90-Day Security Plan Progress Report: May 20

This week:

- **Security and UI refinements**
  - New chime for waiting room, join and leave meeting
  - See Meeting ID under "more" when screen sharing
  - Unmuting requires participant consent / remove unmute all option
  - Interpretation has language abbreviation instead of flag

- **Screen Share on for host only default for Single Pro Users**

  Security and UI refinements
  - More Admin control for Personal Audio Conference (PAC) password locks
  - Option for host to disable login from multiple devices for meetings with registration
  - Temporarily disabling GIPHY integration

May 17

May 20

Coming later in May:

May 22
- **Detailed draft cryptographic design for end-to-end encryption published for feedback**

May 24
- **Report a user for hosts on Web client and from Zoom Rooms**

- **Support for 3rd party virtual camera re-enabled for MacOS**

- **Zoom Rooms Security Updates**
  - Security Icon controls
  - Assign new host when leaving meeting
  - Get dialogue to consent to unmute and an option to always let host unmute

May 30
- **GCM enabled for all accounts**

As we continue on our 90-day plan to improve the security and privacy of our platform, this week's "Ask Eric Anything" webinar focused on meeting safety, Zoom Phone's FedRAMP authorization, and Zoom's bug bounty program.

Zoom CEO Eric S. Yuan was joined by Zoom CPO Oded Gal; Lynn Haaland, Zoom Deputy General Counsel, Chief Compliance and Ethics Officer; and Katie Moussouris, founder and CEO of Luta Security. Zoom CTO Brendan Ittelson and Lea Kissner, former Global Lead of Privacy Technology at Google who is consulting with Zoom on privacy and encryption, joined for the Q&A session.

Key takeaways from this week's session

Zoom Phone FedRAMP authorization approved

We announced today that Zoom Phone authorization under U.S. FedRAMP has been approved. This authorization allows U.S. federal government agencies and contractors to now use Zoom Phone as part of our existing, broader authorized Zoom for Government offering. Zoom for Government provides U.S. government agencies a full Zoom UCaaS platform, including Zoom Meetings and Chat, Zoom Video Webinars, conference room solutions, and now, Zoom Phone.

Meeting safety

Lynn Haaland talked about what Zoom has done over the past couple months to help prevent meeting disruptions from bad actors. This includes adding default security settings like passwords and waiting rooms for certain users, surfacing in-meeting security controls in the Security icon, adding reporting mechanisms, working closely with law enforcement and other online platforms, and educating users on security best practices.

Lynn also reiterated these tips for securing your Zoom meetings:

zoom

90-Day Security Plan Progress Report: May 20

- Do not publicly share your meeting ID and/or passwords.
- Keep Zoom default security features on - these include waiting rooms, passwords, and restricted screen sharing.
- Get to know our host privacy and security features like Disable Video, Mute Participants, Remove Participants, and Lock Meeting.
- Use meeting registration.

Lynn explained that Zoom Meetings is not designed for large-scale or public events where you post the invite on the internet. Instead, we highly recommend you use Zoom Video Webinars, which gives you more control over the audience and experience. Get more details on meetings vs. webinars on our support page: **https://support.zoom. us/hc/en-us/articles/115005474943-Meeting-and- webinar-comparison.**

Zoom's bug bounty program
Katie Moussouris, the founder and CEO of Luta Security and a security consultant for Zoom talked about how Zoom's bug bounty program will work, explaining that it uses a crowd-sourced model that relies on all parties, including security researchers, to find and report bugs. She also noted that before Zoom implements changes to its bug bounty program, we are soliciting feedback from the wider community to optimize these programs.

Zoom 5.0 reminder
Zoom 5.0 became generally available on April 27, and a system-wide account enablement to AES 256-bit GCM encryption will occur on May 30, 2020. Only Zoom clients on version 5.0 or later, including Zoom Rooms, will be able to join Zoom Meetings starting that day. We encourage users to update to 5.0 today: **https://zoom.us/download.** Zoom admins should visit our IT administrators page to

manage this update in their environment: **https://zoom. us/docs/en-us/zoom-v5-admin.html.** Users can preview the GCM experience at **https://zoom.us/testgcm**.

End-to-end encryption design paper coming Friday

We will publish a detailed draft cryptographic design for our end-to-end encryption offering this Friday on GitHub. We will be hosting discussions with cryptographic experts, customers, advocacy groups, and others to solicit feedback to evaluate for the final design.

Q&A

How do you report a security bug?
Visit **https://zoom.us/security** or send an email to security@zoom.us.

If I'm using a Chromebook, how do I download the Zoom 5.0 client?
Chromebook users can download the Zoom Chromebook application from the Google app store or use the Zoom web client, which will always be up to date.

Are account admins notified when a user is reported to Zoom?
When a host or co-host utilizes the Report a User feature to report a meeting participant, a report is sent to Zoom's Trust & Safety Team. However, in the future we plan to notify account admins for certain accounts when one of their users is reported in certain situations.

Can anyone other than the host record a meeting?
The host can grant access to another participant to record, but no one can start a Zoom recording without a host's consent.

Can you give details on the May 22 draft design on end-to-end encryption?
The draft to be released May 22 shares our plan and

design for building an end-to-end-encrypted video service. This draft won't include any actual code. We want to gather and evaluate feedback before developing our end-to-end encryption offering.

Are there any plans to allow private chat with a user in the Waiting Room to help verify their identity?

Oded said that this is one of our most requested enhancements, and it is on our roadmap.

Why has Unmute All been removed, and are there plans to bring it back?

We removed the Unmute All feature from the user interface because hosts could unmute participants without their consent. We will reinstate this feature in the future. However, hosts will need a participant's consent to unmute them during a meeting.

Thank you for your support

Thanks for attending this week's session, and thank you to everyone who submitted questions! We truly appreciate your support on our journey to make Zoom the world's most secure enterprise communications platform.

If you missed this week's session, you can watch the recording here:

https://youtu.be/YRbZ9jOPB5g

To give your feedback or to ask Zoom a question, send an email to answers@zoom.us. And be sure to sign up for next week's "Ask Eric Anything" webinar.

zoom