Joonas Uusi-Autti

Security and privacy issues with video conference applications

Course: Security and privacy economics

January 24, 2022

Author: Joonas Uusi-Autti

Contact information: `ge58wun@mytum.de`

Supervisor: Tibor Posa

Title: Security and privacy issues with video conference applications

Project: Course: Security and privacy economics

Page count: 19+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

2.1 Hypothesis for the survey 2

3 LITERATURE REVIEW 3

3.1 Privacy of video conference applications 3

3.2 Security of video conference applications 4

4 SURVEY 6

4.1 Preparing the survey 6

4.2 Question template 6

5 SURVEY RESULTS 8

5.1 Analysis of the answers 8

5.1.1 Privacy of VCA’s 8

5.1.2 Security of VCA’s 10

6 DISCUSSION 13

6.1 Suggestions 13

6.1.1 Good practices 13

BIBLIOGRAPHY 15

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 2020a), 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 students handle these new threats?

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

In the results section [5], findings are analysed from the survey and observed how students use VCA's and how they react when facing some kind of security issues. And most importantly, are they aware of the data collecting which happens while using these kind of applications.

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 researcher's point of view, which are found in the research process and cannot be generalized, because of the fact that only three applications are being researched and answers came only from two universities.

2 Research aim and question

Research aim is to collect and analyze data and get knowledge about are students concerned about privacy and security issues while using video conference applications. Data collecting is done by questionnaire survey, using the surveymonkey platform.

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. While Microsoft Teams and Google Meet come clearly second and third, they are far behind from Zoom, when observing the user count.

2.1 Hypothesis for the survey

Since the growth of using the video conference applications has been enormous from the beginning of the COVID19 pandemic and every student has been dealing with VCA's in the past two years, it is probable that a small group of students are aware of flaws with these kind of platforms. If a student has been interested about security and privacy issues in general, a student is more likely to have understanding and knowledge of these issues. Especially students in the field of informatics and to be more precise, students who are majoring in cybersecurity. But since the survey is completely anonymous, it is not defined what one is studying.

The hypothesis for the paper is that most of the students are not aware of the privacy and security issues with VCA's. It is believed that they have understanding or knowledge about what is being collected or what kind of security issues there might be but the overall level of concern is not that high. Also it is probable that most of the students do not care about privacy policies when using applications.

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).

In this literature review part, research focuses on privacy point of view and security point of view.

Literature was gathered from Google Scholars and IEEE Xplorer research databases. With 12 different keyword combinations from these two databases, it was possible to gather enough articles for the literature review. It was clear that most researched application was Zoom, mainly because it has been growing to be the biggest platform during the COVID19 pandemic.

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 invidual s. 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 (NSA 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

4.1 Preparing the survey

Survey's questions were conducted from the gathered literature and they were made easy to answer, to get enough data. Survey was sent to studentgroups to two different universities, University of Jyväskylä and Technical University of Munich.

Answers were submitted anonymously, so the analyzed data is general (mp degree programmes, university etc.). Although probably there would have been some differencies within the answers, considering the studyculture, which is a bit different in these two countries.

Questionnaire was online for two weeks for students to answer. N was XX and the questionnaire consisted of 10 questions, privacy and security issues with video conference applications. Questions will be examined more in detail in the next section.

4.2 Question template

In this section you can find questions and short explanation behind the question.

1. Are you aware of data collecting when using video conference applications?(Zoom, Microsoft Teams, Google Meet) Answers: Yes/No. I would assume that not that many students are not aware data collecting while using VCA's.

2. Are you, as a student, concerned about data collecting when using video conference applications?(Zoom, Microsoft Teams, Google Meet) Answers: Yes/No. Follow-up question for the fist one.

3. How concerned you are about data collecting? (1 = Not at all, 4 = Very concerned) Four options to see are the students concerned.

4. What video conference application you use the most? Options are Zoom, Meets, Teams and Other, please specify. Here one sees what platforms students use the most.

5. How often do you read applications privacy policy text? 5 options. It is documented that truthfully speaking, it is rare to read applications privacy policy.

6. What kind of data you think video conference applications collect from users? Open question. Gathering assumptions of what kind of data platforms collect.

Security part of the questionnaire.

7. Do you trust video conference applications security functions? Yes/No. Users trust towards applications.

8. When organizing a meeting, do you protect the meeting with password? Yes/No. Password protection is one of the first ways to protect one's meeting. During the pandemic, this has become more frequent way.

9. What kind of other security measurements you take into consideration when attending/organizing a meeting? (waiting room, link sharing, etc.) Open question. There are other ways of protecting a meeting than a password. Are students familiar with them?

10. What kind of security threats do you think are most common with video conference applications? Open question. Gather information about what students think are the most common security threats.

With these questions appointed to students, we can hopefully see a pattern on how students react to privacy and security issues. And something about their knowledge towards these issues.

