SecureVideo
any telehealth use case

SecureVideo Response to N.Y. Times Article: New York Attorney General Looks Into Zoom’s Privacy Practices (3/30/2020)

A White Paper, by Jonathan Taylor, CEO, SecureVideo – March 31, 2020

Security and Privacy Concerns

On March 30, 2020, the New York Times published an article titled “New York Attorney General Looks Into Zoom’s Privacy Practices”. In this article, the New York Attorney General’s Office was reported to have expressed concern about Zoom’s existing security practices and privacy policies. This document addresses SecureVideo’s Zoom-based implementation with respect to these concerns. The four main security and privacy concerns (hereafter, the “Concerns”) raised in the article were:

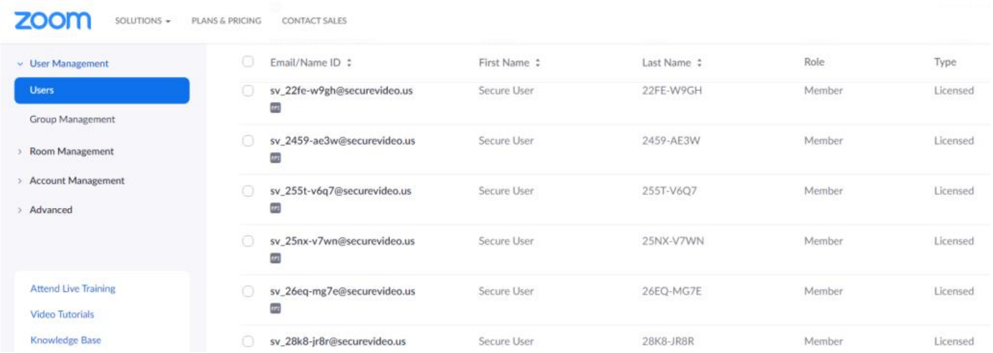
1) Zoom sending user data from its iPhone application to Facebook
2) The possibility of Zoom circumventing New York State laws with respect to educational privacy and student privacy
3) Security researcher Jonathan Leitschuh’s discovery of a Zoom security flaw whereby a user could be tricked into joining a meeting with their camera turned on immediately, thus constituting in invasion of privacy (see https://www.vox.com/recode/2019/7/9/20687689/zoom-mac-vulnerability-medium-jonathan-leitschuh-camera)
4) The practice of “Zoombombing”, where unauthorized users joined Zoom meetings for the purposes of screen sharing unauthorized content

SecureVideo mitigates these concerns using three techniques:

1) We do not send user information to Zoom
2) We require an affirmative user action before the camera is turned on
3) We provide a layer of abstraction between the Zoom Meeting ID and the methods used to enter a Zoom-based SecureVideo session and we blacklist IP addresses after 20 consecutive failed attempts to access a meeting, to prevent brute-force guessing of access codes

Mitigation of Concerns #1 and 2: we do not send user information to Zoom

When Zoom licenses in our system are assigned to SecureVideo users, we do not send the name of the user to Zoom at any point in time. The list of user licenses that Zoom has access to is as follows:

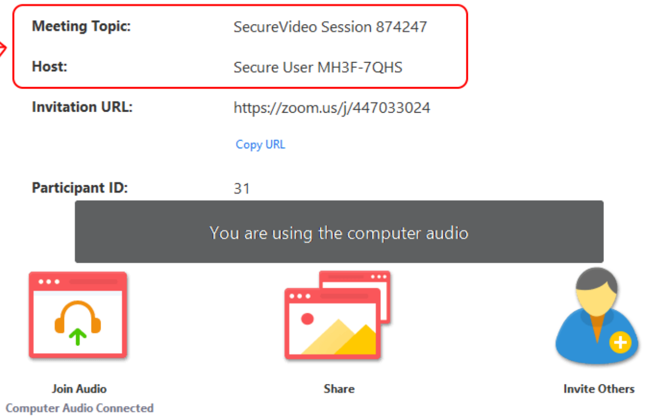


Email/Name ID	First Name	Last Name	Role	Type
sv_22fe-w9gh@securevideo.us	Secure User	22FE-W9GH	Member	Licensed
sv_2459-ae3w@securevideo.us	Secure User	2459-AE3W	Member	Licensed
sv_255t-v6q7@securevideo.us	Secure User	255T-V6Q7	Member	Licensed
sv_25nx-v7wn@securevideo.us	Secure User	25NX-V7WN	Member	Licensed
sv_26eq-mg7e@securevideo.us	Secure User	26EQ-MG7E	Member	Licensed
sv_28k8-jr8r@securevideo.us	Secure User	28K8-JR8R	Member	Licensed

Notice that the E-mail address, First Name, and Last Name are completely anonymized, based on random, 8 character alphanumeric codes.

When you launch a Zoom-based SecureVideo session, you can notice from the below screenshot that the Host information shown is anonymized, and similarly the Meeting Topic is also anonymized to prevent sending Zoom any potentially sensitive information regarding the nature of the session. In a session with two participants, we do not send Zoom the name of any participant for the purposes of displaying on the video panels. In a session with three of more participants, we currently do send Zoom the name of each participant so that participants in a group meeting can identify each other, however in this case we are only sending the name as a text string with no other account information, and this feature can be turned off by request on an account by account basis if it is contemplated by the customer that sessions with 3+ participants will be personal in nature, rather than a business conference. Taken as a whole, we view this approach as a complete mitigation of Concerns #1 raised in the NYT article.

