Zoom Security

Unrecorded Zoom meetings happening in real time have 2 forms of security available:

1. Whether or not the organizer chooses to password protect the meeting, thereby requiring everyone who attends to be an invitee and enter a password (and how secure those passwords are kept)
2. How securely the organizer communicates the link to the meeting

If the meeting is on a calendar that is open to the UCSC community, and someone knows about it, it is possible to simply use the link to connect. A list of the active meeting participants is always available to the organizer and participants, so checking the list of who is in the meeting is one way to understand if only the expected attendees are participating.

As far as what is kept by Zoom and by ITS as meeting records, a list of participants can be retrieved by the organizer for a short period of time after the meeting through the Zoom interface.

UCSC does not support Zoom's Cloud recording service, so any recording of a Zoom meeting is currently stored on the computer of the person who initiates the recording. The organizer can set Zoom so that only they are allowed to record.

According to an ITS director, the following is an important policy rather than a technical aspect:

> from a security and policy perspective both scenarios (lurking or accessing a recording without permission) would be violations of acceptable use policies. We always need explicit permission to view files belonging to our users, whether those files are documents, email, or recordings.

Of course, this does not rule out getting such permission—perhaps even from someone other than the user—but they can't just go in and start poking around.

For more information see the ITS website: https://its.ucsc.edu/zoom/security.html.