The Facts Around Zoom and Encryption for Meetings/Webinars

APRIL 1, 2020 BY ODED GAL

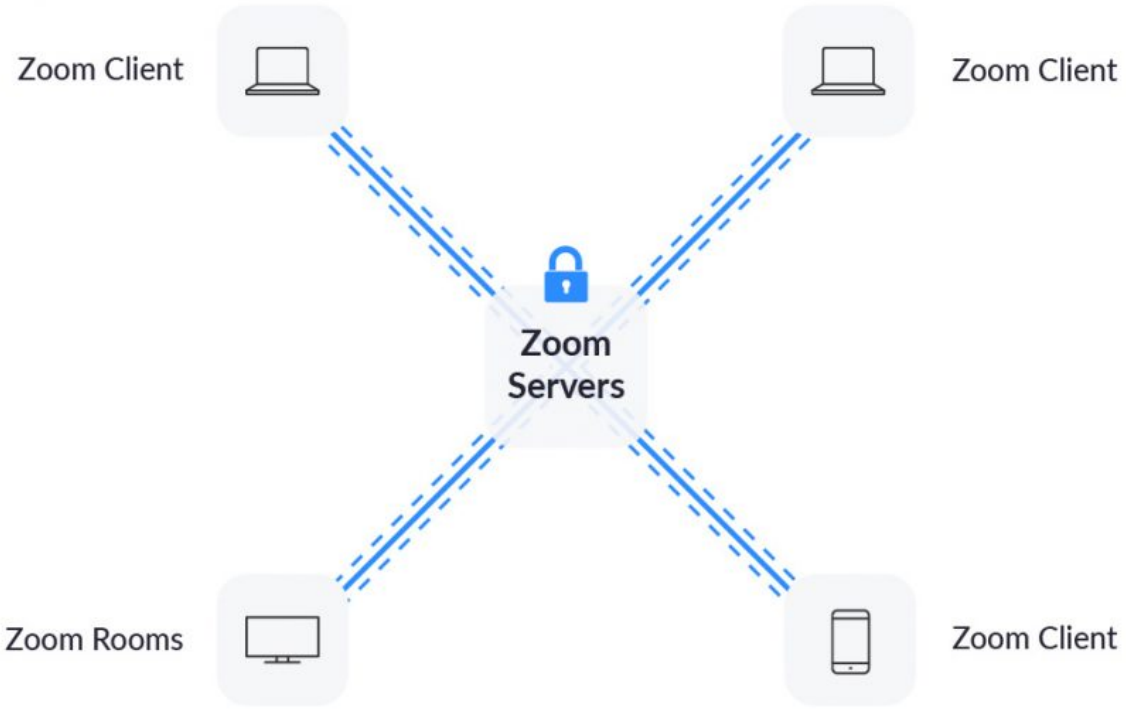
In light of recent interest in our encryption practices, we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption. Zoom has always strived to use encryption to protect content in as many scenarios as possible, and in that spirit, we used the term end-to-end encryption. While we never intended to deceive any of our customers, we recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it. This blog is intended to rectify that discrepancy and clarify exactly how we encrypt the content that moves across our network.

The goal of our encryption design is to provide the maximum amount of privacy possible while supporting the diverse needs of our client base.

To be clear, in a meeting where all of the participants are using Zoom clients, and the meeting is not being recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.

Zoom clients include:

- A laptop or computer running the Zoom app
- A smartphone using our Zoom app
- A Zoom Room



In this scenario, where all participants are using the Zoom app, no user content is available to Zoom's servers or employees at any point during the transmission process.

