A Study of Video Conferencing Software Risks and Mitigation Strategies

Yelena Arishina
Department of Computer Science
Norfolk State University
Norfolk, Virginia, USA
yaarishina@nsu.edu

Yen-Hung (Frank) Hu
Department of Computer Science
Norfolk State University
Norfolk, Virginia, USA
yhu@nsu.edu

Mary Ann Hoppa
Department of Computer Science
Norfolk State University
Norfolk, Virginia, USA
mahoppa@nsu.edu

Abstract—Due to the recent pandemic, video conferencing platforms – once niche products aimed at limited communities have become a pervasive way of conducting business and sustaining social connections on a global scale. This project explored cybersecurity vulnerabilities and risks faced by these platforms – their data, hardware, and the information exchanged during virtual meetings – and explains some ways these issues can be mitigated. Published research was compiled and analyzed to uncover general risks, vulnerabilities, and security measures. Then, three popular platforms – Zoom, Skype and GoToMeeting were subjected to closer scrutiny. Findings show that platform vendors, business organizations, education institutions, and end users all bear responsibility to train themselves and their constituents on specific cybersecurity steps to enhance video conferencing security. Targeted recommendations are shared, along with some opportunities to build upon this research in the future.

Keywords—cybersecurity, video-teleconferencing, Zoom, Skype, GoToMeeting

I. Introduction

The COVID-19 pandemic has thrust the entire world into new digital ways of conducting business and personal interactions. To comply with mandated social distancing, quarantines, and lockdown orders, individuals and organizations have exchanged traditional face-to-face meetings, conferences, classes and even dates and family gatherings for virtual video conferencing experiences. An initial surge in data and identity thefts along with uninvited virtual meeting "crashers" immediately revealed some obvious security gaps. This has prompted platform vendors and users to reconsider and revamp protocols and best practices for safeguarding information and exchanges.

The importance of securing video conferencing communications cannot be understated. As the transition to virtual conferencing and meetings was underway, the Federal Bureau of Investigation (FBI) recommended cybersecurity measures that focused on due diligence and caution, such as not publicly sharing links to meetings or classroom instruction conferences [1]. In other words, responsibility for safe virtual exchanges stretched to encompass the users themselves, since many – especially vulnerable populations like children and the elderly not only might be unaware of underlying risks, but also lack knowledge of security techniques to avoid them [2].

Regarding employees who were sent home to telework during the pandemic, organizations discovered there were many unanticipated challenges. These included redefining individual roles and responsibilities, the degree of access employees required to do their jobs in new ways, and "the operational competence and psychological balance to work alone" [3]. Furthermore, employers needed to measure how aware employees were about security practices at the time teleworking began. Finally, the safety and convenience of the employee's telework environment and their technological reliability and network security turned out to be critical factors that determined how safe it was for them to handle sensitive company data from the comfort of their telework location. Teleworking employees were tested in ways they never experienced before, especially as many employers rolled out new activity surveillance and productivity monitoring on a digital level [3].

The objective of the research discussed in this paper was to identify known vulnerabilities and risks within video conferencing platforms and to suggest mitigation strategies and prevention tactics for users and security specialists. The recommendations included in this research are suited for employees who were sent home to telework, students and educators who have exchanged their face-to-face classes and activities for a digital modality, and vulnerable populations new to video-conferencing platforms. Furthermore, security specialists working on safeguarding video conferencing communication modalities for businesses and organizations are under tremendous pressure to keep up with the rising variations in methods and new tactics used to compromise and/or to intrude on video conferencing events and meetings. This research provides a brief overview of strategies used to prevent and mitigate these known attack tactics.

The remainder of this paper is organized as follows: Section II introduces background on video conferencing platforms. Section III summarizes related work and recent efforts to provide perspective on the scope and importance of video conferencing security. Section IV explains the research methodology. Section V introduces video conferencing security vulnerabilities and risks. Section VI describes

This work was supported [in part] by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation and workforce development. For more information about CCI, visit cyberinitiative.org.

common security measures in video conferencing platforms. Section VII analyzes selected video conferencing platforms through a cybersecurity lens. Section VIII maps strategies for mitigating vulnerabilities in and risks to the selected video conferencing solutions. Section IX discusses recommendations. Section X concludes the paper with some reflections on overall findings and suggestions for future work to build upon them.

II. Background

Due to recent events and an unprecedented pandemic of global proportions, video conferencing platforms have transformed from being niche products to being the ubiquitous solution to staying connected both professionally and personally. This research aims to highlight various risks and vulnerabilities associated with using video conferencing software and provides mitigation strategies for end-users and security specialists within organizations and businesses. Video conferencing providers experienced an unprecedented surge in usage as the world was hit with the pandemic crisis. Three of the leading platforms – Zoom, Skype, and GoToMeeting [4] - will be discussed in more detail.

A. Zoom Overview

Founded by Erik Yuan in 2011, Zoom provides video and audio conferencing capabilities and online messaging options. Although upgraded versions of Zoom cost a fee (around $15 - $100 annually), the basic version is free and allows up to 100 participants to conference for about 40 minutes at a time. Zoom works on both computers and mobile devices and was built on the idea of ease of accessibility and use for its customers. At the end of 2019, there were about 10 million daily Zoom meeting participants. By March 2020, Zoom was hosting more than 200 million participants a day [5], and revenue skyrocketed to $883 million by the end of that year. In other words, Zoom Communications became one of the market leaders and major beneficiaries of the digital shift kicked off by the global pandemic.

