Threat Model and Security Policy of Video Conferencing System

Hsin Hua Sung

Threat Model and Security Policy of Video Conferencing System

Introduction

With the changes in people's work and life patterns, the popularity of video conferencing has accelerated dramatically. Video conferencing systems enable real-time, audio and visual communication between two or more parties in different locations. However, the growing popularity of video conferencing has become a target for attackers, making security issues a significant concern. This paper develops a threat model for video conferencing systems, followed by a security policy presented to address specific threats.

Video Conferencing System

1. Structure

The video conferencing system consists of the following components:

(1) Endpoints: Devices used by participants to connect to the video conference, such as computers, laptops, tablets, phones, etc.

(2) Peripheral equipment: Additional devices that enhance the video conferencing experience, such as a webcam, headset, and projector.

(3) Codecs: Devices or software that compress and decompress audio and video data for transmission over the network.

(4) Multipoint Control Unit (MCU): A hardware or software device that bridges multiple endpoints to enable multi-party video conferencing.

(5) Network: The network infrastructure is responsible for transmitting the video and audio signals between the endpoints and the MCU.

(6) Software infrastructure: All the software components that support the video conferencing system, such as servers, databases, management software, and security software.

2. Operation

The operation of the video conferencing system can be divided into two stages (Wickramasinghe, 2021):

(1) Data compression: Endpoint devices capture analogue audiovisual (AV) input data, and the collection of continuous frequency and amplitude waves is converted and compressed into digital data packets by the codec.

(2) Data transfer and decompression: The compressed data packets are sent over the network to the service provider and transmitted to the other participants. When the data packets reach their destination, the codec converts the retrieved data back to the original format.

Threat Modelling

Threat models help understand system security and identify potential vulnerabilities using cost-effective mitigation techniques (Shostack, 2014). Analysing and prioritising identified threats assist in deciding whether to mitigate the threat or accept the risk, balancing security and cost. The threat model of the video conferencing system is established in five aspects as follows.

1. Threats:

   This stage is to identify possible adversaries and conduct attacker-centric analysis. Potential attackers, their motivations and capabilities are evaluated through the threat landscape (Aucsmith, 2003), and the STRIDE model is used to identify potential threats.

   (1) Potential attacks: There are two main sources of threats, internal and external. In the video conferencing system, internal users include participants and hosts of the video conference (end-users), organisation administrator, and system administrator (Hasan & Hasan, 2021). Potential external attackers include hackers, cybercriminals, nation-state actors, competitors, and so on.

   (2) Motivations and capabilities: Potential attackers have various motivations and levels of capability when attempting to control any part of a system. Possible motivations include espionage, financial gain, business rivalry, fun, ideology, and grudge (Hasan & Hasan, 2021). Malicious insiders may abuse privileges for financial motives; their existing legitimate authority allows them to launch attacks without advanced technical expertise. Nation-state actors are motivated by national interest and may have technical capabilities at the expert or specialist level. Cybercriminals and competitors may have capabilities at the hacker or expert level to acquire financial gain. Hackers' motives may involve personal gain, fame, or curiosity, and their technical capabilities range from low to high (Aucsmith, 2003).

   (3) STRIDE: The STRIDE model is proposed by Microsoft to identify and categorise potential threats to a system (Shostack, 2014). According to the STRIDE model, potential threats to the video conferencing system are identified:

   - Spoofing: Attackers may steal data from users' devices or use a fake login screen to steal users' credentials, and impersonate a legitimate user to authenticate to a server.
   - Tampering: Attackers may modify, delete, or tamper with video or audio data, cloud storage, files, and messages to spread false information.
   - Repudiation: Attackers may deny participation or their actions during a conference, causing disputes and confusion.

- Information disclosure: Attackers may intercept confidential content, leaking personal data or device information. Attackers could copy or transfer data to another unauthorised source during a video conference without affecting the original data.
- Denial of service (DoS): Attackers may flood the system with traffic to overload it or send messages that trigger a crash, making the system unavailable to legitimate users. This can be carried out through flood attacks, amplification attacks, or distributed denial of service (DDoS). Attackers could combine multiple sources to attack a meeting system(DDoS), and even participants' devices are infected as part of the botnet.
- Elevation of privilege: Attacks may gain admin privileges to control the system, cause damage, gain unauthorised access, or steal information.

