Zoom Security - Securing your virtual Meetings

Marc Ruef
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Marisa Tschopp
Research Department, scip AG
mats@scip.ch
https://www.scip.ch

Abstract: Due to the smoldering COVID-19 pandemic more and more meetings, trainings, and lectures are taking place online. Among others, Zoom has become a very popular solution. Attackers are increasingly targeting it. Various measures can be taken to prevent meetings from being compromised or taken over.

Keywords: Android, Anonym, Conference, Corona, Password, Rapid, Tool, Video, Zoom

1. Preface

This paper was written in 2020 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20200406* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

2. Introduction

The coronavirus is about to change our society. A very concrete change affects our working habits, which in many cases are forced to shift to the digital space. As video conferencing increases, attacks on them become more and more interesting. This article deals with the security of the tool *Zoom*.

Zoom [1] is a system for video conferences, web conferences, and webinars. The simplicity and the multitude of possible uses make it particularly attractive. Especially schools rely on this solution. Many teachers and lecturers are challenged by the rapid transition to virtual teaching, which understandably can lead to neglecting a technically secure setup. If these are not specifically optimized, third parties can *interfere with the meetings* [2]. This interference, often called #zoombombing, requires more attention.

The following advice refers to the desktop version of Zoom. The settings on mobile devices, e.g. on Android, deviate from this description and are sometimes difficult to find. Hosts of a meeting are advised not to use mobile devices.

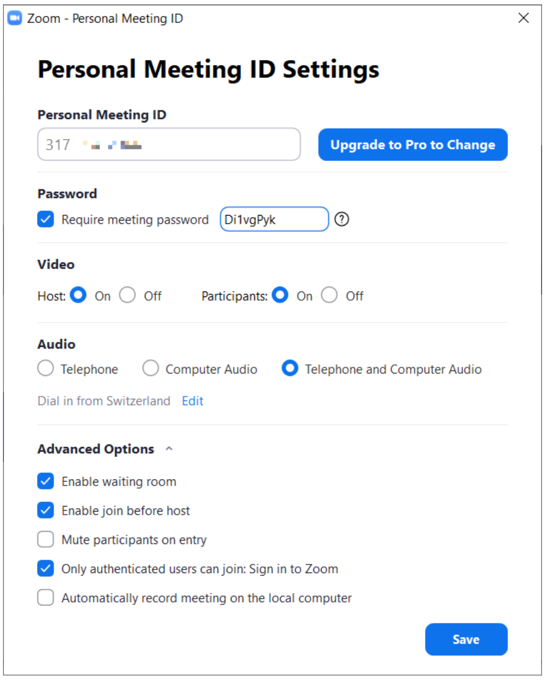
3. Protect the Meeting with a Password

After the Zoom Client has been started, meetings can be joined (Join) and scheduled (Schedule). A new meeting can be started by selecting *New Meeting*. However, this is not recommended for safety reasons.

Instead, the small arrow at *New Meeting* can be clicked to open the context menu. In this, *Use My Personal Meeting ID* should be activated first, to then configure this personal room further down.

First, the option *Require meeting password* should be activated. If you want to enter the room, you must enter the now defined password. As usual, it is worth using a password that is as long and complex as possible to prevent guessing it.

Unfortunately, Zoom limits the possibilities. A password can have a maximum of 10 digits and cannot contain any special characters – for example, exclamation marks or commas. However, allowed are star key, at-sign, hyphen and underscore.



Zoom - Personal Meeting ID

Personal Meeting ID Settings

Personal Meeting ID: 317 [redacted]

Password

☑ Require meeting password: Di1vgPyk

Video

Host: ● On ○ Off   Participants: ● On ○ Off

Audio

○ Telephone ○ Computer Audio ● Telephone and Computer Audio

Dial in from Switzerland Edit

Advanced Options

☑ Enable waiting room
☑ Enable join before host
□ Mute participants on entry
☑ Only authenticated users can join: Sign in to Zoom
□ Automatically record meeting on the local computer

Figure: Configuration of Personal Meeting ID

4. Enable Waiting Room

Also, the waiting room should be activated by selecting the *Enable waiting room* option. The waiting room is like a lobby, in which everyone who wants to join the meeting can enter first.