B. Skype Overview

Developed by a group of Estonians, Skype – a well-known veteran of video communications – was released in 2003 and has been bought and sold by various entities such as eBay, Silver Lake, Andreessen Horowitz, the Canada Pension Plan Investment Board, and finally Microsoft in 2011. Skype offers video conferencing, voice calls, online messaging with capabilities of sending videos, photos, and documents. Skype has also experienced an influx of users during the COVID-19 crisis. Experts estimate that in the Spring of 2020, the platform's use increased by nearly 70 percent [6].

C. GoToMeeting Overview

Developed in 2004, GoToMeeting later became a product of Citrix and LogMeIn [7]. This web-hosted software provides services such as online meetings, video conferencing, and desktop sharing on a fee-for-service basis. Already a powerhouse in the video conferencing arena, GoToMeeting's platform usage increased over tenfold in the first few months of 2020 alone due to the pandemic crisis, with mobile downloads up over 600 percent on Android and over 370 percent on iOS [8].

D. Other Popular Video Conferencing Platforms

A few other platforms were beyond the scope of this project but worth mentioning as important players in the video conferencing landscape. One such platform is the FaceTime feature offered to Apple product users. Although it is limited to Apple devices and can support only 30 participants at a time, it has excellent security features and end-to-end encryption technology. TeamViewer and Cisco Web Meetings are high-powered enterprise-scale platforms that also offer great security features, including end-to-end encryption mechanisms and stringent protocols that are needed in tightly regulated industries. These platforms vary in price and may be beyond the means of smaller businesses and organizations [9] [10].

III. Related Works

Researchers in India have been studying the prevalence and importance of video-conferencing platforms within their population during the COVID-19 pandemic, where it has proven to play a vital role in reconstructing high-level human interaction in commercial, business, educational, and governmental segments. Furthermore, these researchers predict that video-conferencing technology will not be deprecated after the pandemic, since it has demonstrated benefits such as reduced travel and facility costs [11].

Researchers Kagan, Alpert, and Fire demonstrated the ease with which an individual's security and privacy could be jeopardized by participating in Zoom meetings. They collected Zoom "gallery" photo collages, observing key personal information (e.g., age, gender, race). Then, they used image processing software, text recognition tools, and social network analysis to cross-reference to publicly available information. In this way, Kagan et al. were able to put together chillingly accurate profiles of meeting participants. Their studies showed how easily information could be harvested from Zoom meetings with the potential to jeopardize individual security and privacy in both online and real worlds [12].

James Lewis, the Senior Vice President and Director for Strategic Technologies Program with the Center for Strategic & International Studies (CSIS), compiled extensive research on the technology risks associated with video conferencing platforms in a December 2020 Executive Summary. With a focus on information theft and espionage, Lewis divided the security risks prevalent with the use of digital meetings and events into six categories: software development risk, loss of personal information, interception of communications, illicit access to stored data, damage to privacy, and the use for influence operations [13].

While hunting for bugs and vulnerabilities within video conferencing platforms in 2018, Kunushevci discovered a vulnerability in Skype that would allow a hacker to access photos, contact information, and open executable links on a user's Android device. What ended up being a code error was

quickly reported to Microsoft and fixed in a software release shortly after its discovery [14].

In 2018, Silvanovich – a Google Project Zero researcher – disclosed she had located critical vulnerabilities in most common video conferencing architecture implementations, including WebRTC (used by Chrome, Safari, Firefox, Facebook Messenger, Signal, and others), PJSIP (used by WhatsApp), and Apple's proprietary library for FaceTime [15]. Silvanovich explained that she used an end-to-end fuzzing technique for locating these vulnerabilities [16] which, if exploited, could let attackers crash apps using the implementation. A simple video call could be used to trigger a memory heap overflow, and thereby allow the attacker to take over the victim's video calling account [15].

IV. Research Methods

Gaining a better understanding of cybersecurity risks inherent in video conferencing and how to mitigate them is an important and relevant research topic. It is beneficial for individuals and organizations to have up-to-date guidance for protecting their private, proprietary, and high-value information assets that are shared or potentially at risk due to using these platforms.

To support arriving at sound recommendations to improve video conferencing cybersecurity for individuals and organizations, the following steps were followed to conduct this research:

- Collect information about video conferencing platforms, general vulnerabilities and risks.
- Describe common security measures in conferencing platforms.
- Choose exemplary platforms based on the availability of platform details and information about past cybersecurity incidents.
- Cite mitigation approaches for the selected conferencing platforms.
- Make recommendations for improving the cybersecurity of these platforms.
- Summarize conclusions and propose remaining areas for further research.

Due to time and resource constraints, this study focused on just three examples (i.e., Zoom, Skype, and GoToMeeting) of the many video conferencing platforms in use today. Similarly, the analysis of vulnerabilities and potential mitigations was conducted "on paper" by collecting information published in research literature, including use-cases and exploits against the selected platforms, as opposed to conducting hands-on experimentation.

V. Video Conferencing Security Vulnerabilities and Risks

No matter which platform is selected for video conferencing, it is vital to be aware of the various security and privacy risks associated with such digital interactions in general. The following paragraphs briefly describe some known threats to secure communication and collaboration via video conferencing platforms that were uncovered during preparatory information gathering for this project.

