E3S Web of Conferences 371, 05026 (2023) https://doi.org/10.1051/e3sconf/202337105026
AFE-2022

Zoombombing: causes and preventions

Kamran Siddiqui[1*] and Shabir Ahmad[1]

[1]College of Business Administration, Imam Abdulrahman Bin Faisal University Dammam 31451, Saudi Arabia

Abstract. This paper aims to share the Zoombombing: a new phenomenon that emerged during COVID-19, its causes, and measures to prevent Zoombombing. Finally, it provides recommendations to prevent such incidents. Zoom emerged as the most popular alternative teaching tool during COVID-19. However, even though Zoom has utilized state-of-the-art encryption methods, it has underestimated privacy expectations among its exponentially growing customer base. Zoom has many options settings for users to customize and secure their videoconferencing platform to minimize Zoombombing. However, some users overlook these security features, which leaves them vulnerable to offensive material displayed by attackers in a virtual classroom setting. Furthermore, most Zoombombings were made by insiders who had legitimate access to Zoom meetings, particularly students in high school and college classes. To reduce Zoombombing, teachers can enable settings, such as waiting room, restricting access to screen share, and physical reporting. Moreover, severe institutional punishment for the attackers and their insider supporters can discourage such activities.

1 Introduction

During COVID-19, in-person office meetings and academic classrooms were transformed globally into at-home or online video conferencing. Unfortunately, during such meetings and classrooms, a fringe community of students, also known as internet trolls, hijacked and disrupted the online sessions by inserting pornographic, lecherous, and highly offensive racial images and video content on participant's screens, resulting in the aborting of planned meetings. These videos conferencing violent attacks on one's sensibility were labeled as Zoombombing. The name "Zoom" is associated with one of the most popular among many platforms used globally since the start of COVID-19 called "Zoom videoconferencing software program."

Such incidents, of an intrusive and invasive nature, have caused substantial psychological injury to many people in business and academic organizations worldwide. As a result, Zoom was heavily criticized for its insecure videoconferencing platform, and several companies have prohibited their employees from using the Zoom platform.

Zoom's customer base grew exponentially, and so did the venomous incidents of Zoombombing. Finally, the authorities had to step in to decrease such acts by filing

* Corresponding author: KASiddiqui@iau.edu.sa

criminal charges against disruptors of online video conferencing. Since then, Zoom has been diligently working to enhance the security of its software program to reduce video session disruptions and continues to satisfy its customers with its user-friendly platform.

2 Literature Review

Zoom and its users have recently experienced a security crisis named Zoombombing [1]. The phenomenon has emerged in which aggressors join online meetings to disrupt and harass their participants [2, 3]. The idea was started as 'online classroom pranks' and swiftly moved to organized disruption efforts, sometimes also used as a tool for racial harassment and hate speech [4], which the law enforcement agencies have threatened to punish as serious offense [5].

Since the pandemic's beginning, the transformation of our work environment, various videoconferencing tools, including 'Zoom,' 'Google Meet' and 'Microsoft Teams' have replaced our offices with virtual home offices [6]. However, as many businesses and academic institutes communicate online, a new phenomenon called 'zoombombing' has emerged, whose primary purpose is to harass and disrupt videoconference attendees by joining the session. This prank has developed into an organized interruption of videoconferencing, spewing pornographic videos and vile images, which was noticed by the FBI, resulting in an announcement that it would file criminal charges against perpetrators to minimize zoombombing [5]. Searching for the causes of this phenomenon attribute it to the mega-disruption of people's lives due to drastic changes in their life-work habits, and such an environment creates anxiety and embedded harassment traits. It was further suggested that such foggy emotions look for a vent, and they found it in the form of videoconferencing platforms that were used extensively and mainly were insecure [2].

After analyzing zoombombing data, [2] concluded that the harassment attacks were not inflicted by external forces crashing the video session. Instead, these attacks were carried out by the invitees who were authorized to enter the session, especially in the case of high school and college online classes. On the other hand, when Zoom's customer base rapidly increased due to the pandemic, several security problems in their platform were identified. To explain Zoom's dilemma, Konrad says that though Zoom is diligently working to strengthen its platform and minimize security breaks, at the same time, they are hesitant to tinker too much with its user-friendly platform, which is the main attraction of its global popularity.

