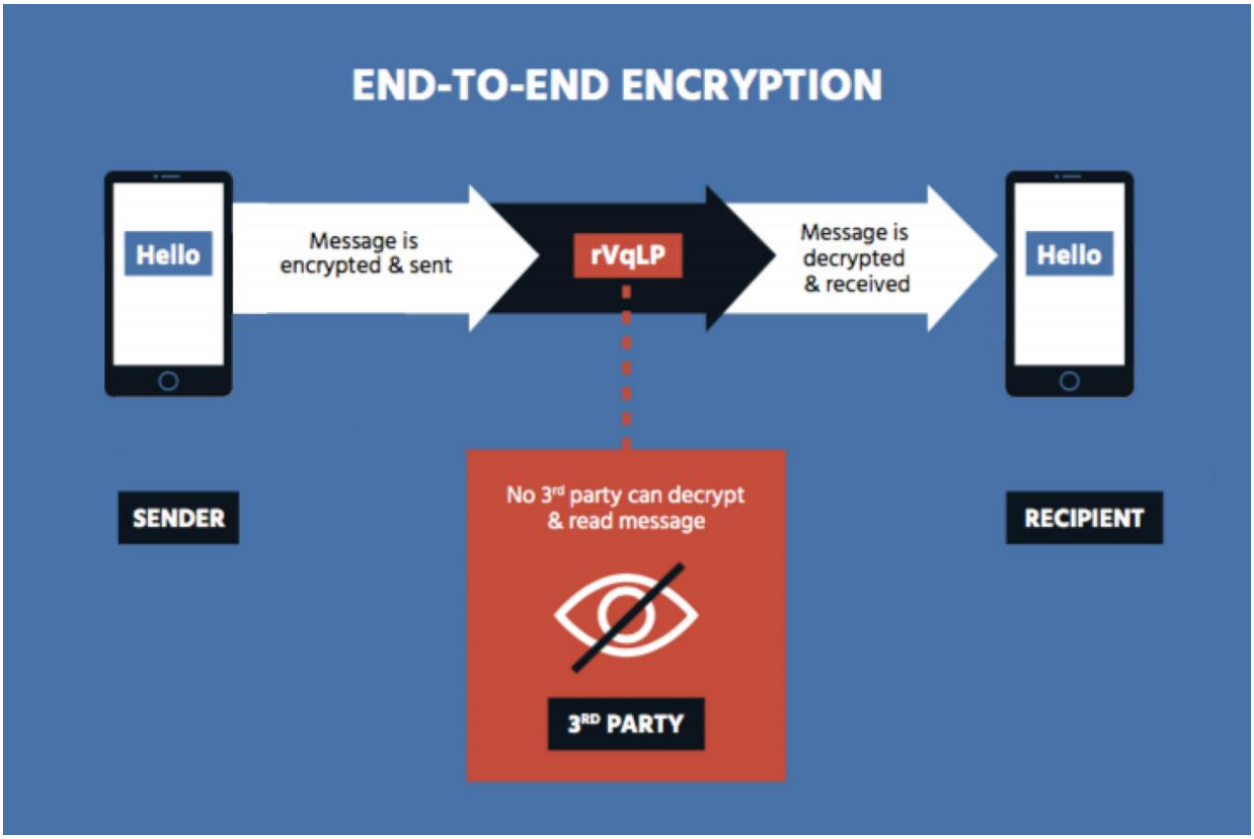
Encryption in Video Conferencing Platforms

In 2020, As governments across the world have placed their citizens on lockdown due to COVID-19 pandemic, downloads of video conferencing apps have soared to record highs. Video conferencing has become popular than ever for attending work meetings, social meetups with friends and family, etc. Switching all meetings to video conferencing poses several security challenges. This blog post will take a look at end-to-end encryption (E2EE), transport layer security (TLS), and their implementation in popular video conferencing platforms.

What is end-to-end encryption (E2EE)?

End-to-end(E2E) encryption is any form of encryption in which only the sender and intended recipient can read the message.
Encryption is a crucial building block of Internet trust, and End-to-end encryption is the most secure form of encryption that you can use.



[End-to-end encryption | Image credits: Internet Society]

End-to-end encryption in video conferencing platforms

We all agree that we need our meetings to be protected and secure. For meetings requiring the highest level of confidentiality, one should use a platform that supports end-to-end encryption (E2EE).

End-to-end encryption means that the meeting content may only be accessible by the meeting participants, not by any intermediaries [for example, Internet Service Provider (ISP), wiretapping, etc.]. In other words, in E2EE-based conferencing options, the server cannot spy on the meeting.

However, E2EE doesn't guarantee the capturing of metadata about the video conference call, such as names, emails, device's network configurations, and IP addresses of the participants.

In many of the conferencing platforms, you will find phone numbers to dial in. In most cases, phone communications are not encrypted at all.