A. Weak Security Settings

Video conferencing platforms often come with optional security settings that must be turned on manually by users. If defaults are left unchanged, malicious actors familiar with the platform being used may be able to access sensitive information by exploiting resulting vulnerabilities. An example of this is Zoom's new end-to-end encryption feature which is "off" by default; the user has to manually enable it. Furthermore, users of video conferencing platforms often forget to change the default settings – including factory default passwords – for their home Wi-Fi equipment to safeguard their devices and sensitive data while they work outside the security of their employer's firewall [16] [17].

B. Cyberbullying

Cyberbullying has been a problem within the digital realm since the beginning of technological communication platforms and social media. Defined as harassment that takes place in a digital environment, cyberbullying can take on many forms in the video conferencing realm. In most cases, the attacker – known as a "troll" – targets a single individual, whom they follow into different virtual events and meetings to harass or embarrass them. Examples include turning off the target individual's microphone and/or video when they are trying to participate and changing their virtual background to an embarrassing image [18].

C. Zoom Bombing

Zoom Bombing occurs when uninvited individuals join a meeting or a social event taking place through a virtual platform. Despite the moniker, this behavior is not limited to the Zoom platform. Once the attackers are logged in, they disrupt the event by using offensive language, hate speech, and sometimes hijacking screen-sharing capabilities to present obscene and inappropriate images to the participants [18]. Investigations by various entities and the police have revealed that Zoom Bombing campaigns have been organized by large groups of trolls and malicious cybercriminals in order to overwhelm and wreak havoc at virtual events, business meetings, and even governmental functions. United Kingdom police and the National Crime Agency (NCA) are now investigating over 120 cases of Zoom video conferencing events where child abuse photographs were displayed to meeting participants [20].

D. Malware Attacks

Malware refers to a variety of malicious software attacks including viruses, spyware and ransomware. Developed specifically for unauthorized malicious execution on users' devices, malware can be used to collect private data and credentials or to compromise systems as one step in a larger exploit. Video conferencing platforms have experienced a surge in malware attacks, including various zero-days that exploited vulnerabilities in Zoom's default security settings

[12] and malicious links and files inadvertently activated by unsuspecting Skype users [3].

E. Information Leakage

Individuals using video conferencing platforms for work and personal communications do not realize that sharing images such as their real-world (not virtual) background can help hackers identify them, their geographic location, where they work, their hobbies and favorite sports teams, members of their family, and even their circle of friends. A simple family photo or team poster hanging on the wall in someone's background during a meeting can help a malicious actor collect many small details about an individual's life and whereabouts. Such unintentional disclosure of personal facts is referred to as information leakage [12].

F. Information Linkage

Once in the hands of a criminal, many small details about a person's life can be pieced together like a jigsaw puzzle through various online searches, social media accounts, and even facial recognition tools. Malicious actors can match publicly available information about an individual – such as social media profile information, employment, and photos of family, friends, and colleagues – with information leaked through watching them during virtual meetings to develop a profile of that individual with a troubling degree of accuracy. These profiles can include such details as an individual's full name, profession, home address, workplace and location, friends (and details about them), colleagues, hobbies, interests, etc. Furthermore, malicious actors can link the individual to various websites, where they can recover passwords and usernames that may be duplicated by the victim within their place of employment. This so-called information linkage process can provide disturbing amounts of personal and private information about a person, which can be used in social engineering attacks for identity theft, impersonation, or even blackmail [21].

G. Phishing Attacks

Prevalent outside of video conferencing software and applications, phishing attacks have skyrocketed since the beginning of the COVID-19 pandemic. By using social engineering techniques and private information collected through information leakage and linkage as discussed above, malicious actors use the phishing attack method to lure unsuspecting victims to bogus websites created by the malicious actors themselves. These sites are presented as a known third-party or an application familiar to the victim. Once there, users are fooled into clicking on an executable link that infects their system with malware, where it can mine for private and sensitive information. These attacks can also be engaged through a legitimate-looking email containing the executable link [22] [23].

At the start of the pandemic, security professionals saw an alarming rise in the number of fake malicious applications masquerading as legitimate video conferencing applications such as Skype, Zoom, Microsoft Teams, and others. Kaspersky Lab conducted an analysis and discovered thousands of malicious malware and adware packages made to look like and trick people into thinking they were legitimate. Kaspersky found that Skype, Zoom, WebEx, GoToMeeting, Flock, and Slack all were among the platforms being spoofed. Consequently, users were urged to be wary of suspicious advertisements and to go to the vendors' official websites to download any needed applications [24].

H. Data and Information Breach

Unlike information leakage, data and information breaches encompass much greater amounts of private and sensitive information and therefore possess a greater potential to damage the victimized individual or organization. One way this can occur is due to many video conferencing providers – especially large-scale platforms like Zoom, WebEx, and Microsoft Teams –offering cloud-based storage space for users to save not only video and audio recordings of entire meetings but also chat records and information on the attendees of meetings, lectures, and conferences [3]. According to a Washington Post article, early on in the COVID-19 crisis thousands of these cloud recordings were left accessible on the web, including but not limited to: one-on-one therapy sessions, telehealth training calls that included people's names and phone numbers, small-business meetings in which private company financial statements were shared, and elementary school classes, in which children's faces, voices, and personal details were exposed [25]. Such data in the wrong hands obviously could be detrimental to the targeted victims, resulting in personal safety concerns, impacts on reputations, and financial losses.