This article has also attempted to compare the most popular video conferencing tools: Google Meet, Microsoft Teams, and Zoom.

Google Meet (formerly known as Hangouts Meet, commonly known as Meet) is a video-communication platform developed by Google LLC. Google is the largest search engine and provides internet-based advertising services. Google is ranked 4th in Interbrand's Top 100 Global Brands (2020), with massive brand equity of USD 165 billion.

Microsoft Teams is a video conferencing tool developed by the world's largest software giant Microsoft. The company produces computer software, consumer electronics, and related services. Microsoft is ranked 3rd in Interbrand's Top 100 Global Brands (2020), with massive brand equity of USD 166 billion (Interbrand, 2021).

Zoom Meetings (commonly known as Zoom) is a proprietary video teleconferencing software developed by Zoom Video Communications. It provides video telephony and online chat services through a cloud-based peer-to-peer software platform. During COVID-19, this platform became the backbone of education and social relations.

2.1 Systems Requirements

Video conferencing comprises a central cloud-based platform connecting calls between personal device clients and centralized cloud-based meeting room device endpoints. The quality of video conferencing services depends on the hardware and software employed in this service, irrespective of the video conferencing platform. A video conferencing system combines capable equipment, a robust network, and the software used to integrate it. However, three essential ingredients for any video conferencing system include: (a) computer should have faster processing, (b) sufficient network bandwidth is needed, and (c), high-resolution webcams with microphones are required. The table below provides a comparative account of systems requirements for the three most popular video conferencing platforms, including Google Meet, Microsoft Teams, and Zoom.

Table 1. A comparative account of Systems Requirements for Meet, Teams & Zoom

Criteria		Google Meet	Microsoft Teams	Zoom
Hardware Requirements	Processor – Minimum	Dual-Core processor	Dual-Core 1.1 GHz or higher	Single-core 1.0 GHz or higher
	Processor – Recommended	Quad-core processor	Quad-core processor	Dual-core 2.0 GHz or higher
	RAM – Minimum	2.0 GB dedicated	4.0 GB dedicated	1.0 GB
	RAM – Recommended	8.0 GB	8.0 GB	4.0 GB
Bandwidth	Minimum bandwidth	3.2 mbps	1.2 mbps	2.0 mbps
Operating Systems Supported	Apple Mac OS	√	√	√
	Google Chrome OS	√		
	Linux	√	√	√
	Microsoft Windows	√	√	√
Mobile Operating Systems	Android	√	√	√
	Apple iOS 12.0	√	√	√
Browsers Supported	Apple Mac: Safari	√	Partial	√
	Google Chrome	√	√	√
	Microsoft Edge	√	√	√
	Microsoft Internet Explorer	√	√	√
	Mozilla Firefox	√		√
Source		Google Meet Help (2021)	Microsoft Teams Support (2021)	Zoom Support (2021)

Two observations can be made here. Firstly, all mainstream operating systems, including Apple Mac, Microsoft Windows, and Linux, were all supported by all three video conferencing platforms. Similarly, three video conferencing giants support two major mobile operating systems, including Android and Apple iOS. In addition, all mainstream browsers, including Google Chrome, Microsoft Edge, Microsoft Internet Explorer, and Apple Mac: Safari, are all supported (fully or partially) by all three major players in the video conferencing industry. A second observation is related to hardware and internet bandwidth requirements. It appears that Zoom has relatively low hardware requirements for video conferencing. However, Microsoft Teams claims to be having minimal requirements for internet bandwidth usage.

2.2 Teaching and Learning Issues

Due to the rise of the COVID-19 pandemic, the teaching-learning process has undergone a significant revamping and moved from physical classrooms to virtual classrooms. Throughout the world, the lecturing process was conducted online. Many video conferencing tools were utilized for the lecturing processes, including Zoom Meetings, Microsoft Teams, and Google Meet. The use of video conferencing tools brings excellent benefits, but on the other hand, it also causes the students to face problems. Therefore, this study aimed to compare the features of these video conferencing tools, the problems they arose, and strategies for solving them in the lecturing process.

