Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
CHAPTER 7

Threat model and security analysis of video conferencing systems as a communication paradigm during the COVID-19 pandemic

Raiful Hasan and Ragib Hasan
Department of Computer Science, University of Alabama at Birmingham, Birmingham, AL, United States

1 Introduction

Video conferencing is a live, visual connection between two or more parties regardless of their locations. It is modern technology that has changed our communication paradigm. This technology is widely used in every sector including business, academics, healthcare, social communication, etc. The demands of video conferencing and collaboration tools have increased excessively, especially during the COVID-19 pandemic. All academic institutions, regardless of their size, in the United States and some other countries such as Canada, Australia, the United Kingdom, etc., have moved online during the pandemic. Besides, people are spending more time with friends and families during the lockdown in video conferencing tools. The casual purpose of video conferencing is called a video call or a video chat. Experts predict that the trend will continue in the future, even after the end of the COVID-19 pandemic (Chen et al., 2020; Fatani, 2020). It will not only change our fundamental communication concept, but also cause a permanent shift in how people work. Activity will increase in those video conferencing tools; more activity means more bad actors will look for vulnerabilities and other ways to exploit the system.

The security of video conferencing is becoming a growing issue for companies and various government agencies. The main concern is the fear of unauthorized access to private and confidential data. For that, many Fortune 500 companies have adopted a cautious approach when using video conferencing with their employees. The video conferencing sessions are transmitted using the Internet Protocol (IP) or Integrated Services Digital Network (ISDN) standard (Bocker, 2012; Simpson, 2013). In the IP standard, the
video packets travel over the transmission medium. Intruders can install sniffing tools in the network path (e.g., at the Switch) to read these packets if there is no secure encryption. In ISDN, the transmitted packets switched their formats multiple times throughout the journey from source to destination. Also, the path of the information is uncertain, so this standard cannot provide maximum privacy. Attackers can use some off-the-shelf tools to monitor these packets, such as ISDN line tester tools.

Another security concern of video conferencing technology is the physical location of the provider’s infrastructure. It is important in international and cross-country video conferencing. The ownership of the provider company, the relationship with the government, and the local law also influence security and privacy. Many countries controlled the telecommunication provider and ruled them to have access to the data or intercept the communication channel (Whittaker, 2013; Yang & Xu, 2018). Besides, there are also vulnerabilities in video conferencing equipment, such as network instruments and communication devices. Rival countries often use these instruments to spy on other countries. Recently, the United States passed a bill to replace the equipment made by Huawei\textsuperscript{a} and ZTE\textsuperscript{b} for security concerns (Drezner, 2020).

As a result, the security, privacy, and vulnerabilities of video conferencing tools are an active research area and have gained attention in both academics and industries. There should be a plan to consider all possible threats against video conferencing; otherwise, the system would be vulnerable to cyber-physical attacks. Proper threat modeling helps to analyze the security breaches and system requirements (Mellado, Blanco, Sánchez, & Fernández-Medina, 2010; Myagmar, Lee, & Yurcik, 2005; Scandariato, Wuyts, & Joosen, 2015). Adaptation of threat modeling is important before implementing the video conferencing system because it helps to understand the nature of threats as well as improve the system performance. Threat modeling helps to understand the complexity of the system and identify the possible dangers. The model analyzes all identified threats based on their priority and helps to decide whether it mitigates the threats or accepts the risk.

**Contributions:** The key contributions in this paper are as follows:

1. A complete threat analysis is provided by characterizing threat components (e.g., assets, potential attackers, etc.).

\textsuperscript{a} Huawei—https://www.huawei.com/us/.

\textsuperscript{b} ZTE—https://www.zte.com.cn/global/.
2. The STRIDE threat model is adopted to identify potential attacks and vulnerabilities.
3. We have suggested a mitigation plan to prevent potential threats and vulnerabilities.

**Organization:** The rest of the paper is organized as follows: **Section 2** provides the background of threat modeling and video conferencing technology. **Sections 3 and 4** identify the assets of video conferencing tools and entry points of attackers, respectively. **Section 5** presents the attacker model. **Sections 6 and 7** describe the vulnerabilities and mitigation strategies. The conclusions and future work are presented in **Section 8**.