Anonymized Topic and Host



Meeting Topic: SecureVideo Session 874247

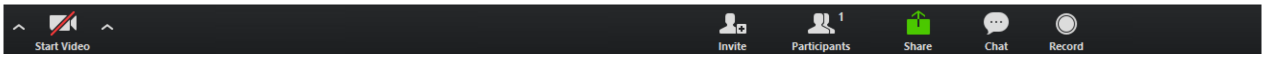
Host: Secure User MH3F-7QHS

Invitation URL: https://zoom.us/j/447033024

Participant ID: 31

You are using the computer audio

Affirmative User Action Required to Start Video



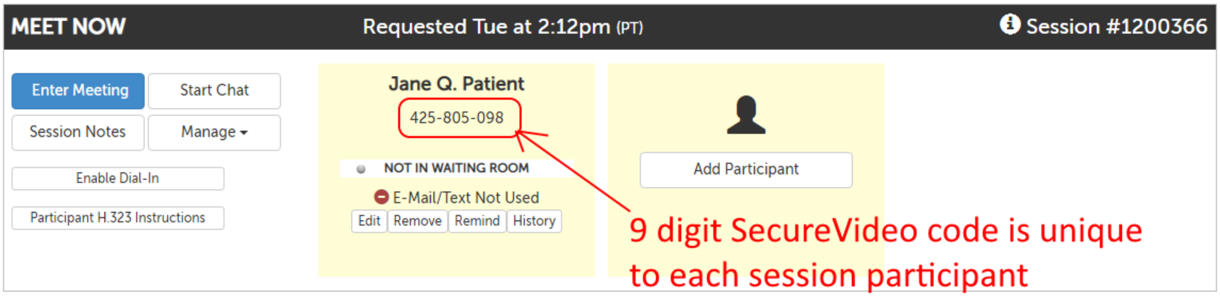
Mitigation of Concern #2: we require an affirmative user action before the camera is turned on

Note in the above screen shot that when a SecureVideo session is started, the camera is off. Therefore, if any would-be hacker is able to trick a user into joining a SecureVideo session, e.g. by tricking them into clicking a phishing link (as in Jonathan Leitschuh's example exploit), there will be no invasion of privacy, as the user would not have their camera on and would need to take an affirmative action to turn the camera on. We view this as a complete mitigation of Concern #3.

Mitigation of Concern #3: we provide a layer of abstraction between the Zoom Meeting ID and the methods used to enter a Zoom-based SecureVideo session and we blacklist IP addresses after 20 consecutive failed attempts to access a meeting, to prevent brute-force guessing of access codes

"Zoombombing", which is the entry of an unauthorized party into a Zoom meeting, requires that the third party have access to the Zoom Meeting ID of a target meeting. Zoom's installed product allows any user to join any meeting if they possess the 9- through 11-digit Zoom meeting ID. In order to invite authorized users to a Zoom meeting, this single Zoom meeting ID is shared to all meeting attendees. In doing this, Zoom is unable to identify which actual participant joined the meeting, as anyone with the link can join.

SecureVideo's approach is to provide a layer of abstraction between the Zoom Meeting ID and the means of entering a SecureVideo session. Each SecureVideo participant receives a unique 9 digit code that is only known to SecureVideo. Upon user entry and our system's validation of that 9 digit code, the SecureVideo system logs that entry as having been performed by that participant, and then ushers the participant into the Zoom meeting.


MEET NOW

Requested Tue at 2:12pm (PT)

Session #1200366

Jane Q. Patient

425-805-098

NOT IN WAITING ROOM

E-Mail/Text Not Used

9 digit SecureVideo code is unique to each session participant

SecureVideo sends this unique, one-time code by e-mail or text message directly to each participant, greatly reducing the likelihood of an unauthorized share. Furthermore, we prevent brute-force guessing of SecureVideo access codes by blacklisting an IP address after 20 consecutive failed attempts at trying an access code.

SecureVideo meetings will also require (in a near-term update) not only this visible access code but a randomly generated 10 character alphanumeric password embedded in the launch sequence when SecureVideo launches the Zoom engine. With this embedded password set, an unauthorized user randomly entering Zoom meetings by guessing 9 digit codes would then have to guess a 10 character alphanumeric code in addition, the odds of which are roughly 1 in 3 quadrillion. Therefore, the likelihood... of "Zoombombing" would be limited to 1) SecureVideo 9 digit codes which are shared by authorized session participants to unauthorized persons outside of the SecureVideo system; and 2) the harvesting of Zoom Meeting IDs from the Zoom interface once a meeting is in progress (we are not able to hide the Zoom meeting ID and password in the Zoom UI) by an authorized session participant and the sending of that Zoom Meeting ID to an unauthorized person. (A host can choose to eliminate even this by choosing to lock the meeting so that no new participants can enter.)

The only technique we view as a complete mitigation is the locking of a meeting, which is something that providers can easily be trained to do. At the same time, we have in the past filed a feature request with Zoom for the option to have the Zoom Meeting ID removed from the Zoom UI, however this feature request has not yet been acted upon. If and when that feature is implemented, SecureVideo will implement a currently backlogged feature to allow customers the option to make SecureVideo 9 digit codes expire after a single use, which would promote security at the expense of usability—e.g., patients who fail to connect on their PC would now have to request a new code from their host to be able to connect on an alternate device such as their smartphone—and thus would comprise a serious risk/reward decision to be made by each customer.