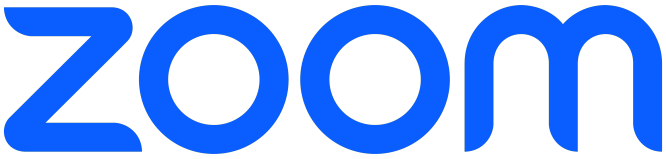
جامعة الملك سعود
King Saud University
كلية علوم الحاسب والمعلومات
قسم هندسة البرمجيات

King Saud University

College of Computer and Information Science

Software Engineering Department

SWE 477 - Software Engineering Code of Ethics



Case Study

Instructor:
Dr. Mashael Aldayel

Prepared By:
Razan Alsaif - 439200624
Khawlah Alghanim - 441201130

ABSTRACT

Coronavirus pandemic forced millions of people to go online for business meetings and learning activities. This has created a huge opportunity for video call conferencing apps. video conferencing platform Zoom founded in 2011 made an exponential increase to 30 times in April 2020, the company counts more than 300 million daily participants in virtual meetings across the world.[4] At this point, new users are completely unaware of the company's privacy practices. Zoom allows employers to share a huge amount of data collected with third parties and has already had a major security vulnerability.

Zoom is a video conferencing platform that enables users to connect online for video conference meetings, webinars, and live chat. It also allows users to create and join virtual meeting rooms where they can communicate with each other through video, and audio. It includes additional features that can give participants the ability to share their screen, share files, chatting service within the meeting group or privately with others in the meeting.

In response to the pandemic, schools and education institutions decided to activate digital tools for remote learning, where zoom became a critical facilitator during the pandemic.

Early in the crisis, many users criticised the video conference company for falling providing sufficient measures to secure its privacy controls.“Zoombombing” was a cause of major concern, as users were exposed to undesired appearance of hackers in the middle of meetings.

Zoombombing is a form of cyberbullying, based on the interception of some calls from unidentified people, who use hateful language and sometimes shared inappropriate and disturbing images.

Researcher Patel demonstrated Zoombombing as “Meeting ID is a relatively short numerical string that can likely be guessed, or brute forced. By constructing an URL to potential meetings, someone can find and join meetings that aren't password protected, even if they weren't invited .As an extra bonus, some people have been posting screenshots from their Zoom meetings that include the ID, so when people find those, they all joins into the open meeting".[6]

This leads to one of the drawbacks of Zoom that is, the default settings don’t require a password to be set for meetings. Additionally, it allows any participants to share their screen. However, Zoom adjusted these default settings for education accounts recently.

Zoom claimed to offer end-to-end encryption but that was controversial as the company also sent user data to Facebook and LinkedIn.

According to a research conducted by Cristóbal Cobo and Pablo Rivera-Vargas [1], they have observed that one of the most common security problems is the vulnerability of Zoom to attacks from various cybercrimes and the vulnerability of user personal.

Zoom refers to two aspects considered relevant for Cobo and Vargas analysis:

• It recognises the collection of a large amount of private information about users: such as name, address, email address, telephone number, position and employer. It acknowledges that the app collects and maintains data about the type of device one uses and IP address, even if the app is used, without creating a Zoom account.

• Zoom verified that it does not sell the personal data of its users to third parties, but that it does share them to benefit the "business" of those companies.

As a result of Zoom vulnerabilities there were multiple damaging impacts related to many aspects mentioned below:

• **Technical**
Zoom lost over 500 million usernames and passwords of their user base. This breach of confidentiality by attackers during virtual meetings caused the leakage of source code, and other highly sensitive information.

• **Financial**
Many organizations banned Zoom as a communications platform, resulting in lowered revenues for monthly subscriptions.

• **Reputational**
Zoom received negative publicity due to the visuals presented, where many organizations have banned Zoom meetings due to the noticeable impact on the general public.