## 2 Background

### 2.1 Privacy and security in COVID-19

User privacy and data protection have brought concerns during the pandemic. Personal and social programs adopted on video conferencing systems were unprecedented even a few years ago including virtual birthdays, funerals, virtual therapies, etc. Millions of users globally had a similar type of experience when the school went remote, with work and business meetings done on virtual. Actually, people shifted their entire lifestyle online and barely regulated virtual sessions were experiencing cyberattacks, racism, and pornography. Experts suggest that data security and user privacy could be threatened at this time for spending more time online and remote work nature (Uberti, 2020). Users are giving tons of personal data to get things they need. Most importantly, people know very little about the current privacy laws or regulations. One study found that more than 63% of Americans know very little or nothing about their data privacy (Uberti, 2020).

### 2.2 Threat modeling

Threat modeling is a process to understand system security and identify the potential vulnerabilities with a cost-effective mitigation technique for the attacks (Shostack, 2014). This technique is widely used in multiple sectors, including software, applications, distributed systems, business process, etc. Due to the emergence of new technology and tools, it is quite impossible to implement a fully secure system. On the other hand, building and maintaining a secure system is expensive. Authorities have to decide the priority and identify the assets and maintain a balance between security and cost. The priority is determined by the value and potential risk of it. The threat model
consists of five components: (i) Identifying Assets, (ii) Defining the Trust Levels of Users, (iii) Attackers Model, (iv) Identifying Threats, and (v) Mitigation Plan.

2.3 Video conferencing technology

A video conferencing system consists of the following components:

- Endpoints—personal computer, smartphone, telepresence system, etc.
- Peripheral equipment—webcam, headset, projector, etc.
- Video conferencing server—to process the video conference.
- Software infrastructure—content transmission, storage, integration, etc.

There are two video conferencing modes based on the participants: (i) Point-to-Point Video Session and (ii) Multipoint Video Conferencing. A point-to-point video session connects two different users or locations. Multipoint or group video conferencing connects more than two users or sites. A multipoint conferencing unit (MCU) is needed to tie the locations together in the multipoint conferencing mode. The MCU can be embedded on a remote server in the system. The MCU-supported system is called centralized multipoint video conferencing. Some systems are capable of conducting multipoint conferencing without any support from the MCU. This approach can afford better quality due to the absence of any central repository and greater convenience (participants can make ad hoc multipoint calls regardless of MCU availability). This technique is called decentralized multipoint video conferencing. However, it requires increased network bandwidth since every node transmits to every other node directly. Fig. 1 shows the different existing video conferencing techniques.

Fig. 1 Different video conferencing modes (A) point-to-point video conferencing, (B) decentralized multipoint video conferencing, and (C) centralized multipoint video conferencing.
2.4 Growth of video conferencing tools in the COVID-19 era

The COVID-19 pandemic has begun a cultural shift worldwide. The situation has pushed people to stay at home and work remotely. Social distancing, lockdown, and work-from-home policies have moved the regular in-person activity online. Video conferencing apps allow us to keep in touch with our dearest ones and conduct our day-to-day lives in education, business, health, etc. Some countries have even conducted their cabinet meeting via video conferencing during this pandemic, which was uncommon. The COVID-19 pandemic has bolstered the growth rate of these tools. According to Statista, the video conferencing app was downloaded nearly 27 million times in March 2020; the number was 2.1 million in January 2020 (Richter, 2020). Besides, the statistics reported that both the daily active users and meeting participants have increased during that time. For example, Zoom (Zoom Video Communications Inc.) active users increased from 10 million to 200 million in just three months (REUTERS, 2020), whereas Teams (Microsoft) reported that it had surpassed 75 million daily active users (Zaveri, 2020). Over 90,000 schools from 20 countries and 96% of the top US universities used Zoom during the COVID-19 outbreak (Yuan, 2020). However, some governments and organizations banned some third-party video conferencing applications due to security issues. For example, SpaceX and NASA banned Zoom; Standard Chartered has banned both Zoom and Google Hangouts (Jain, 2020).

3 Assets of video conferencing tools

An asset of any system is something valuable or a tangible or intangible entity. Assets are the primary target of the system, and the attackers want to gain access, modify, or destroy. Identifying and measuring the asset is the primary step of threat modeling. The asset must have the business value that should be protected from the attacker. Table 1 shows the asset with the description of the video conferencing tools.