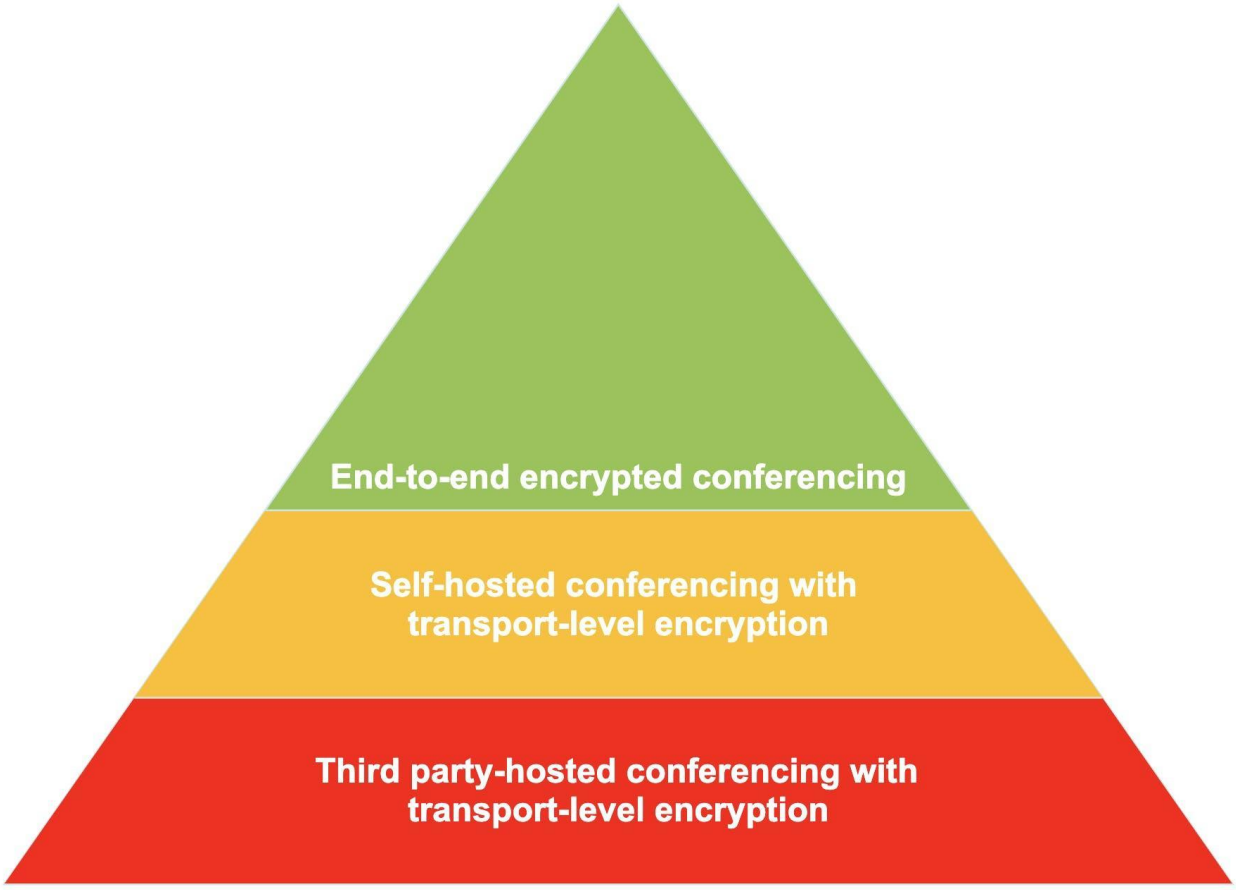
What is transport-layer encryption?

Transport-layer encryption or transport layer security (TLS) provides end-to-end security (not end-to-end encryption) of data sent between applications over the Internet. Messaging service provider or the website you are browsing, or the app you are using - can see unencrypted copies of your messages if they want to or are compelled to by law enforcement. However, an adversary monitoring a WiFi network shouldn't be able to see or hear the content of the communication.

Transport layer encryption in video conferencing platforms

Today's various video conferencing platforms usually provide transport layer encryption with two options self-hosted conferencing or third-party hosted conferencing. Among that, the weakest form of security is transport-level encryption with third-party conference hosting.

If you're attending an online concert or public class, then a Zoom or Google Meet session may be excellent, depending on your threat model.



[Video conferencing security tiers | Image credits: First Look Media (FLM) Security Team]

If your threat model includes adversaries like government agencies, where Microsoft or Google or Zoom can receive and comply with a wiretap request, then a higher security tier is desirable, as shown in the security tier diagram.

Zoom.us

Zoom provides transport-level encryption. On 22nd May 2020, zoom announced that they would offer an end-to-end-encrypted video communication in a 90-day plan. Here is a cryptographic design draft: https://github.com/zoom/zoom-e2e-whitepaper/blob/master/zoom_e2e.pdf

WhatsApp

WhatsApp is end-to-end encrypted and uses the same encryption as behind Signal. While WhatsApp cannot share your conversations, it may share a fair bit of information with the parent company Facebook. For example, WhatsApp shares users' contact lists with Facebook.

