Shashwat Mishra and Joonas Uusi-Autti

Security and privacy issues with conference applications

Course: Security and privacy economics

December 25, 2021

Author: Shashwat Mishra and Joonas Uusi-Autti

Contact information: ge58tid@mytum.de, ge58wun@mytum.de

Supervisor: Tibor Posa

Title: Security and privacy issues with conference applications

Project: Course: Security and privacy economics

Page count: 13+0

Abstract: Small research in the field of security and privacy concerning video conference applications

Keywords: literature review, security, privacy, survey,video conference applications,survey

Contents

1 INTRODUCTION 1

2 RESEARCH AIM AND QUESTION 2

3 LITERATURE REVIEW 3
3.1 Privacy of video conference applications 3
3.2 Security of video conference applications 4

4 SURVEY 6

5 RESULTS 7

6 DISCUSSION 8
6.1 Suggestions 8

BIBLIOGRAPHY 9

1 Introduction

After the COVID-19 pandemic hit hard all over the world, video conference applications (VCA) usage has been increasing a lot in education and work environments and every user is not familiar with applications and their features (Kristóf 2020). Especially education has been affected a lot. Remote-working has been a possibility, although not very common one. Remote-learning has not been common and due to COVID-19 pandemic every student and teacher had to familiarize new techniques. And by rushing into using these applications, it is possible that very rare group of students know what else VCA's do, besides the obvious, giving an opportunity to attend classes and learn. Data collecting is happening nowadays everywhere. It is clear that e.g. Zoom collects data (Dvorak 2020), but do students know what kind of data? And are students even concerned about data collecting? Security problems happens everywhere, where there is network connection involved. High increase of using VCA's has also brought up some new security flaws to these applications. But what kind of issues and how organizations handle these new threats?

We conducted a literature review [3] to gain more background information about the issues and a questionnaire survey focusing on privacy and security issues with VCA's [4]. Survey was directed to university students.

In the results [5] section we open up our findings and (to be continued)

In the end of the research, reader can find discussion about the results and suggestions towards the future [6]. These suggestions are solely based on our point of views, which are found in the research process and cannot be generalized, because of the fact that only three applications are being researched.

2 Research aim and question

Research aim is to collect and analyze data are students concerned about privacy issues while using video conference applications. Data collecting is done by questionnaire survey.

Research question is Security and privacy issues with call applications? Research is focusing on security and privacy problems only in the three biggest VCA applications Zoom, Google Meet and Microsoft Teams. These are are clearly most heavily used and out of the three, Zoom has the most users, 300 million and counting.

3 Literature review

Literature review is a survey of chosen area of study. It synthesizes the infor- mation of selected area of literature, critically analyzing the information. Indications of gaps in knowledge, limitations in theories and new points of view may occur in process, which is done in scientific, organized way ("What is a literature review?" 2021).

3.1 Privacy of video conference applications

There has been a great number of articles in the past years concerning about the privacy issues with VCA's ("Using Video Conferencing Platforms for collecting data from Human Participants" 2021). It is clear for every user that these applications are collecting data from the users but the level of understanding what kind of data is collected and for what data is used for, is not as high as it probably should be.

While the Zoom application is the most used VCA there is, other video conference applications are also vulnerable to privacy issues. Every VCA has different privacy policies but they don't differ that much and basically none of these options aren't great (John 2020). And according to these three biggest companies (Zoom, Google, Microsoft) privacy policies, all of the mentioned companies can collect data when using these applications.

Although every one of these companies stated that they respect customers privacy, has Zoom for example faced investigations towards their privacy practices and especially data privacy laws in the United States makes it hard to defend customers against Zoom's privacy practices (Goodyear 2020). But like stated before it is not just Zoom, problem involves also other companies.

One of the biggest problems concerning privacy policies is that they are very rarely read. And that causes problems to user's data. For example in Zoom, its administrators can see detailed information on how, when and where users are. Also they have access to calls which have been recorded and they can basically join any call at any time (Goodyear 2020). While all this is happening to you, it is also happening to your contacts. Zoom can collect

your contact lists, facebook profiles and contacts facebook profiles. This is all stated in the privacy policies but like stated before, very few people read them and even fewer actually understands the terms.

Now, during the COVID19 pandemic, when people have started to use more of these VCA's, malicious users have had time of their lives. Especially when some conference meeting links have been public on some website. These malicious users have been using machine learning techiques to infiltrate to the meetings and when in a meeting, collected personal data from users. Data such as profile pictures, usernames, voice and personal data which has been shared in the meetings (Dima Kagan 2020). Malicious users can also, with these informations, possibly predict users interests, activities and even social security numbers.