Fig. 2 shows a generic architecture and set of assets of video conferencing tools.

---

Statista—https://www.statista.com.
SpaceX—https://www.spacex.com.
NASA—https://www.nasa.gov.
Standard Chartered—https://www.sc.com/en.
4 Point of entry

Attacks can come from anywhere. It could be internal or external. Attackers target the network, employee software, email, unsecured WiFi, website, even the staff’s mobile to enter the system. Entry points are referred to as target areas where the attackers are able to exploit and gain access. With technological improvement, the points of entry change over time. For example, IoT and smart sensors create a new attack surface, which was

| ID | Asset name | Description |
|----|------------|-------------|
| A1 | End user   | The asset on the user side. |
| A1.1 | User credentials | User login credentials authenticate a user when logging into web/desktop/mobile version. |
| A1.2 | User devices | An end-user device is a personal computer (desktop or laptop), consumer device (smartphone, tablet) |
| A1.3 | Device credentials | End-user device information, such as smartphone IMEI, identification key, etc. |
| A1.4 | Application | An application is a program or group of programs that is designed for the end-user. It is capable of dealing with user inputs (video/audio) and provides the appropriate outputs. |
| A1.5 | Data in application | Sometimes end application stores data related to the users in the local devices. Intruders could grab these data if the device compromised. |
| A1.6 | Peripheral equipment | Peripheral devices add functionality but not essential every time. For example, webcam, microphone, headset, etc. |
| A2 | Conference server | The asset on the server side. |
| A2.1 | Data storage | The data center facility for the purpose of storing, processing, and provide the data. |
| A2.2 | Conference session | Identification of the conference session, such as link, numbers, key, etc. |
| A2.3 | Video, audio data | Contents of the video conference session. However, it can be open if the user makes it public. |
| A2.4 | Log file | Participant’s location, device configuration, time, participant’s number, etc. |
| A3 | Infrastructure | Physical and organizational facilities |
| A3.1 | Service server | Responsible for video processing, content transmission, and integration. |
| A3.2 | Software support | The internal program that is not directly in the application but gives support to run the systems. |

Table 1 Asset and description of the video conferencing tool.
not common in the previous decade. Here are the entry points of the video conferencing system.

### 4.1 Peripheral equipment

Nowadays, smart peripherals such as smart headsets, webcams, etc., are becoming more common in video conferencing. Most of these devices are not secure from cyberattacks (Nissim, Yahalom, & Elovici, 2017; Vlajic & Zhou, 2018). The data communication channel between these devices and the host devices is vulnerable. Besides, cybercriminals can use these devices as access points to get into the network.

### 4.2 Device or application

To attack the participant’s device is the most common way to enter a conference session. Because user devices can be compromised in various ways, the attacker can disrupt the conference call, steal sensitive information such as credentials, call records, etc., and access the private session by malware or phishing attacks.

### 4.3 Conference session

The attackers get into a video conference and make unwanted comments, threatening others, interjecting racism, sharing the malicious link, or making the video unavailable to others. Usually, new and nontechnical users face this type of situation. Sometimes, the attacker coordinates a group attack with a specific session. Though this is not a security flaw, the service provider must take action for the uninterrupted video session.
4.4 Communication medium

The participants of a video conferencing system communicate through the internet with an IP or ISDN standard protocol. Eavesdroppers can exploit these protocols and gain unauthorized access to the communication channel.

4.5 Cloud data storage

The service provider stores the call data in the cloud storage and periodically sends the updates. The attacker could get inside the data center both physically or virtually to launch an attack.

4.6 Application system server

The application server is the heart of the system, and the attacker can launch an attack on it. The server is the most crucial entry point of the conferencing system because previous entries and subsequent attacks only hamper the participants. However, if the attacker gets into the server, then the whole system will be compromised.

5 Attack model

The attack model presents the information that is used to think like an attacker. This section will characterize the user’s accessibility to the system and the attacker’s motives and capabilities.

5.1 Users or potential attacker

Identifying the system users and defining their role is crucial in threat modeling because threats primarily originate from two sources: internal users—who have access authorization, and external agents—who do not have access authorization. Based on accessibility, there are three types of users in video conferencing systems.