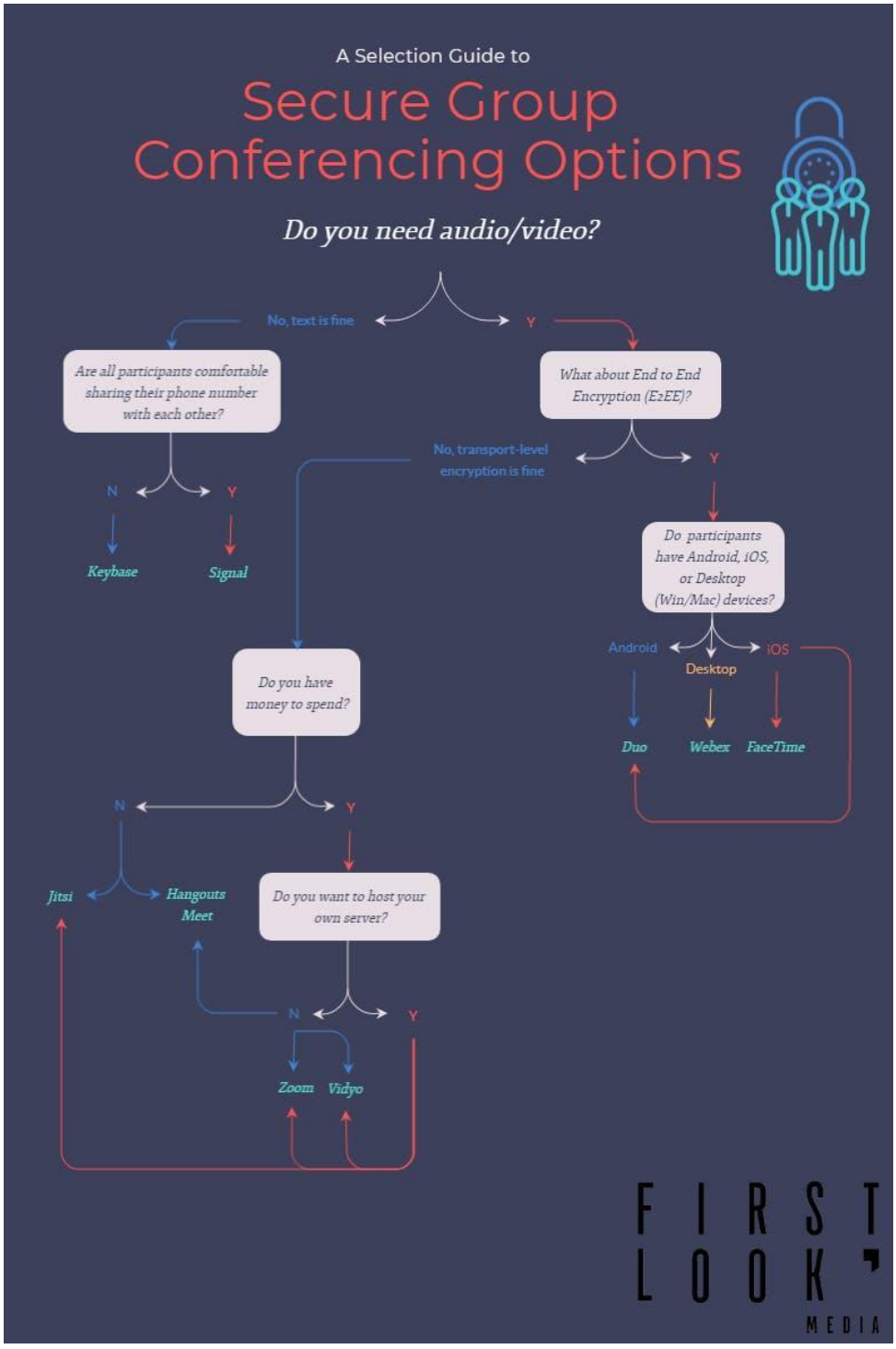
FaceTime

Apple's FaceTime provides end-to-end encryption. Apple keeps a record of metadata, such as who was invited to a call and your device's network configurations, and stores this information for up to 30 days.

Signal
Signal provides end-to-end encryption using the Signal Protocols. Signal requires all participating users in group chat to have a phone number visible to all members of a group chat.

Google Meet
It's not end-to-end encrypted, meaning the company holds the encryption keys needed to read your data.

Here is a handy flowchart from First Look Media (FLM) security team.



[A selection guide to secure group conferencing options | Image Credits: First Look Media (FLM) Security Team]

Who needs to be protected?

- **Whistleblowers** researching corruption

- **Journalists** protecting sources and investigating stories
- **Lawyers** speaking with clients
- **Doctors** and all others with access to medical records
- **Executives** and other high-ranking employees of corporations, especially when traveling to places where internet surveillance is commonplace

And, most importantly, all the **citizens**.

In Conclusion, secure encryption is fundamental to the safe and efficient operation of critical aspects of our society, and our lives – including law enforcement and national security agencies as well as business operations.

To succeed in the long term, Internet Society is building a positive narrative around encryption. Recently, Internet society announced the launch of the Global Encryption Coalition. Join the Coalition: https://www.globalencryption.org

References:

[i] Choosing the right video conferencing tool for the job by Martin Shelton: https://freedom.press/training/blog/videoconferencing-tools/
[ii] A deep dive on end-to-end encryption: how do public-key encryption systems work? by EFF https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work