I. Face Recognition and Fake Avatars (Deepfake)

Developments in facial recognition technology have been instrumental for law enforcement and government agencies in recent decades. The dark side of these incredible tools, of course, is that criminals have been increasingly utilizing these algorithms for personal financial gain and/or to harass individuals, groups, and organizations around the globe. The boom in video conferencing availability and use has exponentially exacerbated the malicious use of facial recognition algorithms. A group of researchers from Ben-Gurion University of the Negev, Israel, conducted a study that used "deep-learning based image processing algorithms to demonstrate that it is possible to identify the same individual's participation at different meetings by simply using either face recognition or other extracted user features. The extracted information about users has the potential to be harmfully used to uncover participants' social networks and other privacy-related factors." If a simple image can provide such factors as full names, gender, approximate age and race, and facial features, one can only deduct that a video recording of a meeting would provide significantly more intel to malicious actors aggregating different sources of such information about targeted individuals, organizations, and businesses [12].

Until recent updates, Zoom was criticized for sending meeting attendees' information, such as email addresses and names, to a data mining company that connected this data to the attendees' LinkedIn profiles, if they had one [26]. Not

only would this have provided malicious actors more opportunities to retrieve personal and professional information on their targets, but it would also allow deeper searches for additional photos and videos of these individuals.

This is so important because both legitimate researchers and criminals have been capitalizing on tools that make it possible to create a fake avatar or map the face of one person onto the video of another – a so-called "deepfake." Companies such as Reface, Snapchat, Wombo.ai, Mug Life, Xpression, and Avatarify have had great success and have gained popularity doing just that. As one example, Avatarify launched in July 2020 and since then has been downloaded millions of times. The founders say that 140 million deepfake videos were created with Avatarify since 2020 alone. There are now 125 million views of videos with the hashtag #avatarify on TikTok [27].

Criminals naturally found new ways to abuse deepfake technology as video conferencing became the norm for most in their everyday exchanges. They could pretend to be a famous individual, CEO, or family member in a virtual meeting, with a goal of embarrassing the real individual by acting inappropriately or even igniting hate and political instability [12]. Table I summarizes the common video conferencing risks discussed above to provide a better understanding of vulnerabilities and potential impacts when platforms are compromised and to act as an organizing construct for the remainder of this report.

TABLE I. VIDEO CONFERENCING VULNERABILITIES AND RISKS

Security Vulnerabilities / Risks	**Damage**
Weak Security Settings: Users do not change key default settings or follow best practices	Leaves platforms and usersopen to other attacks
Cyberbullying: Harassment that takes place during video exchanges	Mental/emotional distress, fear
Zoom Bombing: Disruption of virtual events with offensive language and images via mic and screen-sharing hijacking	Embarrassment to individuals and organizations hosting the event
Malware Attacks: Malicious software used to compromises systems and/or collect private data, credentials, and information	Loss of money and trust; exfiltration of personal and/or proprietary data
Information Leakage: Unintentional disclosure of information during a video conferencing event	Loss of small details of privateinformation
Information Linkage: The aggregation of small details gleaned about targets from leakage and internet mining for later use in more intensive attacks	Loss of privacy; escalation to full-on social engineering attacks
Phishing Attacks: Luring targets to click on executable links to fake websites where additional data is mined from them; to open compromised attachments that launch malware attacks	Loss of private/proprietary data, money and/or reputation,depending on malware type
Data and Information Breaches: Malicious actors gain access to video conferencing recordings stored in the cloudincluding any proprietary informationand files shared during the exchanges	Loss of private/proprietary data; reputation/financial loss; duress and fear if data are used to harass victims
Face Recognition and Face Avatars (Deepfake): Use of facial and/or voice recognition technology to impersonate targets during video or phone exchanges	Embarrass the target; harass others; create chaos, political unrest

VI. COMMON SECURITY MEASURES IN VIDEO CONFERENCING PLATFORMS

Modern video conferencing platforms are not totally unprotected from a cybersecurity standpoint. The following paragraphs detail some general cybersecurity measures that are integrated into many services. However, most of these capabilities require awareness training and for the user or administrator to adjust the security settings that enable them.

A. Using a Secure Connection

Default security settings usually are not optimal; therefore users should opt into more stringent options while setting up their video conferencing user accounts. The risk of malicious actors compromising a connection increases greatly for those who telework outside their employers' firewalls (e.g., from home). Actions such as strengthening default passwords for routers and Wi-Fi networks also are highly recommended. Furthermore, configuring the router to use the WPA2 or WPA3 wireless encryption standard provides an extra layer of security [2].

B. End-to-End Encryption in Video Conferencing Mechanisms

Consumer-based video chatting often deals with day-to-day personal experiences, some of which can be quite private or embarrassing. Business-critical communications frequently center around trade secrets, product and patent details, and personnel records, all of which can have serious legal ramifications if they fall into the wrong hands [17]. For these reasons, it is important to take a closer look at how end-to-end encryption is utilized in the selected video conferencing platform. Blocking third-parties from accessing data packets during transport, along with end-to-end encryption, mitigate exposure of sensitive and confidential data and safeguards the privacy linking sender and recipient. End-to-end encryption is an especially vital cybersecurity

component in government, military, and medical digital exchanges.