5.1.1 Participants

Participants are those who take part in video conferencing and end-users of the system. The host, users with credentials, and users without credentials are the participants. They have access to their own devices and can be an attacker who has a related background, or sometimes a group of participants can organize an attack.
5.1.2 Organization administrator
Organization administrators control all users or part of user’s accessibility of the organization. They can monitor a call within an organization and could access the conference content in the cloud.

5.1.3 System administrator
System admins are responsible for system operation, maintenance, and management. Usually, a group of people do this job and have the highest level of authorization to ensure the correct operation of software and hardware. The super admin, the developer of the system, the database administrator, and other support administrators have admin accessibility. Generally, administrators are very trustworthy; they are highly technical people to attack any part or the whole system.

5.2 Trust levels of system users
Trust levels represent the security rules to the entities of the system. Internal agents are the most trustworthy; however, they are more vulnerable and challenging than external agents because insiders are authorized to access the resources. For example, a super admin has the highest level of privilege to all components of the system; and also has access to all physical entities. If they became an attacker, it would be difficult to prevent the risk. Table 2 shows the trust level of the users.

Table 2 Trust levels of the users of video conferencing system.

| ID  | User                              | Description                                                                 |
|-----|-----------------------------------|-----------------------------------------------------------------------------|
| TL1 | Participants                      | The lowest level of trust; end users and hosts.                              |
| TL1.1| Host                             | Who initiates the conference call and invites the other participants, has access to A1.2 and A1.4. |
| TL1.2| With credentials                | Similar access level of the host, but instead of initiates a new call, they join a call. |
| TL1.3| Without credentials             | Do not have access to A1.4; sometimes can join an invited call.            |
| TL2 | Organization administrator       | Trust level between an individual user and system admin                     |
| TL2.1| Organization IT personnel       | They have authorization for all members of the organization. They can access to A2.3 as well as A1.1, A1.4 for individual users. |
| TL3 | System administrator             | Highest level of trust                                                      |
Table 2  Trust levels of the users of video conferencing system—cont’d

| ID   | User          | Description                                                                                                                                                                                                 |
|------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TL3.1| Developer     | Developers are responsible for creating the applications or systems that run on the computer or another device. Usually, they have access to A3.1 and A3.2. Some developers have T3.4 trust levels. |
| TL3.2| DBA admin     | Database administration (DBA) creates and maintains databases. DBA is a critically important role as they are responsible for database updates, storage, security, and troubleshooting. DBA has authorization on A2.1, A2.2, and A2.3. |
| TL3.3| Support admin | The support admin is responsible for technical issues relating to software implementation, function, and upgrades. They can access A3.1 and A3.2. Sometimes they have superadmin access. |
| TL3.4| Superadmin    | They are responsible for the whole system operation and maintenance. Superadmin has access to all components of the service and system.                                                                        |

5.3 Attacker’s motives
The motivation and goals of attackers depend on the individuals and systems. The primary motivation behind the attack is to access or control any part of the system or assets. Some potential motives are as follows.

5.3.1 Financial gain
Financial gain is the most common motivation behind any attack. According to a study by Verizon, more than 60% of attacks were motivated by financial gain in 2020 (Verizon, 2020). These attacks were launched by private criminals or hired by the rogue nation.

5.3.2 Espionage
Two types of data are targeted for espionage—political movement and national interest. For example, in the COVID-19 era, some renowned research institutions have been attacked by different state-owned groups from other countries (Mehrotra, 2020; Orme, 2020). The attacker’s target was to steal Coronavirus research data.

Verizon—https://www.verizon.com/.
5.3.3 Business rival
Attacks look for secrets that they or their employers can use to dominate in the market. Usually, the same type of organization tries to find security breaches from other companies for a market share. For example, ThyssenKrupp AG\(^h\) (a German steel company) discovered that their trade secret had been compromised by hackers from southeast Asia in 2016 (Auchard & Käckenhoff, 2020).

5.3.4 FIG (Fun, Ideology, Grudge)
The FIG category consists of several other motivations behind the attack, including Fun, Ideology, and Grudge. The most usual tactic of these attacks is to steal credentials and valuable data from the systems. Attackers use web applications, LAN access, or physical access to conduct the attack.

