Subject: Re: Zoom Bombing
Date: Monday, April 20, 2020 at 7:36:29 PM Pacific Daylight Time
From: KATHIRVEL, KANDAN
To: Brett Preston, Tina Tsou
CC: Aaron Williams

Hi Brett,

Thank you for taking this initiative. Let's discuss with TSC this week.

Aaron - Please add this item to the agenda.

Regards
Kandan Kathirvel

From: Brett Preston <bpreston@linuxfoundation.org>
Date: Wednesday, April 15, 2020 at 9:29 AM
To: kk0563 <kk0563@att.com>, Tina Tsou <tina.tsou@arm.com>
Subject: Zoom Bombing

Hi Kandan and Tina,

You've probably seen/heard about "Zoom Bombing" by now.

In an effort to help protect our Zoom calls against such drop-ins, I've prepared a list of some of the Meeting Settings that the Akraino community may want to have updated. Please share with your Working Group chairs (who are hosting the calls) if needed, and let me know which you would like updated across all Akraino calls.

Bear in mind that I am trying to keep calls as open as possible; minimal hurdles for legitimate community members who want to join.

1. Join before host (Allow participants to join the meeting before the host arrives)
   1. Currently, we set to Yes, Allow -- so that if someone doesn't log in as Host, the meeting can still happen.
   2. I would propose moving to No - Do not allow Join before host. Mainly, you always want someone logged in as Host, so that they can remove bad actors, should any join. I have shared LastPass information (containing Zoom log-ins for each of the Akraino accounts) with all WG Chairs, and can resend for those who may not have accepted, or are unsure.
2. Only authenticated users can join meetings (The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.)
   1. Currently set to No
   2. I would rate this as Optional for now. The benefit is it adds a step to prevent bad actors from joining. The downside is that it adds a step potentially inconveniencing the proper attendees from joining.
3. Meeting Password
   1. Currently not set
   2. All articles I have read suggest setting a meeting password. The key would be in

making this accessible for legitimate attendees. Possibly we list alongside the Zoom URL in the meeting location (on Groups.io invite), as well as in the Meeting Description?

4. Screen Sharing
    1. Currently set to allow Participants to Screen Share
    2. Can restrict to Host Only. If a participant needs to share their screen, the Host can upgrade their permissions in the meeting to Host / Co-Host to allow them to do so. I believe this is where a lot of people are being hit with the obscene material, where a bad actor comes in and starts sharing inappropriate content.

I believe the above 4 would give us a good start in the defence against Zoom Bombing. Additional Meeting Settings can be reviewed under the Settings menu when you log-in to the Zoom account.

Let me know your thoughts on the above, and which - if any, you would like me to execute.

Thanks!

Brett

--
Brett Preston
The Linux Foundation
+1 (971) 303-9030
bpreston@linuxfoundation.org

Google Talk: bpreston@linuxfoundation.org
Skype: bprestoncf