5 Survey results

Survey was analyzed question by question, and bigger themes were combined also to one bigger picture. Number of survey participants was 29, and due to a number so small, these results are more of a first scratch or guideline giving results. Survey was shared on different platforms and it reached 497 students and answering percent was 5.84%. Participants were residents of Finland or Germany. Nationalities differ from the place of living. This survey can give insights of the question are students aware of privacy and security issues with video conference applications.

5.1 Analysis of the answers

5.1.1 Privacy of VCA's

There was surprising results concerning privacy issues in VCA's. Over half (58.62%) of the people were aware of data collecting which is happening every day. Although level of awareness should be nowadays higher, due to excessive growth of usage, it is still more than anticipated. Participated students were from different degree programmes (not only informatics), and with that knowledge percentage is satisfactory. While the level of awareness about the issues is good, students are not that concerned about these issues. While the phenomenon of the data collecting is not anything new, students may have not been thinking about the fact that they are dealing with these issues on daily basis. Everybody has heard from legal issues with Facebook (Meyer 2018) but probably students did not realize that even applications which are used to ensure learning, could be problematic. While the percentage of concern was a tight (48.28% were concerned), their level of concern is not that high. About 20% of the students were not concerned at all about privacy issues while majority was slightly concerned (62.07%). Only every tenth student was very concerned about this ongoing issue. This opens up a question that are the students educated enough about what is going on? And in these times, who is responsible for educating the students about their privacy while using different applications. If the lecturer is not aware, then the student tries to find information, if he/she is interested about these kind of issues.

It was not surprise that Zoom was the most used platform. Like stated before, Zoom is by far the most common VCA's in use today. Almost two thirds (62.07%) of the students in this survey use Zoom as their main VCA. Microsoft Teams came second (24.14%) and Google Meet third (10.34%). Skype also was mentioned but only from one student. Zoom is still the most used platform even though it has faced multiple legal issues concerning privacy policies and even in 2020 Zoom chief executive Eric Yuan apologized for falling short of users privacy and security expectation and that they never expected that "every person in the world would suddenly be working, studying, and socializing from home." (Harwell 2020).

Like stated before, every VCA company has their own privacy policies but they do not differ that much (John 2020). In these long and boring texts user can find every detail how and what is collected from the user but it is clear that if the text is really long, it is probable that user just skims through it or do not read that at all. 41.38% of the students never reads privacy policy texts and the same amount of students rarely reads them. While that is alarming, it is also understandable, due to legal point of view of the texts. Even if one reads the whole text, does the future user actually understand what is being agreed upon? A bit over every tenth(13.79%) students reads privacy policies sometimes and only 3.45% usually. This survey showed that no one reads privacy policy texts always when signing up or downloading a new application. It is an agreement like any other valid agreement, so why applications privacy policies are dismissed so often?

Survey participants had a broad and imaginative guesses and knowledge about what kind of data is shared to companies from meetings. Like founded in the literature review section, this kind of data usually consists of names, profile pictures, contact lists, audio/video, emails, location and so on. Everything listed before, was in the answers. Not one listed everything in their answer and on average one student listed three data pieces in the answer. Some of the students even stated in the answers that "Hopefully not images/emails are shared" and this shows that everybody is not aware of these things. Device information was also one of the most common answers and shared links and images during the meeting was quite common, no one thought about ip addresses. And unofortunately, VCA companies collects this information also (Dvorak 2020b).

All in all students level of knowledge and understanding was quite decent in the frame of this study. Comparing these results to the hypothesis, results more positive than negative and shows that students are aware of privacy issues in the world of applications, at least to some extent.

5.1.2 Security of VCA's

When it comes to applications security concerns, it is more highlighted in current times and has been developing more every passing year. Users talk about security point of views when dealing in the internet or when using applications but how familiar they are with risks and most simple functions to icrease security?

Answers were divided closely when asking about trust towards VCA's security. Majority of the students (51.72%) did not trust the security functions in VCA's, but still they "have" to use these applications. It can be hard to process the fact that one lacks trust towards something but still has to deal with it basically on daily basis. Security issues are under a microscope all the time in every field. But still people neglect security issues when dealing with computers and applications. It might be because people do not have deep understanding about these issues. For example if one knows that car doors do not close properly and they just are completely open due to some broken element, everyone fixes the issue somehow. But when dealing with some applications, in this case video conference applications, only about a half (55.17%) of the students secures their meetings with a password. Why is that so "low"? If the meeting is not protected with a password, anyone who has a link can join, collect data or "Zoombomb" the meeting. The issue is important because while teaching aspect has gone online, also student meetings are now online, at least partially. If it is a course-related meeting, catching up to fellow students or some other reason, these "events" have been occuring using VCA's, especially when the restrictions have been very strict. And because of these stated reasons, password protection should be number one on the list how to protect yourself when using VCA's. It is easily implemented and is the first layer of security.

But protecting a meeting with a password is only one "simple" way to enhance security, what other functions and ways students might use when attending or organizing a meeting? Some of the students have no idea how raise the level of security but only just a few. Most common ways to raise the level of security is securing that the meeting link is only available those who should attend the meeting. This is really easy step and makes the meeting again a bit more secure. There have been situations where the link has been on some public webpage or shared through social media accounts and by doing so, the link might end somewhere it does not belong.

