UN Information Security Special Interest Group (UNISSIG)

The Evaluation of Zoom as a UN system Video-Conferencing Solution

Background

Since the outbreak of COVID-19, video-conferencing solutions have emerged as the principle platform for organizations to coordinate, communicate and collaborate with staff and external partners alike. This sudden and widespread change in practice has translated to cultural changes within organizations overnight which for some organizations included a reliance on tools that have not undergone thorough security evaluations. Zoom has emerged as a popular choice to address organizations' immediate needs, in part due to its accessibility and usability benefits but moreover, widespread adoption globally.

Zoom has seen a massive increase in popularity during the COVID-19 crisis, with many individuals and Organizations adopting the solution – often without formal security assessment –to address their remote-working needs. Zoom offers simplicity, functionality, ease of use and tolerance of low bandwidth environments, making it appealing to users and businesses alike.

Zoom is a cloud-based solution, relying on AWS infrastructure, complemented by secondary contracts with telecom providers across the World.

Given the recent uptake of Zoom by many UN system organizations, in its meeting of 6 April the DTN considered the evaluation of the Zoom platform from an information security and privacy perspective to be a priority. On 14 April the UNISSIG met virtually to discuss the information security implications of organizations' uptake of the Zoom platform. Chaired by Thomas Braun (Chief Cybersecurity Section, UN secretariat), this discussion focused on the widely publicized security and privacy concerns of Zoom, and the development of common recommendations on the use of Zoom as a meeting organizer and as a participant. This meeting was well attended and invited widely varying views on the suitability of Zoom for organizations.

Introduction

From the outset, video-conferencing solutions are seen to vary in the manner they address (a) risks to the confidentiality of the content of a meeting (level of encryption, access control, etc.); (b) risks to privacy (collection of metadata about the meeting as well as participants, their devices, locations, etc. and the sharing of this information with third parties), and (c) risks inherent in the client application and how they may expose the computers on which it is installed. An assessment of Zoom from an information security and privacy standpoint, therefore, requires an understanding of an organization's risk profile, benefits and risks inherent to the platform, the data confidentiality requirements of a meeting, the limitations of the platform and the technical controls available to help mitigate risk.

Observations

It was noted that UN system organizations vary in their risk appetite and consequently address the evaluation and adoption of software with the same criteria. There is no common position of UN system organizations on the suitability of Zoom as a video-conferencing solution. No one solution, therefore, can be seen to meet all UN system organization’s functional requirement within acceptable levels of controls for information security and privacy.

While perhaps not an organization's preferred collaboration platform, the adoption of Zoom by some organizations was seen to be more demand-driven and therefore considered a necessity, more an imposition than a preference. There was consensus on the need for clear criteria to support organizations evaluate the suitability of Zoom and competing platforms.

Assertions

All participants agree that, even if all available security controls are implemented, Zoom cannot be considered a secure communication channel and therefore is an inappropriate choice for sensitive discussions. Despite previous statements Zoom does not support end-to-end encryption, and way in which encryption is used is ineffective. It cannot therefore be considered a suitable solution when the confidentiality of discussions is required. Recent changes to the service notwithstanding, there are continuing concerns about its privacy policy and practices, specifically the level of information that is collected and shared with third parties. Zoom applications for mobile platforms (smartphones and tablets) require access to a lot of private information which may not be technically justified. Until April 2020 the platform extensively collected and shared user information with third parties and services such as Facebook and LinkedIn. The extent to which these concerns have been addressed is unclear and have not yet been independently validated. This is of concern for organizations that use Zoom without a specifically negotiated contract.

While vulnerabilities in software applications are common and Zoom recently has been very responsive in addressing reported vulnerabilities, this was not the case prior, and serious vulnerabilities e.g. related to the bypass mechanisms used by the Zoom installer package had been identified and reported by third parties. Security audits of the latest Zoom application for Windows expose poor software development standards, such as usage of outdated and vulnerable software libraries. Installing and using Zoom applications may put at risk the integrity of computer systems of meetings participants.

On 1 April 2020 the vendor announced to *"shift[ing] all our engineering resources to focus on our biggest trust, safety, and privacy issues".* For these reasons, the adoption or further use of Zoom is decisively and comprehensively avoided by some organizations, while others plan to continue using Zoom for specific uses cases. In general, whether Zoom is considered a viable video-conferencing solution for specific requirements was seen to depend on an organization's risk appetite and more specifically, the confidentiality requirements of a meeting.

Security measures are available on different levels. A higher level of control can be achieved if organizations centrally managed the use of the platform for their users and integrate it into existing authentication systems.

Security and privacy risks vary depending the client used by the individual user. Mobile platforms, such as phones and tablets are considered inherently less secure. Web clients present less security vulnerabilities than applications or apps that require installation but rely on the security of the browser.

The remote recording of meetings cannot be prevented in practice. Microsoft Teams is the preferred platform for the majority of organizations that require privacy and confidentiality, particularly when implemented in unison with available Microsoft security controls.