2. Vulnerabilities

This stage is to identify the vulnerabilities within the system which may be targeted by attackers. Attackers may target weaknesses from the following entry points:

(1) Authentication and authorisation mechanisms: Attackers may exploit weaknesses in the access control, such as using stolen credentials or bypassing multi-factor authentication.

(2) Network connections: Insecure network configurations or lack of encryption may be exploited by attackers to intercept, eavesdrop on conversations, or inject malicious data.

(3) Endpoints: Vulnerabilities in the operating system, applications, or firmware of endpoint devices can be exploited to launch attacks.

(4) Peripheral Equipment: The data communication channel between smart peripherals and the host device is vulnerable to attack (Nissim, Yahalom, & Elovici, 2017; Vlajic & Zhou, 2018).

(5) Third-party integrations: The integrations with other applications or services, such as calendars, and messaging platforms, may provide attack vectors.

(6) Cloud storage: Vulnerabilities in the file storage and sharing mechanisms, lack of access controls or encryption may give attackers unauthorised access to confidential data.

(7) Physical infrastructure: Vulnerabilities in servers, routers, or switches can be exploited to launch attacks.

3. Likelihood

The likelihood parameter evaluates the possibility of attacks being launched. The objective approach to estimate likelihood is based on historical data, calculating the occurrence frequency within a certain period. However, data are rarely available and expert opinion is required to assess the likelihood of threats (Othmane et al., 2015). This threat model combines 'the motivation of the potential attacker' and 'the capabilities required to launch the attack' to evaluate the likelihood and divide it into 3 levels, from 1 to 3 representing the likelihood from low to high (Figure 1). More details are shown in Table 1.

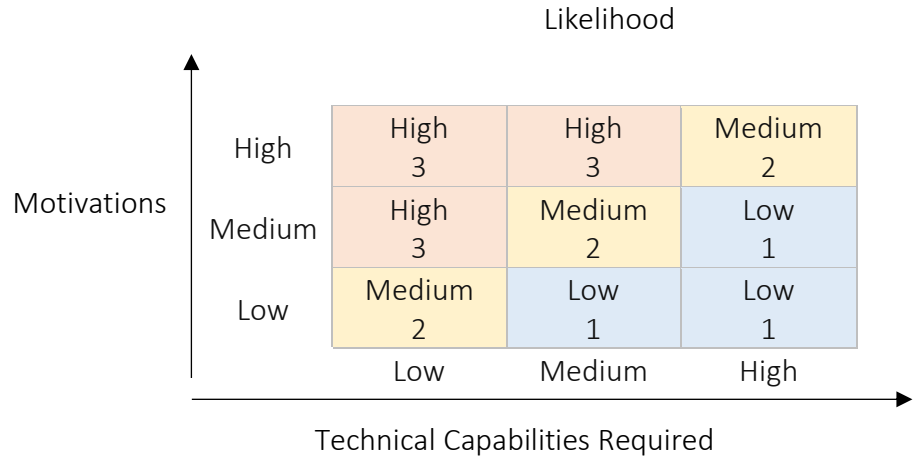

Figure 1 The figure above shows that likelihood is assessed by motivations and capabilities and is divided into three levels.

4. Impact

Impact represents the resulting state of the system after being attacked (Javaid et al., 2012). Attacks may compromise the system's confidentiality, integrity, and availability or endanger organisational assets, including financial, legal, operational, reputation, and privacy (Othmane et al., 2015). As shown in Table 2, the impact of potential threats is measured by the degree of damage and divided into 3 levels, from 1 to 3 representing the impact from low to high. For a given threat, the risk is calculated as the product of impact value and likelihood value (Javaid et al., 2012), combined with a risk matrix to further assess the severity (Figure 2) (Khan et al., 2022).

Table 2 This table shows the criteria (level of damage) by which impact is evaluated and catogorised.

Level of Damage	Impact
• The damage is reversible and repairable.	Low 1
• The attack leads to a short-term loss or interruption of service, or a single or small number of users are affected.	Medium 2
• The attack leads to long-term service loss or interruption, or a large number of users are affected, which may cause illegal or economic losses.	High 3