The next step from link sharing is waiting room for the meeting. Waiting room was also mentioned quite a lot and while it might be annoying to participants or meeting organizer, it is very good way to ensure that there is only those people in the meeting, who should be there. Waiting rooms idea is that admin of the meeting grants access to the meeting from a list of participants who are trying to get in. Usually this means that admin must have some kind of list of the possible participants and the admin checks the names or email-addresses of the possible participants and if there is a match, user is granted an access to the meeting. Waiting room is basic feature of all three biggest VCA's platforms (Zoom, Google Meet and Microsoft Teams).

There was also couple of answers that attendance should be possible with an alias. When using alises it protects the user from not giving his/her own name out there. But then there might be a problem for the organizer who is not sure of the participants, since there might be some made up names. Then there was lonely answers including covering webcam, when sharing a screen there should be only one window open and when linking webpages to the meeting, they should be only from trusted sources.

And do students know about most common security threats with VCA's? While these three biggest platforms tries to improve their security, there is still some problems with it. Students answers were on the right track. Hijacking or "Zoombombing" the meeting, suspicious links/users were the most common answers. These are true and usually made possible by the user itself. One answer stated this possibility and answered "The most important security threat still locates between a screen and a chair". If there appears, in a chat for example, a link which seems to be irrelevant or suspicious in any other way, it is users responsibility to decide what to do with it. Behind these links might be some malicious scripts which then are performed and might be very harmful for the person who clicked. One common answer was also issues regarding recording the meetings. In some cases, lecturer do not want to record the meetings, due to reasons like discussion oriented lectures, so that students would be encouraged to participate in the discussion without a fear that it is recorded. Discussions can sometimes contain personal information and students do not want personal information to be shared and stored somewhere. And again, only a few did not know what kind of threats could be common when using these applications.

This study shows with a small sample that many of the students are clearly concerned about the security issues. They also have knowledge about how to easily protect themselves from them and what are the possible threats.

6 Discussion

Although survey results were better than expected, these issues need more close examination. Survey sample was relatively small (N=29) and consisted of only two universities. With bigger sample and wider variety of students (eg. high-school students included) the results would be more precise. Still this survey can show general trend to some extent.

While students who participated to this study had a decent level of privacy issues, it needs to be higher. Educating students about the issues concerning applications privacy policies should be somehow included in the studies, to be more precise, it would be great if lower level educational organizations (elementary school, high-school) provided common knowledge to students about application privacy policies. It could be part of a computerclass or social studies, since basically everything is in the internet in current times. When approving application agreements it is like approving a rental agreement and everyone reads rental agreements carefully. The difference is that rarely you can have a "sneak-peak" of an application versus one has a chance see the room/apartment before signing rental agreement.

And same applies to security issues. People have a tendency to secure their lives somehow. Depositing money to the bank versus hiding it under a matress for example. But like in applications and real life, sometimes security flaws comes from the person/user itself. This is not always the case and accidents happen but whether you are securing your housedoor with a lock or securing a online meeting with a password, it should be clear as a water that this is the standard to follow.

6.1 Suggestions

6.1.1 Good practices

Suggestions and good practices when dealing with video conference applications from privacy and security point of views.

Privacy Good practices and application functionalities for protecting privacy while using video conference applications (NSA 2020).

1. Does the service implement end-to-end encryption?

2. Are strong, well-known, testable encryption standards used?

3. Can users see and control who connects to collaboration sessions?

4. Does the service privacy policy allow the vendor to share data with third parties or affiliates?

5. Do users have the ability to securely delete data from the service and its repositories as needed?

6. Has the collaboration service's source code been shared publicly (e.g. open source)?

7. Always read privacy policy texts

Security Good practices and application functionalities for secure video conferencing (CISA 2021; NSA 2020).

1. Connect securely

2. Control access

3. Manage file, screen sharing and recordings

4. Update to latest versions of applications

5. Has the service and/or app been reviewed or certified for use by a security-focused nationally recognized or government body?

With these rules and suggestions user has a good foundation to use video conference applications more securely and protect own privacy.

Bibliography

CISA. 2021. “Guidance for securing video conferencing”, https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.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. 2020a. “What Data Does Zoom Collect?”, https://www.reviews.org/internet-service/what-data-zoom-collects/.

———. 2020b. “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.

Harwell, Drew. 2020. “Everybody seems to be using Zoom. But its security flaws could leave users at risk”, https://www.washingtonpost.com/technology/2020/04/02/everybody-seems-be-using-zoom-its-security-flaws-could-leave-people-risk/.

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.

Meyer, David. 2018. “Facebook is breaking law in how it collects your personal data, court rules”, https://www.zdnet.com/article/facebook-is-breaking-law-in-how-it-collects-your-personal-data-court-rules/.

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.

NSA. 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.

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/.