Many teaching and learning features are standard among all three platforms, including inviting external participants, screen sharing, recording, virtual backgrounds, joining from the browser, native mobile apps, flexible layouts, student engagement tracking, accessibility, whiteboarding, classroom-oriented chat, specialized hybrid learning, in-conference text chat, event hosting with participant roles. However, five teaching and learning features make Zoom the preferred choice for educators. These five features include Learning Management System (LMS) integration with Zoom, breakout rooms in Zoom meetings, polling, recordings, and in-conference chat.

Zoom integrates more than 150 learning management systems, almost with all mainstream players, including Blackboard and SAP Litmos. LMS-Zoom integration enables the teachers to bypass the laborious step of manually enrolling each student in the session. LMS-Zoom integration can automatically notify enrolled students and record all data in a single system, providing easy setup procedures

Zoom Breakout rooms allow the teacher to split the Zoom classroom meeting into 50 separate sessions and allocate participants to different breakout rooms. Alternatively, participants may also choose to enter breakout sessions as they please. In addition, the host can join any breakout room at any time

Table 2. Comparison of Meet, Teams, and Zoom for Learning Features

Assessment variable	Google Meet	Microsoft Teams	Zoom
Preferred for	Online work meetings	Online work meetings	Online teaching & work meetings
Meeting length	300 Hours	24 Hours	30 Hours
Meeting Participants	150	300	100
Unlimited number of meetings	√	√	√
Invite external participants	√	√	√
Screen sharing	√	√	√
Cloud Recording	√	√	√
Virtual background	√	√	√
Join from browser	√	√	√
Native Mobile Apps	√	√	√
Adjustable layouts	√	√	√

 https://doi.org/10.1051/e3sconf/202337105026

Student engagement tracking	√	√	√
Accessibility	√	√	√
White-boarding	√	√	√
Classroom oriented chat	√	√	√
Specialized hybrid learning	√	√	√
In-conference text chat	√	√	√
Event hosting with participant roles	√	√	√
LMS integration		√	√
In-conference private chat			√
Polling			√
Local Recordings			√
Breakout Rooms			√

Source: Datalink Networks. Datalink Networks is a US based premier IT Solutions provider; specialized in business, non-profits, K-12, higher education and government (2021)

Zoom's polling feature allows the teacher to create true/false or multiple-choice polling questions for students. The teacher will be able to launch the poll during the online session and gather the responses from students. If the poll is a graded item, LMS will automatically update all student's grades

The Zoom recording feature allows participants to record their meetings to a cloud-based drive or a local computer. Unfortunately, this feature is unavailable with the other two giants

The in-conference private chat feature allows participants to send private messages to other participants while in a meeting. Private messages between participants are not viewable by the host. Disabling private chat prevents participants from privately messaging other participants but still allows participants and the host to send private messages to each other. Hosts can also disable chat for everyone in the meeting.

2.3 Security Issues

Zoom, Google Meet, and Microsoft Teams are the most popular videoconferencing platforms, and they are examined for their security issues [7]. They have forwarded five observations for security concerns. Firstly, none of those mentioned above video conferencing platforms have open-source code. Secondly, each video conferencing platform has documented its security settings and provided its security policies. Thirdly, these platforms utilized state-of-the-art encryption methods. Fourth, Zoom seems to leave many options for users to customize in terms of security, and some users may overlook these features, which could leave them vulnerable. This could pose more of a problem than it seems. Fifth, Zoom does not encrypt data if stored locally, while the other two platforms encrypt all data at rest by default. Finally, Zoom does not require users to sign in by default when joining a meeting. Meet and Teams both require users to sign in by default and add that extra layer of security to ensure that contact's identities are verifiable. It is easy to conclude that Zoom users are more vulnerable to security issues than the other two platforms, Google Meet and Microsoft Teams [7].

Table 3. A comparative account of Meet, Teams, and Zoom for Security Features [7]

Security Features	Google Meet	Microsoft Teams	Zoom
Encrypted in transit	√	√	√

Encrypted at rest	√	√	
Encryption Feature available	√	√	√
Contacts identities verifiable	√	√	
Required sign in before joining by default	√	√	
Option to require to sign in before joining	√	√	√
Security design properly documented	√	√	√
Code Open source			
Encrypted so the provider cannot read			

Zoom and its users have recently experienced a security crisis named Zoombombing [1]. The phenomenon has emerged in which aggressors join online meetings to disrupt and harass their participants [2-3]. The idea was started as 'online classroom pranks' and swiftly moved to organized disruption efforts, sometimes also used as a tool for harassment and hate speech [4], which the law enforcement agencies have threatened to punish as serious offenses [5].