The host can then bring the participants from this waiting room into the meeting. To do this, he must select the *Participants* function. If unwanted participants appear in the lobby, they do not have to be admitted. If a participant has nevertheless been admitted and proves to be disturbing, he can be muted or sent back to the lobby.

5. Require Registration

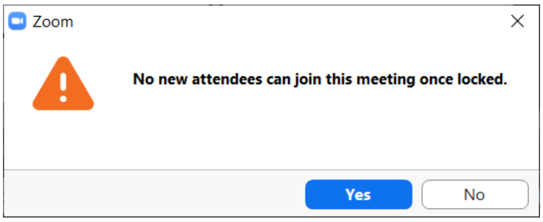
Everyone can now join the meeting if they know their ID or URL and the secret password. It is not necessary to create a zoom account.

To prevent attackers from acting with little effort and with a certain degree of anonymity, *Advanced Options* can be opened below. There you will find the entry *Only authenticated users can join: Sign in to Zoom*. As soon as this is activated, a regular zoom account is required to participate in the meeting. The user must, therefore, register with a valid email address and log in with it before access.

Once the meeting has been created, these options cannot be altered. This is only possible before a meeting has been created. However, the settings can be changed as desired. The choice of password, particularly, should be adjusted regularly.

6. Lock Meeting

Once a meeting has been successfully established with all participants, it can be locked. At the same place where the participants are managed, click on *More* below to open another context menu. There is the entry *Lock Meeting*, with which the current constellation is permanently established. No other participants can now join the meeting. If this should still be possible temporarily, this setting must be deactivated.



Zoom

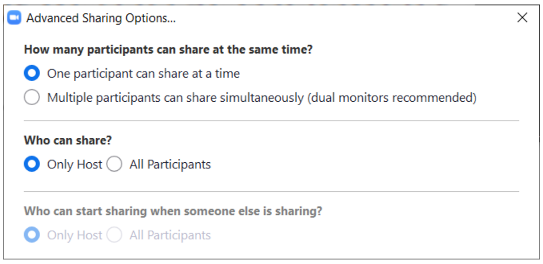
No new attendees can join this meeting once locked.

Figure: Lock meeting

7. Restrict Access

When the meeting starts, the other participants can join. By default, everyone can share their screen. This can, of course, be misused, which is why it is advisable to switch off this setting.

At the bottom, click on the arrow next to the icon for *Share Screen* to select the entry *Advanced Sharing Options* in the context menu. This opens a new window in which the sharing settings can be made. With *Who can share? _ You should switch to _Only Host*.



Advanced Sharing Options...

How many participants can share at the same time?

● One participant can share at a time
○ Multiple participants can share simultaneously (dual monitors recommended)

Who can share?

● Only Host ○ All Participants

Who can start sharing when someone else is sharing?

● Only Host ○ All Participants

Figure: Limit possibilites of influence

When screen sharing takes place, the so-called *annotations* can be made. All participants can mark any places with a pen and make comments. To limit the abuse here, the mouse can be moved to the top of the shared screen to display the menu. On the far right, choose *More* to display the context menu.

In a first step *Show Names of Annotators* can be activated. As a result, all scribbles are given the name of the corresponding author. Anonymous remarks no longer possible.

It is recommended, however, that the annotations be switched off for everyone. The entry *Disable participants annotation* can be found at the same place. If this setting is activated, only the host can add respective annotations.

8. Conclusion

Securing newly available products is not always easy when the experience is lacking. The new situation that video conferencing is used in many places is overwhelming. Zoom offers a number of setting options to make life difficult for attackers. It is a pity that these are *not established by default* [3], but must be used manually. But once understood and done correctly, you no longer have to fear that your meetings could be compromised or taken over.

9. External Links

[1] https://zoom.us/
[2] https://www.scip.ch/en/?news.20200403
[3] https://www.engadget.com/2020-04-04-zoom-waiting-rooms-default.html