June 2020

Audience Identification For Secure Video Streaming

Loren Groves

Audience Identification For Secure Video Streaming

ABSTRACT

Organizations that utilize video conferencing, live streaming, or provide recordings of internal events, are at risk of organizational information being leaked, if an unauthorized participant, e.g., another person in the same room as an authorized event participant, gains access to such events. This disclosure describes the use of remote participant audio/video feed to prevent information leakage from a restricted event. Prior to remote participation in an event, user permission is obtained to receive and record media from the remote participant device. The received media are reviewed, e.g., by security personnel, or by automated tools, to detect the presence of unauthorized persons. If unauthorized persons are detected, the remote participant's access to the event is revoked. Recorded media can be utilized post-facto for investigations in case information leakage occurs.

KEYWORDS

- Video conference
- Livestream
- Remote participant
- Information safety
- Data leaks
- Security footage
- Compliance

BACKGROUND

Many organizations utilize video conferencing applications for internal meetings, e.g., all-hands meetings for a company, department meetings, team meetings, etc. When employees,

interns, contractors, etc. participate in such meetings, the organization has little control over who is watching or able to listen, e.g., others in the participant's household, or if the participant joins from a public place (e.g., coffee shop, train, airport, etc.), others near them. There is a risk of organization internal information shared during a video conference being leaked due to the presence of such unauthorized parties. Currently, the only option for organizations is to reduce or eliminate such meetings.

DESCRIPTION

This disclosure describes techniques to secure a videoconference from unauthorized participants. The techniques are implemented with permission from users who participate in the videoconference. Users that deny such permission may be restricted from participating in the videoconference or their mode of participation may be limited, e.g., they may be restricted from viewing shared screen content or from receiving audio of the meeting.

A user that participates in a video conference, views a live stream, or a pre-recorded video, user permission is obtained to enable the camera and microphone of the user device that is in use. The camera is used to authorize the person to begin watching the content, as well as to provide permission to continue watching.

The microphone is activated to detect if another person is present in the room where the participant is located, e.g., by detecting shuffling, the sounds of doors opening or closing, typing sounds that are off-camera, etc. If such noises are detected, participation of the user is stopped or security personnel are added to the videoconference. The user is prompted to move to a private location to continue participation. Participation is denied if the problem persists, e.g., noises continue to be detected.

Still further, participation is granted only after the user's camera and microphone are enabled. With user permission, media from the microphone and camera can be recorded, viewed live by security personnel, or reviewed for security risks using automated techniques.

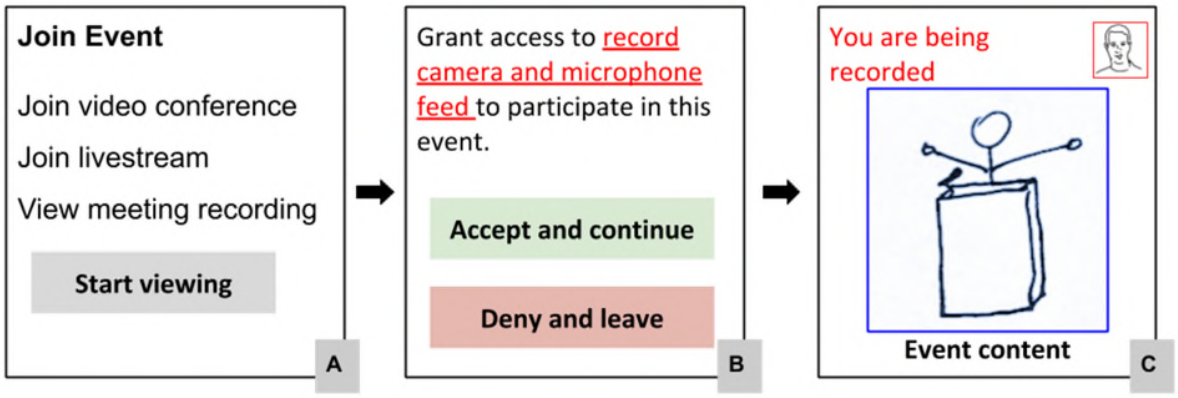

Fig. 1: User flow to join an event: (A) Participant selects an event; (B) Participant provides permission to record; (C) Participant joints the event; warning is provided that the participant is being recorded.

- **Manual review of participant recordings:** Audio and video feeds are obtained from a user device that participates remotely in an event (e.g., a video conference, livestream, or viewing of recorded video). For example, instead of providing a normal video conference use interface, a video player interface is displayed, with a clear indication that the user's audio/video are being recorded. The recorded media are stored, e.g., using a default storage period. If secure data that was provided during the event is leaked, the organization can investigate the leak by reviewing the recorded audio and/or video for every remote viewer.
- **Live review by security personnel:** Audio and video feeds are obtained from a user device that participates remotely in an event (e.g., a video conference, livestream, or viewing of recorded video) and are provided live to security personnel. The security personnel are also provided additional information regarding each participant. With user permission, and based

on the specific configuration, such additional information can include the participant's organizational identifier (e.g., username), network information (e.g., IP address), length of participation, secure video views, etc. The security personnel can also disconnect the participant, or pause the event stream and engage in interaction with the participant, e.g., to ask security questions.

- **Automated review:** Automated techniques, e.g., machine learning based or other video analytics techniques, are used to analyze participant audio and video feeds to detect if there is a threat of information leakage. Upon detection of a likely threat, security personnel are notified and/or the user's participation in the event is terminated. For example, the machine learning model can be trained using prior media content of live events such as meetings. The model is trained to detect the presence of multiple users at a remote participant endpoint based on audio only, video only, or a combination. Multiple viewers can register at a participant endpoint, e.g., two employees participating from the same endpoint. Registration can be based on organizational username. With user permission, the automated analysis can include verifying the identity of the remote viewers, e.g., based on face recognition.

Further to the descriptions above, a user is provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., username, user's image, network address, audio/video feed, participation in video conferences, prior videos viewed, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no

personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes the use of remote participant audio/video feed to prevent information leakage from a video conference, livestream, or views of recorded video content, all corresponding to a restricted event. Prior to remote participation in an event, user permission is obtained to receive and record media from the remote participant device. The received media are reviewed, e.g., by security personnel, or by automated tools, to detect the presence of unauthorized persons. If unauthorized persons are detected, the remote participant's access to the event is revoked. Recorded media can be utilized post-facto for investigations in case information leakage occurs.