From an information security point of view, many lessons were learned from this crisis. Firstly, it is becoming increasingly important for companies to incorporate privacy by design[1], and this observation is not restricted to only video conferencing tools. Secondly, the only effective defense against Zoombombing is creating unique join links for each participant [3]. Thirdly, Zoom has underestimated the privacy expectations of its exponentially growing customer base, and they must make details about their privacy practices to the general public who has a growing interest in, and dissatisfaction with, corporate privacy practices [1]. Fourth, most Zoombombing attempts were made by insiders who had legitimate access to the Zoom meetings, particularly students in high school and college classes. The teachers can handle this issue in a class by Zoom features like enabling the waiting room, restricting access to screen share or physical reporting, and ultimate institutional punishments for Zoombombing attackers and their insider supporters. Fifth, this case has given a lesson for end-users as they need to prepare for the challenges and approaches adopted before, during, and after the Zoom meetings [6]. Finally, this situation has taught another lesson of balancing the focus between the default settings for levels of customization versus the level of privacy [5].

2.4 Possible Causes of Zoombombing

High compatibility with other applications and low system requirements: Zoom is a standalone video conferencing platform compared to giant rivals like Microsoft Teams and Google Meet, which integrate other applications and a security layer. On one end, Zoom supports all operating systems, including Apple Mac, Microsoft Windows, and Linux, and supports two major mobile operating systems, including Android and Apple iOS. In addition, Zoom also supports all mainstream browsers, including Google Chrome, Microsoft Edge, Microsoft Internet Explorer, Apple Mac, and Safari. On the other hand, Zoom has relatively low hardware, software, and internet bandwidth requirements for video conferencing. This makes Zoom an ideal target for zoombombing.

Best Video Conferencing Tool for Teaching and Learning: Although videoconferencing platforms have been used as an alternative to classroom teaching, most of them have similar features, except Zoom, which has five unique teaching and learning advantages that make Zoom the preferred choice for educators. These five qualities include Learning Management System (LMS) integration with Zoom, breakout rooms, Zoom meetings, polling, recordings, and in-conference chat. Unfortunately, popularity on campus made

https://doi.org/10.1051/e3sconf/202337105026

Zoom a prime candidate for pranks, and as internet trolling continued, it became organized and vicious.

Zoom's Security Issues: Zoom seems to leave many options for users to customize regarding security, but some ignore these critical security settings, making the meetings unsafe, and this could pose more of a problem than it seems. Zoom does not encrypt data if stored locally, while the other two platforms encrypt all data by default. Finally, there is no requirement to sign in to enter a Zoom meeting, while Teams and Meet require all attendees to sign in, which adds an extra security layer and verifies the identities of the invited members. It is easy to figure out that Zoom users are more vulnerable to security issues than other platforms like Microsoft Teams and Google Meet [7].

2.5 Preventive measures before the Zoom meeting to avoid Zoombombing

Many precautionary measures can be taken while organizing the Zoom meeting to avoid Zoombombing attempts. Making some Zoom settings' OFF' will make Zoom meetings will make safer from zoombombing, including (a) participant video OFF on join, (b) join before host OFF, (c) private chat OFF, (d) allowing removed participants to rejoin OFF. At the same time, making some Zoom settings 'ON' will also prevent Zoombombing occurrences, including (a) requiring a password when scheduling new meetings ON, (b) requiring a password for participants joining by phone ON, (c) mute participants upon entry ON, (d) group chat ON, (e) make co-host ON, (f) allow the host to put the attendee on hold ON, (g) make waiting room ON.