C. Other General Security Measures

There are many other potential options offered to better secure video conferencing platforms and sessions. Platforms typically generate a link for use by intended meeting participants. It befalls meeting organizers to control the distribution of said link to ensure it is shared only with authorized meeting participants. A password mechanism also may be offered as part of a multi-stage security protocol. To support meetings aimed at broader public participation, platforms may feature a registration mechanism coupled with a CAPTCHA to help thwart automated penetration. To help weed out potential attackers, "lobbies" are another mechanism that some platforms offered to allow meeting organizers to screen participants prior to admitting them into the meeting. The meeting organizer also may be given blanket powers to enable or disable audio and video for individual or all participants as a means to thwart attacks in real-time.

Further discussion of all security mechanisms is beyond the scope of this report. Additional details can be found in [2] [19] [29]. The bottom line observation is, security measures vary across platforms, and default settings may not be optimal for every situation. In the end, considerable responsibility is placed squarely on users, who must educate themselves on what security measures are potentially available, determine which features are actually available in the platform being used, then activate and put them into practice accordingly.

VII. Selection of Platforms to Investigate

One of the simplest solutions to securing virtual meetings and conferences is using a platform with strong security options already in place. However, in general practice – and particularly during the pandemic – most individuals and organizations likely just start using whichever platform they already have at hand. For this research, a more methodical investigation was done of three popular platforms to better understand the cybersecurity implications of choosing them.

To make the best use of the limited time available to conduct this research, and to include a variety of software and platform types, three notable and widely-used platforms were selected for scrutiny: Zoom Meeting and Skype (free options); and GoToMeeting (fee-based option). The unique features of each platform were inspected. Then, the security features of each platform were considered, along with recommendations for avoiding compromise.

A. Zoom Analysis

It has been interesting to watch Zoom evolve throughout the COVID-19 pandemic to meet the needs of the new video conferencing era. The company has been heavily scrutinized every step of the way by the popular media and came under heavy criticism for its end-to-end encryption (E2EE) claims. At the beginning of the COVID-19 pandemic, Zoom publicly claimed that their meetings were secured with E2EE as long as everyone connected to the meeting using computer audio instead of a cellphone, but a spokesperson later admitted this was not the case. Zoom was actually using Transport Layer Security (TLS) to protect meetings, which provided them the technical ability to access meeting content, including video and audio. Although denied by Zoom officials, there was speculation that these data streams were being mined for targeting advertisements to Zoom users [16].

On October 26, 2020, Zoom released its new version 5.4.0 (58636.1026), which allowed both paid and unpaid users to utilize E2EE with the following restrictions: all meeting participants had to download the Zoom desktop client, mobile application, or Zoom Rooms; and a few features – such as join before host, cloud recording, streaming, live transcription, Breakout Rooms, polling, and meeting reactions– were disabled. However, with the rollout of version 5.5.0 for desktop, mobile, and Zoom Rooms, all features are supported in E2EE meetings. Zoom now also provides the option of using a hybrid cloud service through Zoom Meeting Connector, located internally on the organization's or company's network. According to Zoom, entities utilizing this service will be able to manage meeting metadata in the public cloud while hosting the meetings in their private cloud [30].

When it comes to end-to-end encryption, Zoom now presents the following statement on its Frequently Asked Questions page "Zoom's E2EE offering uses public key cryptography. In short, the keys for each Zoom meeting are generated by participants' machines, not by Zoom's servers. Encrypted data relayed through Zoom's servers is indecipherable by Zoom, since Zoom's servers do not have the necessary decryption key. This key management strategy is similar to that used by most end-to-end encrypted messaging platforms today." Users are notified of E2EE during meetings by a light green shield icon bearing a padlock in the middle.

B. Skype Analysis

Skype has for some time used strong 256-bit encryption. According to Microsoft, Skype exchanges use the Advanced Encryption Standard (AES), also known as Rijndael. This is the same level of encryption used by the U.S. Government to protect sensitive information. User public keys are certified by the Skype server at login using 1536 or 2048-bit RSA certificates [31]. As of July 2021, Microsoft replaced Skype for Business with Microsoft Teams, but will continue extended support until October 14, 2025. With the focus now shifting to Teams, there is some worry that security may relax in the meantime for the soon-to-be obsolete Skype for Business [6]. As mentioned earlier, Microsoft was able to dodge a huge bad publicity bullet early in the pandemic by acting quickly to repair a Skype coding error that otherwise would have allowed multiple hacks. Hopefully that same level of vigilance will continue during Skype's sunset years.

C. GoToMeeting Analysis

Recently, GoToMeeting witnessed a unique vulnerability that allowed multiple Common Weakness Enumerations (CWEs) in PSIRT, a video conferencing tool used by GoToMeeting, thereby exposing its customers to tremendous

risk. Luckily, Swascan – a European security-monitoring firm – stepped in to resolve GoToMeeting's vulnerabilities. GoToMeeting asserts that with its timely actions, it is now nearly impossible for hackers to impersonate genuine users or crash a given program [33].