6 Threats and vulnerabilities
6.1 STRIDE threat modeling process
STRIDE is an acronym that stands for six categories of security risks. The STRIDE model is proposed by Microsoft to identify the threats of a system (Shostack, 2014). STRIDE stands for:
- Spoofing—access with a fake identity
- Tampering—modification of data or code
- Repudiation—denying the signature authenticity
- Information disclosure—expose the data to an unauthorized person
- Denial of service—making a service unavailable
- Elevation of privilege—gain control with improper authorization
The STRIDE threat model is developed from a developer’s perspective. While designing security for applications, developers and software engineers must consider security threats early in the Software Development Life Cycle. Table 3 shows the different types of threats and vulnerabilities according to STRIDE threat modeling.

6.2 More attacks and vulnerabilities
In recent years, security experts have been warning about the growing risk and potential impact of cyber–physical attacks on the system. The list of attacks and techniques is increasing rapidly due to technological advancement. The video conferencing system is highly dependent on the physical

\(^h\) ThyssenKrupp—https://www.thyssenkrupp.com.
Table 3 Threats of a video conferencing system in STRIDE threat modeling.

| STRIDE | ID  | Potential threats                                                                 |
|--------|-----|-----------------------------------------------------------------------------------|
| Spoofing | T1.1 | **Participants Identity Theft**: The attacker can steal the credentials from the participants and then use that identity to accomplish a goal. The attacker does not need any special resources for this attack. |
|         | T1.2 | **Source Device Spoofing**: The attacker can steal the user’s device data and pretend to be a legitimate device by performing the authentication to the server. |
|         | T1.3 | **Content Spoofing**: An adversary modifies the video/audio content between participants. Any data can be spoofed, including text messages, files, or communication protocols. |
|         | T1.4 | **Action Spoofing**: The attacker gets inside the system and disguises an action for another one. The user performs this action as a real action and gets attacked. |
| Tampering | T2.1 | **Call Content Tampering**: Conference call transfer through the Internet in data packets, an intruder can intercept these packets and modify them. |
|         | T2.2 | **Cloud Storage Tampering**: The attacker may insert, delete, or manipulate data to the storage. Tampering through the Application Programming Interfaces (APIs) can affect the availability and security of the cloud storage. |
|         | T2.3 | **Log Files Tampering**: Logs tampering attacks involve an attacker gain unauthorized access to the system and injecting, deleting, or otherwise tampering the files. They do that to masking for other malicious activities. |
| Repudiation | T3.1 | **Content Repudiation**: The participants deny or claim not receiving, sending, or editing the data. The attacker can change the authoring information by the malicious program and log the wrong information. |
|         | T3.2 | **Activity Hiding**: The intruders hide the activity after getting inside the system. They try to deny for being convicted in future investigations. |
| Information disclosure | T4.1 | **Participant Information Disclosure**: The attacker may unauthorizedly access the participant’s information such as name, age, location, etc. Later they can use this data or publish publicly. |
|         | T4.2 | **Device Information Disclosure**: Device information, such as device location, device identity, device type, etc. could disclose or can use for further attack. |
|         | T4.3 | **Call Data Disclosure**: The attacker may copy or transmit the data to another unauthorized source, without affecting the original data during the video conferencing. |
server and storage; the telemetry vulnerabilities of the hardware can allow cyber tampering and the interception of data. Table 4 shows some more threats that are not listed in Table 3.

### 7 Mitigation strategies

Several studies have been conducted and proposed to implement a tamper-proof system to protect privacy and security (Chang, Muñoz, & Ramachandran, 2020; Chauhan, Kaur, & Chang, 2020; Correia, Liu, & Xu, 2020; Suciu, Stefanescu, Beceanu, & Ceaparu, 2020). Each threat category has a corresponding set of countermeasure techniques that should be used to reduce risk. Though the appropriate countermeasure depends on the specific attack, we have summarized the mitigation plan in Table 5 for the video conferencing tools.