These privacy issues can lead to serious risks and damage the companies or inviduals. And how the issues concern users and are users usually aware of them, will be surveyed here 4.

3.2 Security of video conference applications

Since the COVID19 pandemic has been tearing the earth, video conference applications usage has been increasing tremendiously. And usually when a application or software generates popularity to such an extend (e.g. Zoom went from 10 million daily users to 300 million daily users (Wagenseil 2021)), there is usually security flaws involved. In march 2020, when basically everything went online (work,education), different organizations started to use different platforms. Like stated before, three biggest platform considering VCA's, are Google Meet, Zoom and Microsoft Teams.

One of most common security issues was end-to-end-encryption(E2EE), which allowed other users in the meeting see lot about you and some people could "Zoombomb", these meetings (Wagenseil 2021). "Zoombombing" is a phenomenon where malicious user "hijacks" the meeting and shares content which is disruptive for users. End-to-end-encryption is a scheme for communication for VCA's and other messaging applications in which only user in that precise meeting can only send and receive messages. For "Zoombombing", this is the most important security scheme (Takanori Isobe 2020). Out of these three VCA applications, only Zoom provides E2EE but only in text chat and when sharing files. Google

Meet and Microsoft Teams do not provide E2EE in any of the following criterias: text chat, voice calls, video calls, file sharing and screen sharing (agency 2020). While these findings are from 2020, E2EE functions may have been upgraded.

While these three biggest VCA platforms have similiraties, there are some differencies how these three applications operate. User can use every one of them via browser but Google Meet operates solely in browser and this feature separates Meet from the other two. Google has said that it limits the attack surface of their platform, because they can immediately deploy changes, since it is only accesible on the browser. In addition, Meet requires Single Sign-On(SSO) with their Google accounts, when joining the meeting. Usually Google accounts consists of two-step verification and with these functios, Google focuses on preventing phishing, account hacking and similar attacks as "Zoomboming" (Nicholas Hunter Gauthier 2020).

4 Survey

5 Results

6 Discussion

6.1 Suggestions

Bibliography

agency, National security. 2020. “Selecting and Safely Using Collaboration Services for Telework - UPDATE”, https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/CSI_%20SELECTING_AND_USING_COLLABORATION_SERVICES_SECURELY_FULL_20200814.PDF.

Dima Kagan, Michael Fire, Galit Fuhrmann Alpert. 2020. “Zooming Into Video Conferencing Privacy and Security Threats”, https://arxiv.org/pdf/2007.01059.pdf.

Dvorak, Chyelle. 2020. “What Data Does Zoom Collect?”, https://www.reviews.org/internet-service/what-data-zoom-collects/.

Goodyear, Michael. 2020. “The dark side of videoconferencing: The privacy tribulations of Zoom and the fragmented state of U.S. data privacy law”, https://houstonlawreview.org/article/12850.pdf.

John, Allen St. 2020. “It’s Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.”, https://www.hawaii.edu/its/wp-content/uploads/sites/2/2020/05/Google-Meet-Microsoft-Teams-Webex-Privacy-Issues-Consumer-Reports.pdf.

Kristóf, Zsolt. 2020. “International Trends of Remote Teaching Ordered in Light of the Coronavirus (COVID-19) and its Most Popular Video Conferencing Applications that Implement Communication”, https://ojs.lib.unideb.hu/CEJER/article/download/7917/7236.

Nicholas Hunter Gauthier, Mohammad Iftekhar Husain. 2020. “Dynamic Security Analysis of Zoom, Google Meet and Microsoft Teams”, https://svcc2020.svcsi.org/accepted-papers/Dynamic-Security-Analysis-of-Zoom,-Google-Meet-and-Microsoft-Teams.

Takanori Isobe, Ryoma Ito. 2020. “Security Analysis of End-to-End Encryption for Zoom Meetings”, https://eprint.iacr.org/2021/486.pdf.

“Using Video Conferencing Platforms for collecting data from Human Participants”. 2021, https://research.mcmaster.ca/ethics/mcmaster-research-ethics-board-mreb/videoconferencing/.

Wagenseil, Paul. 2021. “Zoom security issues: Everything that’s gone wrong (so far)”, https://www.tomsguide.com/news/zoom-security-privacy-woes.

“What is a literature review?” 2021, https://www.rlf.org.uk/resources/what-is-a-literature-review/.