Frequently Asked Questions about Zoom Security

Frequently Asked Questions about Zoom Security

How is MIT protecting Zoom sessions used for teaching, learning, and working?
MIT's enterprise license agreement with Zoom was developed by a consortium of US higher-education institutions and provides for security, privacy, and residency of MIT data consistent with FERPA, HIPAA, and MIT Office of General Counsel requirements. In addition, all videos that any of us produce on Zoom and store in the Zoom Cloud can only be accessed by those who authenticate using MIT Touchstone. Note that users of the "free" level of service from Zoom are not afforded these protections. It is strongly recommended that MIT faculty, students, staff, and affiliates use MIT's Touchstone-protected enterprise instance at mit.zoom.us to conduct MIT activities.

What is "ZoomBombing" and what can we at MIT do about it?
The "ZoomBombing" phenomenon is the unauthorized joining of a meeting by outside parties with the intention to disrupt, attack, or offend the meeting participants. MIT has taken measures to tighten its security requirements for the use of Zoom by both educating the MIT community to the risks, and also encouraging the community to only allow MIT-authenticated users to join their meeting, or using passcodes or the waiting room features to keep their Zoom meetings secure. To learn more, see Limiting Access and Reducing Disruptive Behavior in Zoom.

Does Zoom use end-to-end encryption?
As reported here, Zoom was initially not being clear in how they use encryption in their product, and the technical claim about using end-to-end (E2E) encryption was inaccurate. E2E encryption would require that Zoom not only encrypted the traffic but also did not possess the encryption keys used to encrypt the video or audio meeting content. This type of measure would enhance the overall security of the meeting but also comes with considerable impact on the overall functionality available during these sessions. As an example for Zoom the functionality to focus the video on the active speaker, recording, transcribing or captioning the meeting content would be very difficult in a scenario using E2E encryption. Zoom is using encryption in their product, and they are using it in the same manner as many web based technologies as well as similar products like Google Hangouts. A comparison of different products can be found here. Zoom's mistake was using the terminology end-to-end encryption, which is not accurate. Subsequent to the writing of these articles, Zoom has implemented an end-to-end encryption design and has made that public to be peer reviewed by the cryptographic community. It plans to release this optional feature later in the 2020. Note that Webex does support an option to schedule a meeting using E2E encryption, but there is a trade-off as not all features are available when using Webex meetings with E2E encryption.

Are Zoom transmissions routed through China?
This issue occurred, but has been corrected. There was a brief period of time when Zoom was rapidly scaling up their capacity to meet the unprecedented demand they were seeing, that they started to leverage resources they had available around the globe to meet that demand. That included the use of computing resources they had access to in China. This has since been corrected and measures are in place to ensure that Zoom calls and data flows stay and use resources only within their geographic region. In MIT's case, this means the United States as specified in our Zoom contract.

Does Zoom share my data with Facebook?
As reported here, the Zoom Apple mobile client was using Facebook’s login functionality to allow users to login to Zoom with their Facebook account. The integration of this functionality into their Apple mobile client with Facebook’s development kit also resulted in their mobile app transmitting information to Facebook that Facebook should not have been receiving. Zoom has removed this from their Apple mobile client in their most recent update as of March 27th.

I read about a security exploit where Zoom can be used to take over a computer. What is the risk?
The vulnerability reported here requires physical access to your computer in order to modify your system to take advantage of this exploit. The exploit is real, but the likelihood of exploit is fairly low.

How is Zoom addressing security concerns?
Zoom's CEO has announced that the company is dedicating resources to better identify, address, and fix security issues proactively, and committed to being transparent throughout this process. Zoom regularly updates their best practices blog with advice intended to address these community concerns.

See Also

- Zoom Landing Page