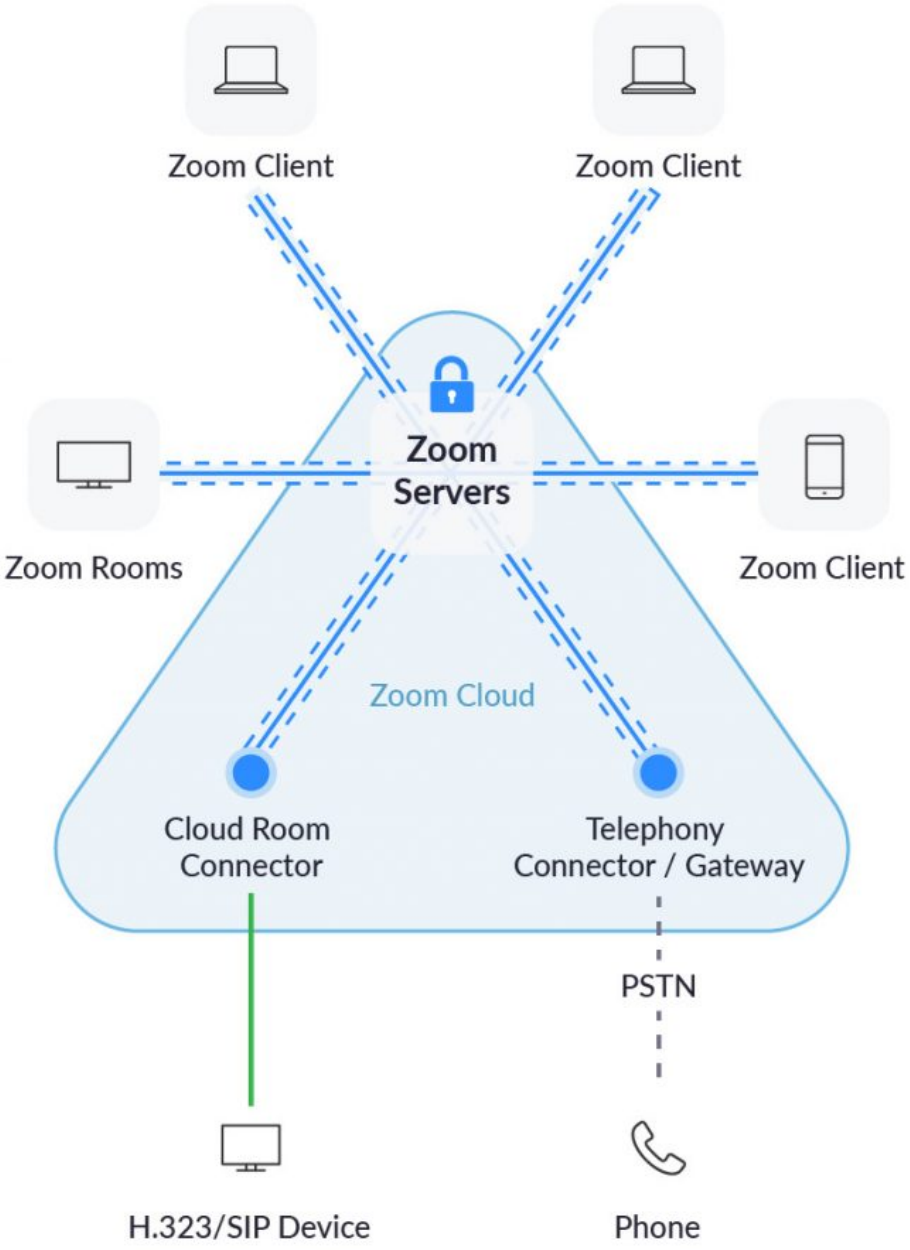
Zoom supports a diverse ecosystem of communication channels in order to offer our users as many ways to connect as possible. When users join Zoom meetings using devices that do not inherently use Zoom's communication protocol, such as a phone (connected via traditional telephone line, rather than the app) or SIP/H.323 room-based systems, Zoom's encryption cannot be applied directly by that phone or device. That said, our goal is to keep data encrypted throughout as much of the transmission process as possible. To achieve this, we have created specialized clients to translate between our encrypted meetings and legacy systems. We call these Zoom Connectors, and they include:

- Zoom Telephony Connector
- Zoom Conference Room Connector
- Skype for Business Connector
- Cloud Recording Connector
- Live Streaming Connector

These connectors are effectively Zoom clients that operate in Zoom's cloud. Content remains encrypted to each connector, and when possible we will encrypt data between each connector and the eventual destination (such as a non-Zoom room system).

Connectors may also be invited to the meeting upon the request of the meeting host to help perform services for the meeting. Examples of this include the Live Streaming Connector, which serves as a Zoom client that can translate the meeting's content into a live streaming format, such as for use with other webcasting services.

We believe that there is still value in encrypting content between clients even in the scenario where connectors are necessary, as this reduces the number of systems at Zoom with access to customer content and serves as a defense-in-depth.



To ensure this entire process meets the needs of our customers around the clock and around the world, Zoom currently maintains the key management system for these systems in the cloud. Importantly, Zoom has implemented robust and validated internal controls to prevent unauthorized access to any content that users share during meetings, including – but not limited to – the video, audio, and chat content of those meetings.

Zoom has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list.

For those who want additional control of their keys, an on-premise solution exists today for the entire meeting infrastructure, and a solution will be available later this year to allow organizations to leverage Zoom's cloud infrastructure but host the key management system within their environment. Additionally, enterprise customers have the option to run certain versions of our connectors within their own data centers if they would like to manage the decryption and translation process themselves.

We are committed to doing the right thing by users when it comes to both security and privacy, and understand the enormity of this moment. With hospitals, universities, schools, and other organizations across the world relying on Zoom to stay connected and operational, we are proud of the work we have done to protect the data of those critical institutions with encryption – and we look forward to sharing more information on our security practices in the near future.

ANNOUNCEMENTS