Preventive measures during the Zoom meeting to avoid Zoombombing

Specific measures can be taken during the Zoom meeting session to reduce the Zoombombing menace drastically. These steps would prohibit bombing of business meetings or academic classrooms. Firstly, make the Zoom meeting private when hosting it and distribute passwords or links to join the Zoom meeting/classroom. Secondly, do not publicize the password or meeting links on any website or social media. Thirdly, enable the "waiting room" feature to manually control each participant's entry into the virtual meeting room. Fourth, remove the party-crashers by removing suspected user names. Finally, take control over screen sharing and disable file sharing so nobody can take control of the screen.

3. Conclusion

This paper aims to share Zoombombing: a new phenomenon that emerged during COVID-19, its causes, and measures to prevent Zoombombing. This paper also provides a comparative account of three video conferencing platforms, i.e., Google Meet, Microsoft Teams, and Zoom, as alternative teaching and learning tools during COVID-19. Many lessons were learned during this exercise.

Firstly, all major operating systems (Apple Mac, Microsoft Windows, and Linux), major mobile operating systems (Android and Apple iOS), and all mainstream browsers (Google Chrome, Microsoft Edge, Microsoft Internet Explorer, Apple Mac: Safari) were all supported by all three video conferencing platforms including Google Meet, Microsoft Teams, and Zoom.

Secondly, many teaching and learning features (including inviting external participants, screen sharing, recording, virtual backgrounds, joining from the browser, native mobile apps, flexible layouts, student engagement tracking, accessibility, whiteboarding, classroom-oriented chat, specialized hybrid learning, in-conference text chat, event hosting with participant roles) are standard among all three platforms.

Thirdly, many security features (protection against open source code, well-documented security design, explicitly cover their compliance policies, threat protection, transparency policies, privacy policies, security features, and utilized state-of-the-art encryption methods) are shared among all three video conferencing platforms.

Finally, Zoom has relatively low hardware requirements for video conferencing and teaching features, making Zoom the preferred choice for educators. These teaching features include LMS integration with Zoom, breakout rooms in Zoom meetings, polling, recordings, and in-conference chat. However, Zoom users are more vulnerable to security issues than the other two platforms, Google Meet and Microsoft Teams. Nevertheless, zoom is the highest reviewed conferencing software for educational purposes and an excellent option for a standalone video conferencing solution.

From an information security point of view, many lessons were learned from this crisis. Firstly, it is becoming increasingly important for companies to incorporate privacy by design[1] and this observation is not restricted to only video conferencing tools. Secondly, the only effective defense against Zoombombing is creating unique join links for each participant [3]. Thirdly, Zoom has underestimated the privacy expectations of its exponentially growing customer base, and they must make details about their privacy practices available to the public who has a growing interest in, and dissatisfaction with, corporate privacy practices [1]. Fourth, most Zoombombing attempts were made by insiders who had legitimate access to the Zoom meetings, particularly students in high school and college classes. Teachers can handle this issue in a class by enabling Zoom features like the waiting room, restricting access to screen share or physical reporting, and imposing ultimate institutional punishments for Zoombombing attackers and their insider supporters. Fifth, this case has given a lesson for end-users as they need to prepare for the challenges and approaches adopted before, during, and after Zoom meetings [8]. Finally, this situation has taught another lesson of balancing the focus between the default settings for levels of customization versus the level of privacy [5].

References

1. S. Young, Journal of Business and Technical Communication 35(1) (2021). https://doi.org/10.1177/1050651920959201
2. G. Elmer, S. J. Neville, A. Burton, S. Ward-Kimola, Social Media and Society 7(3) (2021). https://doi.org/10.1177/20563051211035356
3. C.G. Walsh, K.M. Unertl, J.S. Ebert, Academic Medicine, E6-E7 (2021). https://doi.org/10.1097/ACM.0000000000003739
4. L. Nakamura, H. Stiverson, K. Lindsey, Racist Zoombombing (Routledge, New York, 2021) https://doi.org/10.4324/9781003157328
5. I. Secara, Network Security 8 (2020). https://doi.org/10.1016/S1353-4858(20)30094-5.
6. R. Li, J.R. Morelock, D. May, Adv. Eng. Educ. 8, (2020).
7. N.H. Gauthier, M.I. Husain, Silicon Valley Cybersecurity Conference (2020). Springer, Cham.
8. Y. Lan, K.C. Gupta, T. Huang, S. Chelliah, J. M. Spector, Educational Technology and Society 24(1) (2021).