Security and Privacy Issues of Zoom Application in Education System

Akhil Haridas[1], Dhanya Job[2]

[1]U.G.Scholar
Department Of Computer Science
Santhigiri College Of Computer Science, Vazhithala
akhilharidas04@gmail.com

[2]Head Of Department
Department Of Computer Science
Santhigiri College Of Computer Science, Vazhithala
dhanyajob@santhigiricollege.com

Abstract*: Social networking is the process of building and maintaining social relationships. It is the utilization of internet-based social media programs to form connections with friends, family, classmates, customers and clients. In educational technology, social networking refers to the professional or education/pedagogical use of social networking software. About 3 out of each 5 students say that they use social media to debate educational topics if they need access to the web. With much of the planet shifting to performing from home thanks to public health concerns with COVID-19, video conferencing is booming. Businesses, and even colleges and schools, are turning to platforms such as Zoom, Microsoft Teams other technologies to stay connected. Zoom places security because the highest priority within the operations of its suite of products and services. But in recent days, Zoom has come under fire due to security issues with the platform. The topic which I am going to present is about the Security and Privacy issues of Zoom Application in Education System.*

Keywords: Social Networking, Education System, Zoom Application, Security and privacy issues and solutions.

1. Introduction

Social media plays a very important role in the life of every students. It is often easier and more convenient to access information, provide information and communicate through social media. Tutors and students are often connected to every other and may observe use of those platforms for the advantage of their learning and teaching. Social media provides a platform where you'll share your knowledge and gain credibility in your chosen field(s) or specialism(s). It are often very cost effective communication medium and is typically free for the end-user. Since there are many advantages for social media, there also are many disadvantages also. While we employ our social media accounts, there's someone who keeps on spying us and our social media accounts. These are the social media hackers who get into our accounts by getting our account credentials known. Along side this sort of risk, there are more dangers and risks associated with social media.

Information security is extremely important lately to anyone employing a computer or to any organization that employs computers and networking in their day to day operations. Information security is choppy into three major areas, which are called the CIA of data security. These areas are confidentiality, integrity, and availability. Confidentiality deals with ensuring only authorized people have access to the knowledge. Integrity deals with ensuring that the knowledge isn't tampered with or corrupted in any way. and eventually, availability is simply ensuring the knowledge are often accessed and where it's alleged to be. this is often about protecting information in storage, transmission, and processing, using policy, education, and technology, consistent with the McCumber Cube model of data security.

With much of the world shifting to working from home due to public health concerns with COVID-19, video conferencing is booming. Businesses, and even colleges and schools, are turning to platforms such as Zoom, Microsoft Teams other technologies to stay connected. Zoom places security as the highest priority in the operations of its suite of products and services. Zoom strives to continually provide a robust set of security features to protect the data of users. But in recent days, Zoom has come under fire due to security issues with the platform. A zero-day vulnerability has recently been disclosed, and numerous users have noted that Zoom bombers are joining open meetings and sharing undesirable content. Zoom has also been found to overshare data with Facebook via their iOS app, a problem now fixed. Even with their recent troubles, there are many reasons why Zoom is so popular. It’s easy to use, inexpensive, reliable and convenient. When security is paramount, however, using an alternative with a better security history makes sense. The larger concern is the expectation of security with a widely used product. This lulls users into a sense of security when it is not warranted.[1]

2. Zoom and It's Privacy Policies

Figure 1: Zoom app

Zoom is a web-based video conferencing tool with an area, desktop client and a mobile app that permits users to satisfy online, with or without video. Zoom users can prefer to record sessions, collaborate on projects, and share or annotate on one another's screens, all with one easy-to-use platform. Zoom offers a quality audio, video, and a wireless screen-sharing performance across Windows, Mac, Linux, iOS, Android, Blackberry, Zoom Rooms, and H. 323/SIP room systems. Securing Zoom Meetings can start before the event even begins, with a robust set of pre-meeting features like Waiting rooms, Passwords and Join by Domain. Zoom ensure that meetings are secure and disruption free through security options in toolbar and allows to Lock the meeting, Remove participants, Put participant on hold, Disable video, Mute participants etc.

Zoom privacy statements:
This Statement applies to the personal data they process as a data controller, that is, as the party that determines what data to collect and why. We provide some of this data directly, and they get some of it by collecting data about our interactions, use, and experiences with the Services. The data they collect depends on the factors of our interactions with Zoom and the choices we make, and it also includes the products and features we use. They also obtain data about us from third parties.

2.1 Zoom for Government

The following section on Zoom for Government (ZfG) add-on this Privacy Statement.
If we use the ZfG service:

- All data collected about us while using the ZfG service or the ZfG website is stored in the United States of America.
- Our data is only processed by Zoom in accordance with FedRAMP "moderate impact level" control standards.
- The sections in this Statement related to data handling outside the United States do not apply to the personal data collected by Zoom about us in connection with our use of the ZfG service or ZfG website.
- With regard to the Zoom App Marketplace, they do not allow third parties to use any personal data obtained from them for their own purposes, unless it is with your consent.