| STRIDE | ID | Potential threats |
|--------|----|-------------------|
| DOS    | T4.4 | **Application Error Disclosure:** The error or warning messages of the application may expose the crucial and sensitive information of the internal function and architecture. The message may contain the location of the file, cause of the errors, internal calculations, etc. |
| Elevation of privilege | T5.1 | **Denial of Service (DoS):** To make the conferencing unavailable to legitimate users. The attacker accomplishes this by flooding the system with traffic or sending it information that triggers a crash. DoS attack is performed by a single computer to launch the attack. |
| Elevation of privilege | T5.2 | **Distributed Denial of Service (DDoS):** Multiple sources combinedly attack the conferencing system; it is a type of DoS attack. Even the participant’s device can use as a source of an attack. |
| Elevation of privilege | T6.1 | **Unauthorized Admin Privilege:** The attacker tries to obtain crucial privileges by a variety of techniques, such as phishing, brute force, etc. The legitimate owner might not even realize the account has been compromised. |
| Elevation of privilege | T6.2 | **Unauthorized Access:** The superadmin, system admin, and the DBA gain unauthorized access to the participant’s call content, credentials, information, etc. |
| Elevation of privilege | T6.3 | **Privilege Abuse:** The attacker exploits some features reserved for the privileged or administrator user; they make them accessible to those who are not authorized to use them. |
| Attack                | ID   | Potential threats                                                                                           |
|----------------------|------|-------------------------------------------------------------------------------------------------------------|
| Physical             | T7.1 | **Hardware Integrity Attack:** The intruders can exploit the system or install a malicious part on hardware to espionage the conference session (Villasenor, 2011). Most of these attacks are related to firmware. Firmware is a software that comes with the hardware and is stored in ROM or flash memory. |
|                       | T7.2 | **Bypassing Physical Security:** System facilities often used some physical security, such as traditional locks, electronic entry systems, RFID tags for tracking assets, etc. However, these security is not sufficient for the well-planned attacks. |
| Information engineering | T8.1 | **Excavation:** The attacker sends the syntactically invalid or nonstandard request to the system and gathers intelligence about the target by the various responses, such as error response, URL pattern, etc. |
|                       | T8.2 | **Reverse Engineering:** The attacker can target the customer application and reveal the structure, function, and composition of an object by reverse engineering. Nowadays, intruders can launch an attack easily because many reverse engineering tools are available in the market for commercial purposes. |
|                       | T8.3 | **Footprinting:** Adversary learns the information of call sessions, including associated ports, networks, peripherals, etc., through footprinting. Though this is not directly harmful, it may often pave the way for more damaging attacks. |
| Probabilistic         | T9.1 | **Fuzzing:** Fuzzing is a software security and functionality testing method that discover the weakness in the system from the various input. It is a black box technique and totally free from any preconceptions about the system. |
|                       | T9.2 | **Brute Force:** The attacker launches an attack on a trial-and-error basis to gain access to valuable assets and secrets of the systems. The attack exhaustively explores all the possible ways to enter the system. The potential secrets include credentials, encryption keys, database lookup keys, etc. |
Table 5  Mitigation strategies.

| Threat                      | ID                  | Mitigation plan                                                                 |
|-----------------------------|---------------------|---------------------------------------------------------------------------------|
| Spoofing                    | T1.1, T1.2, T1.3, T1.4 | **Encryption:** All credentials must be encrypted by a strong encryption algorithm. It needs to make sure that no one has been able to retrieve the actual credentials in any part of the communication, even the system administrator.  
**Zero-Trust Approach:** The system needs to implement protocols that rely on trust relationships as little as possible. In addition, all connections must be verified through a proper security guideline.  
**Packet Filtering:** All data are transmitted across the network as the packet. The packet filter restricts the suspicious packet with the conflicting source address. It is useful for IP spoofing attacks. |
| Tampering                   | T2.1, T2.2, T2.3    | **Authorization:** The strong authorization has to be implemented that will confirm only the authenticated user can perform a given action on a specific resource.  
**Data Signing and Hashing:** The data signing and hashing will prevent data alteration in communication between the participants and the system. |
| Repudiation                 | T3.1, T3.2          | **Use Digital Signatures:** In data transfer, the system needs to provide nonrepudiation. Digital signatures create one-way hashes that are similar to the checksum function and prevent repudiation.  
**Secure Audit Trails:** All activities have to be logged in and recorded for future auditing. This log will assist in access control monitoring and can provide audit trails when investigating an incident. |
| Information disclosure      | T4.1, T4.2, T4.3, T4.4 | **Avoiding Self-Signed Certificates:** A trusted certificate authority (CA) has to be used for both external and internal communications.  
**Avoid Secrets in Plaintext:** There should be a policy to not store, transmit, and display secrets in plaintext at any point of the communication. |

