesperson said:

"Zoom takes user privacy, security, and trust extremely seriously. Zoom was originally developed for enterprise use, and has been confidently selected for complete deployment by a large number of institutions globally, following security reviews of our user, network and datacenter layers.

"During the COVID-19 pandemic, we are working around-the-clock to ensure that businesses, schools, and other organizations across the world can stay connected and operational. As more and new kinds of users start using Zoom during this time, Zoom has been proactively engaging to make sure they understand Zoom's relevant policies, as well as the best ways to use the platform and protect their meetings."

Provided by The Conversation