2.2 Zoom and Children

Zoom does not knowingly allow children under the age of 16 to sign up for their own accounts. Primary and secondary schools or districts register to use Zoom's video communications platform through a "K-12/Primary and Secondary Account."

2.3 Personal data they process

Information they collect when we register for a free Zoom Account, such as:

- Date of birth (for age-verification purposes only**,** Zoom does not retain or use this information for any other purpose**)**
- First Name
- Last Name
- Phone (optional)
- Email
- Language preference
- User IDs and Password (if Single Sign On is not used)
- Profile Picture for avatar (optional)
- Department (optional)
- Meeting schedule

2.4 Customer Content

Customer content is the "in-session" information we give them directly through our use of the Services, such as meeting recordings, files, chat logs, and transcripts, and any other information uploaded while using the Services. Zoom uses customer content only in connection with providing the Services – they do not monitor, sell or use customer content for any other purposes.

2.5 Security

Zoom is committed to protecting our personal data. They use reasonable and appropriate technical and organizational measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

2.6 Sharing of personal data

They only share personal data with companies, organizations or individuals outside of Zoom when one of the following circumstances applies:

- They may share personal data with companies, organizations, individuals outside of Zoom and others when they have consent from an individual (as applicable).
- If Zoom received our personal data from a third-party partner and we become a Customer, Zoom may disclose select personal data to that partner or our designee for the purpose of the partnership agreement.
- They may share personal data with actual or prospective acquirers, representatives and other relevant participants in, or during negotiations of, any sale, merger, acquisition, restructuring, or change on top of things involving all or some of Zoom's

business or assets, including in reference to bankruptcy or similar proceedings.

- They provide personal data to vendors and services providers to assist them provide the Services and for Zoom's business purposes. Examples include public cloud storage vendors, carriers, payment processor, and repair provider for managing customer support tickets.[2]

3. Online Education System Applications

Figure 2: Online Applications

Some of the online education system applications alternative to Zoom are:

3.1 Google Meet

Google Meet (formerly referred to as Hangouts Meet) is a video-communication service developed by Google. it's one among two apps that constitute the replacement for Google Hangouts, the opposite being Google Chat. It's pricing is free.

3.2 Skype

Microsoft's video calling platform which will be used via mobile app through web browsers. it's stream recording, live subtitles, and can also be used for phone calls also . Skype can support up to 50 participants on one video conference. It's pricing is free.

3.3 Webex

Webex is owned by Cisco. It is a standard business platform that gives many of the normal features for video streaming for online meetings, from video conferencing to larger, online events and team whiteboarding. This one could also be a far better fit a faculty department or district event instead of teacher to student interactions. Pricing: Free tier to 100 participants; prices for paid plans range from $13.50 to $26.95/month.

3.4 Microsoft Teams

With Skype integration, Microsoft Teams is beneficial for online teaching. Like Slack, Trello, and other online team-based platforms, Microsoft Teams is way more of a 'teaching platform' (though it's not designed expressly for teachers) than Zoom. It's basically a sort of communication and resource hub that we simply can use to anchor our remote teaching–allowing us to think about using an alternate to Zoom which will have fewer features since we'll be using Microsoft Teams to speak , plan, share, and document, etc.

3.5 YouTube streaming

YouTube streaming is probably going best for individual 'learning channels' that deliver consistent education-based content instead of how for an educator to host a classroom.That said, the latter is feasible with a touch planning if we already use and have extensive content on YouTube.[4]

4. Privacy and Security Issues in Zoom

Figure 3: Security breach in Zoom

The major security and privacy issues while using Zoom application are:

4.1 Zoom Bombing

Zoom Bombing is that allows just anyone easily hack into meetings and show inappropriate content. While the meeting host can remove these users from the meetings, they often come with new accounts. this is often possible because Zoom requires meeting IDs which if call at the open becomes very vulnerable.

4.2 False End-to-End Encryption Claims

Zoom deliberately advertised its end-to-end encryption as a key feature. It means that all communications between us and the other people in our chat would only be visible to those parties; nobody could decrypt them.
The claims were quickly shown to be false. Data was encrypted, but only between us and the Zoom servers.

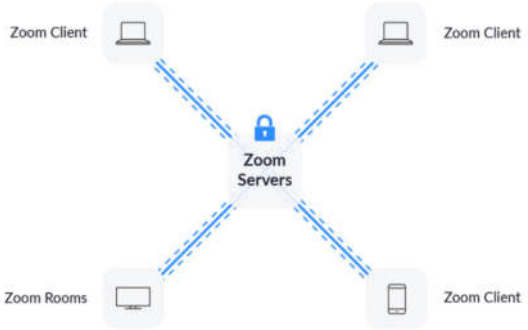

Figure 4: Data transferring in Zoom

4.3 Unsecure Desktop Apps

If we want to use Zoom on a desktop machine, we have two options: the desktop app or the web app. The desktop app is not much secure compare to web apps. Because desktop apps donot get latest security updates.