Citrix GoToMeeting application 5.0.799.1238 for Android contained a vulnerability that logged HTTP requests containing sensitive information about its users, and allowed malicious actors to collect meeting details, authentication tokens, and user IDs. This vulnerability risked exposure of sensitive information to unauthorized actors. GoToMeeting claims to have modified the vulnerability to fix this issue in 2018 [34].

VIII. Mitigating Vulnerabilities and Risks in Selected Video Conferencing

A. Mapping Vulnerabilities to Platforms

Table II shows a quick summary assessment of which platforms examined in this project are subject to the vulnerabilities and risks explored in Section 5. Obviously, despite recent efforts on the part of providers to fix their cybersecurity gaps, much work remains to be done to provide more secure video conferencing options to end users.

TABLE II. Mapping of Vulnerabilities and Risks to Platforms

X indicates platform exhibits vulnerability / risk

Security Vulnerabilities / Risks	**Zoom**	**Skype**	**GoTo Meeting**
Weak Security Settings	X	X	X
Cyberbullying	X	X	X
Zoom Bombing	X	X	
Malware Attacks	X	X	X
Information Leakage	X	X	X
Information Linkage	X	X	X
Phishing Attacks	X	X	X
Data and Information Breaches	X	X	X
Face Recognition andFace Avatars (Deepfake)	X	X	X

B. Mitigations for Typical Vulnerabilities and Risks

Awareness of the risks associated with video conferencing is a common theme in decreasing the likelihood of victimization via a cyberattack in the new virtual exchange modality. From opting into stronger security settings on the platform being utilized, to knowing what to do if a virtual meeting is compromised by an attacker, security training and education are paramount in safeguarding virtual events. Table III summarizes mitigations for the video conferencing security vulnerabilities and risks discussed in this report. The proposed mitigations will benefit all three platforms examined, since in nearly every case, all of them are vulnerable to each cited weakness. These general recommendations and suggestions likewise fall in line with advice from the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

TABLE III. Mitigations for Typical Video Conferencing Vulnerabilities and Risks

Security Vulnerabilities / Risks	**Mitigation**
Weak Security Settings	• Employers provide security training; focuson video conferencing cybersecurity risks while teleworking • User self-education regarding threats and security options/settings in the platforms they use • Extra security guidance and training for vulnerable populations (e.g., children, elderly) [12]
Cyberbullying	• Employers establish anti-bullying / harassment policies, along with disciplinary and grievance processes • Establish employee awareness and management-specific training [18]
Zoom Bombing	• Keep video conferencing apps updatedand patched • Limit screensharing to hosts and speakers[28]
Malware Attacks	• Keep video conferencing apps updatedand patched • Limit file transfer and sharing capabilities during virtual events [28] • Train employees to recognize malware attacks and how to react appropriately [28]
Information Leakage	• Use generic virtual backgrounds and generic pseudo names in video • Avoiding video streaming and public sharing of videos/photos in social media [12]
Information Linkage	• Do not expose meeting details on the web, social media, or blogs • Vary individual virtual backgrounds and pseudonames each time to impede malicious actors from cross-referencing [12]

Phishing Attacks	• Keep video-conferencing apps updatedand patched appropriately • Train employees to recognize phishing attacks and how to react appropriately
Data and Information Breaches	• Save meeting recordings to local storage, not the provider's cloud • Keep video conferencing apps updated and patched appropriately • Limit sharing sensitive date, and only if E2EE is activated end-to-end encrypted (E2EE) is activated [12]

Security Vulnerabilities / Risks	**Mitigation**
Face Recognition andFace Avatars (Deepfake)	• Turn on video only if it is mandated and truly needed to limit image theft • Use anti-facial recognition accessories if available and allowed [12]

IX. Recommendations

The various vulnerabilities and risks discussed in the previous sections were examined in the context of the three selected platforms together with potential targets affected by malicious attacks or compromise. This enabled proposing solutions and mitigations to better security video conferences experiences.

A. Zoom Recommendations

Since initial difficulties at the start of the pandemic, Zoom has repeatedly revamped their security features, investing considerable efforts to attain more stringent protection for their customers. New features like the Waiting Room have proven useful for keeping unwanted intruders out by controlling the admittance of guests by the moderator/host of the meeting [1]. Zoom meetings now can be locked by the host too, further decreasing the risk of anyone gaining unauthorized access and/or hijacking the meeting [19].

Zoom users should familiarize themselves with all the various Zoom settings and security features. They should avoid posting links and meeting IDs on public sites, especially social media platforms such as Facebook and Twitter. Screen sharing also has been a weak point of Zoom meetings, since it enables uninvited individuals to steal or take control of what is presented to the group. To combat this, meeting hosts should configure advanced features on the screen sharing menu so only they can share their screen by default, and to allow others to share on an as-needed basis only [19].

B. Skype Recommendations

Microsoft has been very proactive and, in part, reactive to the risks associated with the pandemic crisis and the influx of Skype users. Their website contains many suggestions for users to keep themselves and their devices safe from fraud, hijacking and other attacks [35].

One of the main risks of using Skype is its vulnerability to transmit viruses. Since it is free and easily acquired by people around the world, viruses and malware often are sent to people via files and attachments within the Skype session. To protect themselves from these threats, users should never download any attachments from individuals they do not recognize. Even if they do recognize the person who sent the file or the attachment, it is always better to double check to ensure that their account was not hacked. Having updated antivirus software is also very important to safeguard the user's computer and/or device from unwanted Skype-borne infections [35].