UNISSIG recognizes that personnel of UN entities will continue to participate in Zoom meetings that are organized by third parties, either external or UN system organizations that actively use Zoom. The following recommendations are provided for general utilization of **any** remote meeting, and two different scenarios specifically for Zoom meetings: (a) the use of Zoom as an organizer of a meeting, and (b) the use of Zoom as a participant/attendee.

Recommendations

The following recommendations apply to all versions of Zoom videoconferencing available up to and including April 2020.

Recommendations applicable for any remote meeting system

I. Before joining a meeting, make sure the meeting invitation you are responding to was sent by a trusted party (you recognise the invitation sender, and would expect to participate in the subject of the meeting)

II. As far as possible, avoid joining a meeting using the "local dial in" (telephone) option for the audio (as this bypass any encryption that might be applied to the meeting).

III. Make sure the meeting requires a password to join (if it does not, it is open to the public)

IV. Disable camera and mute the microphone when they are not required. Enable only when needed. (You may be asked to turn on your camera and introduce yourself by the meeting host to verify your identity.)

V. Do not accept any links or downloads you are not expecting, especially from meeting participants that you do not know. Such links and downloads may be malicious or harmful to your computer.

VI. Be aware that a remote conference can be easily recorded by any participant. It is impossible to prevent, or even detect it.

VII. Choose a neutral video background, such as a white wall, or use a virtual background.

VIII. **At the end of the meeting**, leave promptly, ensuring that your **microphone and video are turned off** before you leave. Close the browser after leaving the meeting. If your camera has a privacy filter / slider, ensure that this is enabled to protect against unauthorised use of the camera. If you do not have a fitted filter, consider using self-adhesive note paper.

Recommendations for Zoom Meeting Attendees

In addition to the general guidance applicable to all remote meeting services;

I. **Do not use Zoom to exchange confidential information.**

II. **Do not expect Zoom to respect your right to privacy.**

– Whenever possible, **use a standard Web browser only to join Zoom meetings**.
Zoom offers three modes for user-connectivity:
- Web-browser (e.g. Chrome, Edge, etc.); reportedly the Google Chrome browser provides the best support for Zoom meetings, recommended in the following order:
- Computer client (installed application)
- Mobile app (i.e. smartphone, tablet)

III. If using Zoom software
- make sure you download it from the official source (https://zoom.us/download)
- make sure you always use the latest version
- do not use the Facebook or Google login option, instead create a dedicated account for Zoom; you may choose your institutional email *address* but <u>must</u> chose a different and unrelated, strong password.

IV. Do not share Zoom meeting links publicly (e.g. on social networks or in online forum posts).

Recommendations for Zoom Meeting Organizers

Recommendations for safe configuration of Zoom teleconferencing for organisers of meetings, for organisations with corporate Zoom license and centralised control

I. Use generated random meeting ID’s reduce the risk of Zoom Bombings, which are more easily achieved by having static meeting ID’s for each user.

II. Do not share passwords with Zoom.

III. Modify Zoom’s configuration to automatically restrict screen sharing to the meeting organizer or meeting “Host“. In this way, the meeting host controls the screen sharing feature preventing participants from sharing content freely without the host consent. Should you wish to have one of your meeting participants share content, simply move the “Host” or “Co-Host” rights to this participant, which will enable them to share on-line content.

IV. We recommend using more secure alternatives for meetings with less than 10 participants. If you have more than 10 participants and you have participants that come from bandwidth challenged locations, then Zoom works well.

V. Allow only registered users to join meetings

VI. Disable the embed password in meeting link for “one-click join” feature

VII. Disable the “join before host” feature

VIII. Make use of the waiting room feature and allow only registered participants to join the meeting

IX. If all expected participants are present, lock the meeting once it starts, which will restrict even those with passwords from joining

For organisations without corporate Zoom license but users are using Zoom

I. Do not reuse the organization's credentials (username/passwords) when registering for a zoom account. It is suggested that any email address used for Zoom (or others) has multi-factor authentication applied to it (for email access), such that loss of the credential in Zoom does not lead to compromise of email.

II. Use of Zoom should be limited to meetings where no confidential topics are discussed, and users should not have any expectations of privacy.

III. If the Zoom application is used in preference to the browser, always install the Zoom software updates as soon as you are notified. This will ensure you are protected against newly discovered security vulnerabilities.

IV. Always use Zoom's "Waiting Room" feature, which provides you the ability to screen participants prior to admitting them to the conference / webinar / meeting. This does impose a certain level of security and should be taken inconsideration, as this may not be practical for all meeting types

V. Generate your Zoom meetings with a complex **password** by default.

VI. Enable "Screen Sharing" for **host only.** This will limit the display of any inappropriate content. (Set 'Who can Share' and 'Who can start sharing…' to 'Host' only)

VII. If screen is shared, limit screen sharing to '**One participant at a time**'

VIII. **Disable** file sharing

IX. **Disable remote control by participants**

X. To avoid over-crowding, the meeting may be **locked** a few minutes after start time

XI. **Disable** microphones except for panellists

XII. Limit chat to **panellists, host only, or no chat at all**. Again, use the options that suit your purpose.

XIII. If the meeting is being recorded, make sure this is announced to all participants.