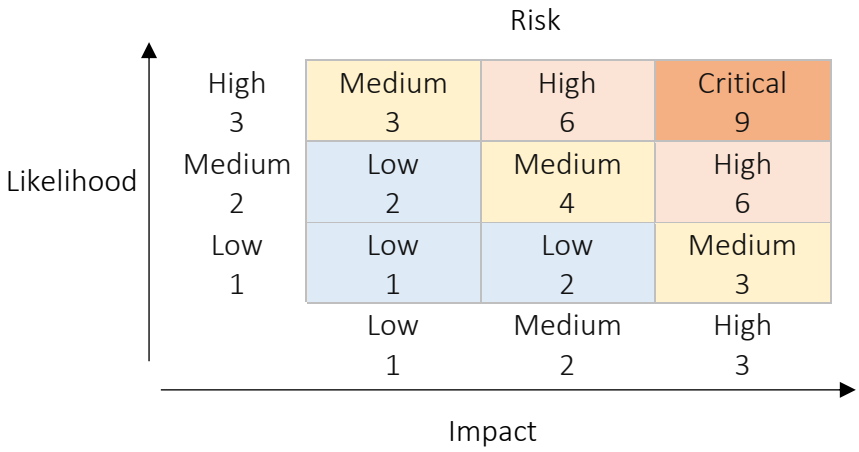

Figure 2 The risk matrix above shows that risk is measured by multiplying likelihood value and impact value.

5. Protection

Based on the above, protective measures for each potential threat are presented in Table 1. With limited resources, the cost should be taken into consideration. The cost, including hardware, software, personnel, training, and maintenance costs, is estimated and divided into 3 levels (low, moderate, and high). When evaluating the cost, the potential impact of the threat should be considered comprehensively, including potential economic losses, data losses, reputation damage, etc. Assessing the cost in conjunction with the potential impact of threats helps to make cost-effective decisions and prioritise protection.

Table 1 Threat model of the video conferencing system.

Threat	Motivations	Capa-bilities	Likeli-hood	Impact	Risk	Protection	Cost
Unauthorised access to meetings (Zoombombing)	Medium • Stealing sensitive information • Disrupting business operations • Causing disruption to meetings or events • Making a political statement	Low	High 3	Medium 2	High 6	• Implement strong authentication and access control measures • Randomly generate meeting IDs • Avoid public sharing of meeting links • Use waiting rooms to screen participants before admitting them to the meeting • Limit screensharing to hosts and speakers	Moderate
Eavesdropping and interception	High • Stealing valuable information • Gaining a competitive advantage • Conducting espionage	High	Medium 2	High 3	High 6	• Use end-to-end encryption to secure audio and video transmissions • Use secure communication protocols like TLS/SSL to protect data in transit • Use Virtual Private Network (VPN) connections to ensure secure remote access	Moderate to High
Tampering with audio-visual data, files, cloud storage	High • Sabotage • Industrial espionage • Financial gain • Political or social agendas • Personal vendettas	High	Medium 2	High 3	High 6	• Implement strong authentication and access control measures • Store data and files in secure and encrypted cloud storage platforms • Use secure file transfer protocols such as SFTP or SCP • Limit access to files and data based on user roles and permissions • Use digital signatures to verify the authenticity of files and data • Use anti-malware software and keep it updated to detect and prevent file-based threats	High

Information disclosure or data leakage	Medium • Stealing personal data • Financial gain • Causing reputational damage to an individual or organisation	Medium	Medium 2	High 3	High 6	• Limit access to sensitive data to authorised personnel only • Use encryption to protect data • Use data loss prevention (DLP) tools to monitor data access and usage • Implement policies and procedures to govern data handling and sharing	Moderate to High
Man-in-the-middle attacks (include specific types of MITM attacks, such as SSL stripping or DNS spoofing)	Medium • Stealing confidential information • Gaining unauthorised access to sensitive data	High	Low 1	High 3	Medium 3	• Use secure communication protocols like TLS/SSL to protect data in transit • Use digital certificates to verify the identity of servers and clients • Use VPN connections to prevent eavesdropping and protect against MITM attacks • Ensure that software and firmware on devices are up to date	High
Malware attacks (software based threats, viruses, trojans, keyloggers, etc.)	High • Stealing confidential information • Gaining unauthorised access • Causing damage to systems or networks • Demand ransom	High	Medium 2	High 3	High 6	• Use updated antivirus and anti-malware software • Use firewalls to block incoming and outgoing traffic from known malicious IP addresses • Implement policies to restrict the installation of unauthorised software • Keep operating systems and software up to date with the latest security patches • Use education and training to help prevent malware infections	Moderate to High