C. GoToMeeting Recommendations

GoToMeeting also faces the challenges of unwanted intruders crashing meetings. To combat this, the meeting organizer should use the Meeting Lock feature to keep everyone else out of the meeting once all invited attendees have joined [29]. Like Zoom, GoToMeeting also has a Waiting Room feature where individuals trying to join after the meeting has been locked must wait for the host to let them in. This provides the opportunity to ensure those individuals are legitimate and not malicious.

D. General Video Conferencing Security Recommendations

With the sudden surge in video conferencing platform use, malicious actors have zoned in on some easy opportunities to commit both old and new cybercrimes. There is always a risk of someone getting access to a user's password by either guessing it or acquiring it elsewhere. Attackers commonly will try credentials they have stolen from other accounts against high-value accounts such as video conferencing apps, mail providers, and social networks to see if they can get access. To combat this, well-known password guidance applies: use long, strong passwords; do not use the same credentials across multiple accounts; change passwords regularly or immediately if compromise is suspected [31].

Other general recommendations for tightening security of exchanges in this medium include not making virtual classrooms, meetings and conferences public and always requiring a meeting password. Another example is the newly implemented "waiting room" features that are useful for keeping unwanted intruders out [1]. Another easy way to enhance security is to encourage users to adopt the latest versions of the platforms they are using. Similarly, security teams should implement patches as soon as they are released by the vendors. Those who host video conferencing meetings and other virtual events should consider not allowing all participants in these environments to screen share by default. This ability can be provided to each user on an as-needed basis when appropriate to ensure the security of the information exchanged within the meeting [37]. Users also are encouraged by experts to disable the video feature on any call for which video is not essential. If malicious actors hack the meeting, intercepted video and audio potentially can be

used for social engineering attacks in the future, such as deepfake generation as discussed in earlier sections [37]. Meeting hosts should act swiftly if a video event is affected by malicious actions. The host should mute the participants, announce that the event was compromised, then end the meeting. They should report the incident to the organization's security team, the platform vendor, and in some cases, external legal authorities [28].

In addition to the specific recommendations discussed above based upon research findings, additional general recommendations from governing security agencies likewise are applicable. The FBI offers practical information security and physical security guidelines for devices used for video conferencing purposes [1], along with a portal for citizens to report hijackings and threats made by uninvited intruders during virtual meetings [36]. CISA also provides some tips for mitigating security risks and vulnerabilities while using video-conferencing platforms [2].

X. Conclusions & Future Directions

Cybersecurity in video conferencing is a serious matter. This research looked at general vulnerabilities and risks, then took a deeper dive look at three platforms to suggest specific practices that individuals and organizations should adopt to better safeguard their privacy and high-value digital assets. Everyone involved needs to remember that meetings can be recorded surreptitiously by any participant which provides an easy pathway for leaking private and proprietary information [16]. In these unprecedented times, security must be a forethought – not an afterthought – while making the transition to working from home and utilizing video conferencing software to maintain both business and social connections.

Providing the means to safeguard the individuals and organizations involved in meetings and the devices they are using may originate with the platform vendor, but end users of these platforms also must take on their share of responsibility. General recommendations for all users of video conferencing platforms include keeping passwords strong and secured; and never posting meeting links in public venues. Businesses should ensure proper training for their employees. Schools and universities have to safeguard their students, instructors, and staff to ensure smooth operation and less risky behavior. This includes keeping video conferencing software up-to-date and ongoing cybersecurity education.

This research supports the overall observation that – when considering the best ways to secure video conferencing platforms – a balance must be struck between following the guidance suggested by the platform vendors themselves, while also taking into consideration authoritative guidance suggested by governmental agencies and cybersecurity governing bodies. During these trying times, remaining naive about the dangers lurking behind the screen is unwise. Education about risks and vulnerabilities and awareness training for the myriad of tactics used by malicious actors to compromise and abuse social exchanges taking place over video conferencing platforms are vital for not only for working professionals and security teams, but also anyone else using these communication tools.

To keep the scope of this project reasonable, just three representative video conference platforms were selected for closer scrutiny. An obvious option to further this research is to conduct a deeper dive on more platforms to uncover common patterns, differences, and cybersecurity solutions to apply across them. Under controlled conditions, attempts could be made to replicate some of the described attacks – such as bullying and bombing – to recommend better use of existing security settings to prevent them and identify gaps where more built-in security measures are needed.

References

[1] K. Setera, "FBI Warns of Teleconferencing and Online Classroom Hi-jacking During COVID-19 Pandemic," Federal Bureau of Investigation (FBI), Boston, 2020, https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[2] "Guidance for Securing Video Conferencing," Cybersecurity & Infrastructure Security Agency, 2021, https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf

[3] K. Okereafor, M. Philip, "Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic," Research Gate, 8.13-23, Deploying Effective Cybersecurity Education Project, June 2020, https://www.researchgate.net/publication/341895001_Understanding_Cybersecurity_Challenges_of_Telecommuting_and_Video_Conferencing_Applications_in_the_COVID-19_Pandemic

[4] GoToMeeting, https://www.goto.com/meeting

[5] E. S. Yuan, "A Message to Our Users," Zoom Communications – Company News, April 1, 2020, https://blog.zoom.us/a-message-to-our-users/