Continued
| Threat ID | Mitigation plan |
|-----------|----------------|
| T5.1, T5.2 | **Validate and Filter Input:** All incoming traffic has to be validated and automatically filtered out from the malicious automated bot requests. **Throttling Techniques:** Usually, the video conferencing service provider has a large bandwidth. But to prevent DoS or DDoS attacks, it has to implement throttling techniques. Also, some architecture has to perform, including servers in different data centers, data centers in different networks, etc. |
| T6.1, T6.2, T6.3 | **Principle of Least Privilege (POLP):** A security concept to limiting access if they absolutely do not need that. The concept is not only for the users but also for the hardware, systems, process, applications, etc. **Access Control:** Access control is the application of constraints on whom or what can perform attempted actions or access resources that they have requested. There should be proper system-wide access control. Recent research suggests IoT-based self-adapt access control for medical data (Yang, Zheng, Guo, Liu, & Chang, 2019). |
| T7.1, T7.2 | **Foster a Culture of Security:** To defend from the physical attack and secure the hardware, the providers have to adopt awareness within the entire system and employees. **Tamper-Resistant System Design:** There should be security primitives as well as design and architecture-based countermeasures for hardware tampering and counterfeiting. |
| T8.1, T8.2 | **Proper Error Response:** In order to protect the secret, the system has to give a short and proper error response. **Code Obfuscation Techniques:** This is a mechanism for hiding the original code, algorithm, data structure from the unauthorized reverse engineering process. The production software must be obfuscated. |
| T9.1, T9.2 | **Account and IP Lockouts:** There should be a policy to block the account after multiple unsuccessful login attempts. The system needs to block the device and associated IP address. **Comprehensive Fuzz Testing:** The production application has to be tested thoroughly during the development phase to detect any unexpected behavior and ensure the system behaves as per specification. |
8 Conclusion and future work

This paper presents the video conferencing system’s security threat modeling and analysis. The security team of the video conferencing system should address these vulnerabilities and threats during the development cycle. A detailed mitigation plan is also presented; they should apply those mitigation approaches. It would be beneficial for the system administrator to monitor and alert the requirements. In addition, this model can be useful for systems designers, researchers, information security practitioners to identify security threats and vulnerabilities. It will help to develop automated testing tools at the early stages of the systems development life cycle for the video conferencing systems. Due to technological improvements, new security threats and attacks will be introduced in the future. Threat modeling will help to understand and classify these upcoming threats and attacks. We will focus on developing a prototype of the video conferencing system and address all the security concerns mentioned in this paper. Besides, we will analyze new threats and vulnerabilities within this system.

Acknowledgments

This research was supported by the National Science Foundation through awards DGE-1723768, ACI-1642078, CNS-1351038, and ECCS-1952090 and by the National Institutes of Health Grant 1R21HD095270-01.

References

Auchard, E., & Käckenhoff, T. (2020). ThyssenKrupp secrets stolen in ‘massive’ cyber attack. https://www.reuters.com/article/us-thyssenkrupp-cyber-idUSKBN13X0VW (Last accessed 05 May 2021).
Bocker, P. (2012). ISDN the integrated services digital network: Concept, methods, systems. Springer Science & Business Media.
Chang, V., Muñoz, V. M., & Ramachandran, M. (2020). Emerging applications of Internet of things, big data, security, and complexity: Special issue on collaboration opportunity for IoTBDSS and COMPLEXIS. Computing, 102, 1301–1304. https://doi.org/10.1007/s00607-020-00811-y.
Chauhan, R., Kaur, H., & Chang, V. (2020). An Optimized Integrated Framework of Big Data Analytics Managing Security and Privacy in Healthcare Data. Wireless Personal Communications, 117, 87–108. https://doi.org/10.1007/s11277-020-07040-8.
Chen, T., Peng, L., Jing, B., Wu, C., Yang, J., & Cong, G. (2020). The Impact of the COVID-19 Pandemic on User Experience with Online Education Platforms in China. Sustainability, 12, 7329. https://doi.org/10.3390/su12187329.
Correia, A. P., Liu, C., & Xu, F. (2020). Evaluating videoconferencing systems for the quality of the educational experience. Distance Education, 41, 429–452. https://doi.org/10.1080/01587919.2020.1821607.
Drezner, D. (2020). What, exactly, is the Trump administration’s 5G policy? https://www.washingtonpost.com/outlook/2020/02/10/what-exactly-is-trump-administrations-5g-policy/ (Last accessed 05 May 2021).