Denial of Service (DoS) attacks	Medium • Causing disruption to business operations • Disrupt video conferencing services • Cause inconvenience and frustration for users • Demand ransom	Medium	Medium 2	Medium 2	Medium 4	• Monitor network traffic and identify and mitigate DoS attacks in real-time • Use firewalls and intrusion prevention systems (IPS) to block DoS traffic • Use rate limiting to prevent excessive traffic from overwhelming servers • Use load balancers to distribute the network traffic evenly and avoid overloading the servers • Use cloud-based services and content delivery networks (CDNs) to handle large amounts of traffic and prevent DoS attacks	High
Phishing attacks	Medium • Stealing personal information • Gaining unauthorised access to sensitive data	Low	High 3	Low 1	Medium 3	• Educate users on how to identify and avoid phishing attacks • Use spam filters and email authentication technologies to block phishing emails • Implement policies and procedures to govern access to sensitive data and systems • Use multi-factor authentication	Low to Moderate
Social engineering attacks	Medium • Stealing confidential information • Gaining unauthorised access • Causing reputational damage to an individual or organisation	Low	High 3	Low 1	Medium 3	• Educate users on how to identify and avoid social engineering tactics • Implement policies and procedures to govern access to sensitive data and systems • Use multi-factor authentication	Low to Moderate

Focusing on ‘Zoombombing’

From the threat model above, high-risk threats are identified, including unauthorised access to meetings, eavesdropping and interception, tempering, information disclosure, and malware attacks. A comprehensive assessment of the severity of potential threats and the cost of preventive measures allowed us to prioritise the threat and focus on zoombombing.

Zoombombing is when uninvited trolls disrupt a video conference with racist, hateful, or pornographic content, leading to interruptions or termination. The FBI received 195 incidents of zoombombing involving child abuse as of May 2020 (Kan, 2020); the UK's National Crime Agency reported more than 120 such cases in the same year (Mee, 2020). Videos and livestreams of zoombombing have circulated on social media, leading to more parodies (Lorenz & Alba, 2020). The Iowa State Senate, Gwinnett County high school, University of Florida, and Alcoholics Anonymous meetings all fell victim to zoombombing (Murphy, 2023; Yu, 2020; Wilson, 2020; Holmes,2020), causing chaos across industries and creating unnecessary panic in society.

1. Security Policy

   To protect the system against the threat of zoombombing, a security policy is presented:

   (1) Access control
   - Use strong authentication mechanisms to ensure only authorised users can access the system, such as multi-factor authentication.
   - Implement a zero-trust approach which requires constant verification of identity for all access attempts.
   - Block the account after certain unsuccessful login attempts.

   (2) Meeting IDs protection
   - Generate random meeting IDs and avoid using personal meeting IDs to host public meetings.
   - Use strong passwords to protect each meeting.
   - Meeting IDs, links and passwords are only provided to those who need to attend the meeting.
   - Avoid sharing meeting IDs or links on social media.

   (3) Meeting configuration

   (a) Enable features
   - Enable the 'waiting room' feature and only authorised attendees are allowed to join the meeting.
   - Enable notifications when participants enter a meeting.
   - Enable the 'lock the meeting' feature once all authorised attendees have joined.

   (b) Restrict features

- Limit screen sharing and annotation tools to hosts and designated presenters only.
- Preset video off and audio mute when attendees enter.
- Use a Zoom Webinar license which only allows attendees limited privileges by default.

(c) Disable features

- Disable file transfer and private chat options.
- Disable the 'Join Before Host' and 'allowing removed participants to rejoin meetings' options.

(4) Secure network

- Use a virtual private network (VPN) to encrypt communication.
- Use secure communication protocols to protect data in transit.

(5) Software update

- Regularly update the software with the latest security patches.

(6) Education training

- Provide users with education on using strong passwords and securing meetings.

(7) Incident response plans

- Design incident response plans to rapidly respond and mitigate the impact of attacks.
- Have a co-host in the meeting prepared to act in case of disruptive behaviours.

2. Design Principles

The following design principles (Saltzer & Schroeder, 1975) are involved:

(1) Least privilege: Only those who need to attend are provided with the link and meeting password; each participant is given the minimum level of privileges necessary to attend the meeting.

(2) Separation of responsibilities: The control of security-sensitive operations is assigned to multiple roles. The co-host is responsible for monitoring the attendee list during the meeting and acting in case of disturbances.

(3) Complete mediation: The access to meetings is tightly controlled and checked for authorisation.

(4) Fail-safe default: Some features are restricted or disabled to minimise the potential damage.