Zoom-bombings disrupt online meetings and classrooms displaying offensive content ,conveying offensive audio messages and posting threats of violence and this violates the following principles:

- Principle 1: Public: Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:
  1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.
  Zoombombing used to disrupt online meetings and classrooms to post threats and display offensive content.
- Principle 2: Client and Employer: Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:
  2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.
  Meeting ID is short and can likely be guessed, or brute forced that caused Zoombombing.
  2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer o another appropriate authority of the ethical concern.
  Zoom shared personal information of users with third parties like facebook and google without the consent of users.

- Principle 4: Judgment: Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate
  4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

Zoom claimed to offer end-to-end encryption but that was controversial.

Zoom reaches $85 million settlement over user privacy and Zoombombing, The Court ruled on Zoom's motion to dismiss, addressing several novel issues raised by the case, including application of Section 230 of the Communication Decency Act and alleged violation of privacy and unfair competition laws in California. Section 230 is a critical protection for online intermediaries, designed to ensure that when online misconduct occurs, courts and local law enforcement do not 'shoot the messenger' by blaming the intermediary instead of the bad actor.

Zoom violated their policy " We do not sell or rent your Personal Data to third parties for any purposes, including marketing. " But they shared it with third parties like facebook and google without the consent of users.

Zoom implemented mitigation strategies to prevent and detect and correct the security issues that it had such as: Implementation of single-use meeting IDs and random meeting pins to minimize attackers replaying previous meeting invites or guessing new meetings, Auditing administrative settings for deletion and inactive account monitoring.

Reference

1- C. C. Romaní and P. Rivera-Vargas, (2022) "*TURN OFF YOUR CAMERA AND TURN ON YOUR PRIVACY A case study about Zoom and digital education in South American countries*", 28-Apr-2022. [Online]. Available: osf.io/preprints/socarxiv/yanzw (Accessed: January 26, 2023).

2- Minhas, S., Hussain, T. and Sajid, K. (2022) *Exploring students online learning: A study of zoom application*, *Research Gate*. Feb-2022 Available at:https://www.researchgate.net/publication/349664179_EXPLORING_STUDENTS_ONLINE_LEARNING_A_STUDY_OF_ZOOM_APPLICATION (Accessed: January 26, 2023).

3- Cohney, S. (2021) *Virtual classrooms and real harms: Remote learning at U.S. universities*, *USENIX*. Available at: https://atc.usenix.org/system/files/soups2021-cohney.pdf (Accessed: January 26, 2023).

4- IQBAL, MANSOOR. (2023) *Zoom revenue and Usage Statistics*, *Business of Apps*. Available at: https://www.businessofapps.com/data/zoom-statistics/ (Accessed: January 26, 2023).

5- Krenz, N. (2022) *An analysis of the 2020 zoom breach*, *CSA*. Available at: https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach/ (Accessed: January 26, 2023).

6- K. Townsend, (2022) "Zoom's Security and Privacy Woes Violated GDPR, Expert Says," SecurityWeek, Apr. 02, 2020. https://www.securityweek.com/zooms-security-and-privacy-woes-violated-gdpr-expert-says/ (accessed Jan. 28, 2023).

7- *Security bulletin* (2023) *Zoom*. Available at: https://explore.zoom.us/en/trust/security/security-bulletin/ (Accessed: January 26, 2023).

8- A. Kumar, "Cotchett, Pitre & McCarthy, LLP and Ahdoot & Wolfson Announce Federal Court Grants Final approval of historic privacy settlement for Zoom App Users nationwide - web hosting: Cloud computing: Datacenter: Domain news," *Web Hosting | Cloud Computing | Datacenter | Domain News*, 22-Apr-2022. [Online]. Available: https://www.dailyhostnews.com/cotchett-pitre-mccarthy-llp-and-ahdoot-wolfson-announce-federal-court-grants-final-approval-of-historic-privacy-settlement-for-zoom-app-users-nationwide. [Accessed: 29-Jan-2023].

9- M. Schruers, "Why State Regulation of online services threatens the internet economy," *Disruptive Competition Project*, 03-Aug-2017. [Online]. Available: https://www.project-disco.org/innovation/080317-state-regulation-section-230-threats-to-internet-econ/. [Accessed: 29-Jan-2023].