4.4 Installers with bundled malware

Now a days, Zoom installer has been widely copied and redistributed. Many of these redistributions had malware bundled in with the installer in an effort to trick unsuspecting users.

The most famous example is that the cryptocurrency-mining malware that was found in Zoom installers in April 2020. If installed, it might eat through our CPU and GPU during a bid to mine Bitcoin, leaving us with little free power to try to to anything on our machine.

4.5 Leaked password

While on video-conferencing in Zoom, the other people on Zoom call could theoretically tell what we are typing by watching the movements in our arms and shoulders. All the hacker would need to do is record our call in 1080p and then feed it through a computer program that strips the background. By monitoring our arms and shoulders relative to our head, they would be able to tell exactly what keystrokes we had made.[3]

5. Solutions to Security Issues

These are some of the solutions to the security issues with Zoom:

5.1 Protect your account

A Zoom account is just another account, and in setting up ours, we should apply the basics of account protection. Use a strong and unique password, and protect our account with two-factor authentication, which makes our account harder to hack and better protected, even if our account data leaks .

5.2 Use our work email to register with Zoom

To register with Zoom, use our work e-mail. Sharing our work contact details with our real colleagues is not be a big deal. If we don't have a work e-mail, we can use a burner account with a well-known public domain to keep our personal contact details private.

5.3 Don't fall for fake Zoom apps

Only use Zoom's official website — zoom.us — to download Zoom safely for Mac and PC, and go to the App Store or Google Play for your mobile devices.

5.4 Don't use social media to share conference links

Sometimes we want to host some public events, and in most cases online events are the only type of public events available these days, so Zoom is attracting more and more people. But even if our event is truly open to everyone, we should avoid sharing the link on social media.

5.5 Protect every meeting with a password

Setting up a password for our meeting remains the best means of ensuring that only the people you want in your meeting can attend it. Recently Zoom turned password protection on by default. Don't confuse the meeting password with our Zoom account password. And like meeting links, make sure that meeting passwords never appear on social media or other public channels.

5.6 Enable Waiting Room

Waiting Room makes participants wait during a "waiting room" until the host approves all.that provides us the power to regulate who joins our meeting, albeit someone who wasn't alleged to participate somehow got the password for it. It also allows you to kick an unwanted person out of the meeting and into the lounge. it's recommended to go away this box ticked.

5.7 Pay attention to screen-sharing features

Every normal videoconference app offers screen-sharing - the power of 1 participant to point out their screen to the others and Zoom is not any exception. we will limit screen-sharing ability to the us/host or extend it to everyone on the decision. If we don't need people to point out their screens, we will choose the precise option.

5.8 Don't believe in Zoom's advertised end-to-end encryption

With end-to-end encryption, all communications between us and therefore the refore the people we are calling are encrypted during a way that only us and the people on the decision can decrypt them. All other parties, including the service providers, cannot. It sounds cool, but it's next to impossible, as security researchers have acknowledged. Zoom had to acknowledge that in its case, the opposite end means the Zoom server — that means the video is encrypted, but the Zoom employees and the potentially enforcement agencies, have access to the data. So, we should always keep it in mind and avoid discussing personal or trade secrets on Zoom.[3]

6. Conclusion

With much of the planet shifting to performing from home thanks to public health concerns with COVID-19, video conferencing is booming. Businesses, and even colleges and schools, are turning to platforms like Zoom, Microsoft Teams other technologies to remain connected. Zoom, video communications software has raised some online security concerns these days. The video conferencing channels have certain loopholes in their system that don't encounter unauthorized access and thus the confidential data of teachers and students get compromised. Zoom's security has had tons of holes, although some are fixed over the past few months. Recently, Zoom added two-factor authentication as an account security option, giving users a strong weapon to stay their accounts safe from takeover.[6]

References

[1] www.investopedia.com/terms/s/social-networking.asp
[2] https://zoom.us/privacy
[3] https://usa.kaspersky.com/blog/zoom-security-ten-tips/21374/
[4] https://www.teachthought.com/technology/alternatives-to-zoom-for-online-teaching/
[5] https://www.themobileindian.com/top-5/top-5-zoom-alternatives-for-teachers-30610
[6] https://www.muo.com/is-zoom-safe/

Author Profile

Akhil Haridas pursuing the Bachelor of Computer Application from Santhigiri College of Computer sciences, Vazhithala in 2018-2021.

Dhanya Job received the M.sc. professional degree and Ph.D in Computer Science. Currently working as HOD of Computer Science Department in Santhigiri College of Computer Sciences, Vazhithala.