(5) Defense in depth: Multiple layers of security controls are implemented, including pre-meeting configuration, access control, secure network and incident response plans. If one layer fails, there are still other layers of protection in place.

(6) Prudent paranoia: Every participant is assumed to be a potential attacker and needs to go through strict access control, with only limited features available in the meeting. Incident response plans assume the system is always under attack and are prepared for the worst-case scenario.

3. Evaluation of the Policy

(1) Advantages:

- Multiple layers of protection are provided against unauthorised access and disruptive behaviour.
- Technical and non-technical measures are leveraged to ensure secure and private video conferencing sessions.
- Cost-effective, practical, and few changes to existing workflows.

(2) Disadvantages:

- Implementing strict access control measures may result in a complicated process and violate the principle of economy of mechanisms.
- Adjusting default settings may cause inconvenience to users and violate the principle of psychological acceptability.
- Limiting meeting features may not be user-friendly and restrict system functionality.
- Implementing and maintaining security measures may require extra resources, such as co-hosts or a Zoom Webinar license.

References

Wickramasinghe, S. (2021) *How does video conferencing work?*, *Cloud Infrastructure Services*. Available at: https://cloudinfrastructureservices.co.uk/how-does-video-conferencing-work/

Shostack, A. (2014) *Threat modeling: Designing for security*. Crosspoint, IN: John Wiley & Sons, 481.

Aucsmith, D. (2003) "Threat Personas", Microsoft internal document, version 0.9, 2003.

Hasan, R. & Hasan, R. (2021) Towards a Threat Model and Security Analysis of Video Conferencing Systems. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2021, pp. 1-4, doi: 10.1109/CCNC49032.2021.9369505.

Nissim, N., Yahalom, R. and Elovici, Y. (2017) USB-based attacks. *Computers & Security*, *70*, pp.675-688.

Vlajic, N. and Zhou, D. (2018) IoT as a land of opportunity for DDoS hackers. *Computer*, *51*(7), pp.26-34.

ben Othmane, L., Ranchal, R., Fernando, R., Bhargava, B. and Bodden, E. (2015) Incorporating attacker capabilities in risk estimation and mitigation. *Computers & Security*, *51*, pp.41-61.

Javaid, A.Y., Sun, W., Devabhaktuni, V.K. and Alam, M. (2012) November. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 585-590). IEEE.

Khan, R., Barakat, S., AlAbduljabbar, L., AlTayash, Y., AlMussa, N., AlQattan, M., & Jamail, N. S. M. (2022). WhatsApp: Cyber Security Risk Management, Governance and Control. In *2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU)* (pp. 160-165). IEEE.

Kan, M. (2020) *FBI: Disturbing Number of Zoom-Bombings Include Child Porn Images.* Available at: https://uk.pcmag.com/encryption/127054/fbi-disturbing-number-of-zoom-bombings-include-child-porn-images

Mee, E. (2020) *More than 120 'zoombombing' child abuse cases investigated by UK authorities, Sky News.* Available at: https://news.sky.com/story/more-than-120-zoombombing-child-abuse-cases-investigated-by-uk-authorities-11990648

Lorenz T., Alba D. (2020) *"Zoombombing" becomes a dangerous organized effort. The New York Times***.** Available at: https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

Murphy, E. (2023) *Iowa Legislative Hearings Disrupted by Zoombombing***.** Available at: https://www.govtech.com/security/iowa-legislative-hearings-disrupted-by-zoombombing

Yu, J. (2020) *Gwinnett County High School Virtual class gets 'zoom-bombed'*, *FOX 5 Atlanta*. Available at: https://www.fox5atlanta.com/news/gwinnett-county-high-school-virtual-class-gets-zoom-bombed

Wilson, D. (2020) *UF Student Government Meeting 'zoom bombed'*, *Florida Politics - Campaigns & Elections. Lobbying & Government.* Available at: https://floridapolitics.com/archives/326284-uf-student-government-meeting-zoom-bombed/

Holmes, A. (2020) *'Alcohol is soooo good': Trolls are breaking into AA meetings held on Zoom video calls and harassing recovering alcoholics*. Available at: https://www.vrsfreedom365.com/2020/04/06/trolls-are-breaking-into-aa-meetings-held-on-zoom-video-calls-and-harassing-recovering-alcoholics/

Saltzer, J.H. and Schroeder, M.D. (1975) The protection of information in computer systems. Proceedings of the *IEEE*, *63*(9), pp.1278-1308.