Fatani, T. H. (2020). Student satisfaction with videoconferencing teaching quality during the covid-19 pandemic. BMC Medical Education, 20, 1–8. https://doi.org/10.1186/s12909-020-02310-2.

Jain, R. (2020). Zoom and Google hangouts banned by large companies and government organizations. https://www.businessinsider.in/tech/news/companies-and-organisations-that-have-banned-zoom-and-google-hangouts/articleshow/75156719.cms (Last accessed 05 May 2021).

Mehrotra, K. (2020). Hackers target California University leading Covid research. https://www.bloomberg.com/news/articles/2020-06-04/hackers-target-california-university-leading-covid-19-research (Last accessed 05 May 2021).

Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. (2010). A systematic review of security requirements engineering. Computer Standards & Interfaces, 32(4), 153–165. https://doi.org/10.1016/j.csi.2010.01.006.

Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Threat modeling as a basis for security requirements. In Symposium on requirements engineering for information security (SREIS) (pp. 1–8). Citeseer.

Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks. Computers & Security, 70, 675–688. https://doi.org/10.1016/j.cose.2017.08.002.

Orme, J. (2020). Successive cyber attacks shut down European super-computers working on Covid-19 research. https://techerati.com/news-hub/successive-cyber-attacks-shut-down-european-supercomputers-working-on-covid-19-research/ (Last accessed 21 May 2021).

REUTERS. (2020). Zoom’s daily active users jumped from 10 million to over 200 million in 3 months. https://venturebeat.com/2020/04/02/zooms-daily-active-users-jumped-from-10-million-to-over-200-million-in-3-months/ (Last accessed 21 May 2021).

Richter, F. (2020). Video chat apps rise to prominence amid pandemic. https://www.statista.com/chart/21268/global-downloads-of-video-chat-apps-amid-covid-19-pandemic/ (Last accessed 05 May 2021).

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft’s threat modeling technique. Requirements Engineering, 20, 163–180. https://doi.org/10.1007/s00766-013-0195-2.

Shostack, A. (2014). Threat Modeling: Designing for security. John Wiley & Sons.

Simpson, W. (2013). Video Over IP: IPTV, Internet Video, H. 264, P2P, Web TV, and Streaming: A complete guide to understanding the technology. Taylor & Francis.

Suciu, G., Stăfănescu, S., Beceanu, C., & Ceaparu, M. (2020). WebRTC role in real-time communication and video conferencing. 1–6.. Global Internet of Things Summit (GIoTS): IEEE.

Uberti, D. (2020). Coronavirus cybersecurity fallout might not be felt for weeks or longer. https://www.wsj.com/articles/coronavirus-cybersecurity-fallout-might-not-be-felt-for-weeks-or-longer-11585128601 (Last accessed 05 May 2021).

Verizon. (2020). 2020 data breach investigations report. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (Last accessed 05 May 2021).

Villasenor, J. D. (2011). Ensuring Hardware Cybersecurity. Center for Technology Innovation at Brookings.

Vlajic, N., & Zhou, D. (2018). IoT as a Land of Opportunity for DDoS Hackers. Computer, 51(7), 26–34. https://doi.org/10.1109/MC.2018.3011046.

Whittaker, Z. (2013). What Google does when a government requests your data. https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/ (Last accessed 05 May 2021).
Yang, F., & Xu, J. (2018). Privacy concerns in China’s smart city campaign: The Deficit of China’s Cybersecurity Law. *Asia & the Pacific Policy Studies, 5*, 533–543. https://doi.org/10.1002/app5.246.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Information Sciences, 479*, 567–592. https://doi.org/10.1016/j.ins.2018.02.005.

Yuan, E. (2020). *A message to our users*. https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ (Last accessed 21 May 2021).

Zaveri, P. (2020). *Microsoft Teams now has 75 million daily active users, adding 31 million in just over a month*. https://www.businessinsider.com/microsoft-teams-hits-75-million-daily-active-users-2020-4 (Last accessed 21 May 2021).