[6] I. Sherr, "Microsoft's Skype sees massive increase in usage as coronavirus spreads," CNET, March 30, 2020, https://www.cnet.com/news/microsofts-skype-sees-massive-increase-in-usage-as-coronavirus-spreads/

[7] J. Greathouse, "My Mistake Led To LogMeIn Eclipsing GoToMeeting," Forbes, Feb 11, 2017, https://www.forbes.com/sites/johngreathouse/2017/02/11/my-mistake-led-to-logmein-eclipsing-gotomeeting/#7dc5523 21f7d

[8] A. Roy, "GoToMeeting Review: A Well-Deserved Industry Leader," UC Today, June 11, 2020, https://www.uctoday.com/reviews/collaboration_reviews/gotomeeting-review/

[9] J. Evans, "12 Zoom alternatives for secure video collaboration," Computerworld, 2020, https://www.computerworld.com/article/3536471/12-zoom-alternatives-for-secure-video-collaboration.html

[10] "Why use Signal: Share without Insecurity," Signal Webpage, https://signal.org/en/#:~:text=Share%20Without%20Insecurity,no%20one%20else%20can%20either.&text=Every%20message%2C%20every%20call%2C%20every%20time

[11] A. Gupta, "Role of Video-Conferencing Platforms to Change the Face of Communication During the Lockdown," Research Gate, ISBN: 978-1-71695-479-5, August, 2020, https://www.researchgate.net/publication/343921484_ROLE_OF_VIDEO-CONFERENCING_PLATFORMS_TO_CHANGE_THE_FACE_OF_COMMUNICATION_DURING_THE_LOCKDOWN

[12] D. Kagan, G. F. Alpert, and M. Fire, "Zooming Into Video Conferencing Privacy and Security Threats," Cornell University

Department of Computer Science, July 2, 2020, https://arxiv.org/abs/2007.01059

[13] J. Lewis, "Executive Summary: Video Conferencing Technology and Risk," Center for Strategic & International Studies (CSIS), December 3, 2020, https://www.csis.org/analysis/video-conferencing-technology-and-risk

[14] I. Arghire, "Vulnerability in Skype for Android Exposes User Data," January 4, 2019, https://www.securityweek.com/vulnerability-skype-android-exposes-user-data

[15] R. Slavin, "Hacking Video Conferencing Platforms- The Next Big Thing?" Infosecurity Magazine, Opinion, February 4, 2019, https://www.infosecurity-magazine.com/opinions/hacking-video-conferencing/

[16] M. Lee, Y. Grauer, "Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing - The videoconferencing service can access conversations on its platform," The Intercept, March 31, 2020, https://theintercept.com/2020/03/31/zoom-meeting-encryption/

[17] "End-to-End Encryption & How it Works in Video Conferencing," TECH NOTES, WEBRTC, Lifesize, October 10, 2019, https://www.lifesize.com/en/blog/end-to-end-encryption/

[18] K. Churm, "Cyber Bullying in the Workplace During Remote Working," HR Magazine, April 17, 2020, https://www.hrmagazine.co.uk/content/features/cyber-bullying-in-the-workplace-during-remote-working

[19] "How to Keep Uninvited Guests Out of Your Zoom Event," Zoom Blog, March 4, 2021, https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

[20] E. Mee, "More than 120 Cases of Child Abuse Zoombombing in UK Being Investigated," Sky News, May 18, 2020, https://news.sky.com/story/more-than-120-zoombombing-child-abuse-cases-investigated-by-uk-authorities-11990648

[21] M. Lee, "Zoom's Encryption is "Not Suited for Secrets" and has Surprising Links to China, Researchers Discover," The Intercept, April 3 2020, https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/

[22] S. Baskerville, "5 Top Features of Office 365 Advanced Threat Protection," Proserveit, June 16, 2020, https://www.proserveit.com/blog/5-features-office-365-advanced-threat-protection

[23] B. Christensen, "Skype 'Password Successfully Changed' Scam Email," Hoax-Slayer, October 4, 2012, https://www.hoax-slayer.com/skype-password-changed-scam.shtml

[24] T. Seals, "ThreatList: Skype-Themed Apps Hide a Raft of Malware," Threatpost, April 8, 2020, https://threatpost.com/skype-apps-hide-mal ware/154566/

[25] D. Harwell, "Thousands of Zoom Video Calls Left Exposed on Open Web," The Washington Post, April 3, 2020, https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

[26] A. Krolik, N. Singer, "A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles," The New York Times, April 2, 2020, https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html

[27] M. Butcher, "Deepfake Video App Avatarify, which Processes On-Phone, Plans Digital Watermark for Videos," Tech Crunch, April 14, 2021, https://techcrunch.com/2021/04/14/deep-fake-video-app-avatarify-which-process-on-phone-plans-digital-watermark-for-videos/

[28] D. Bisson. "Video Conferencing Security Tips You May Have Overlooked." Security Intelligence, July 8, 2020, https://securityintelligence.com/articles/best-practices-securing-video-conferencing-apps/

[29] L. Craffort, "5 Best Practices for Secure Video Conferencing with GoToMeeting," GoToMeeting Blog, March 27, 2020, https://blog.gotomeeting.com/5-best-practices-staying-secure-gotomeeting/

[30] "Meeting Connector Core Concepts," Zoom Help Center, https://support.zoom.us/hc/en-us/articles/201363113-Meeting-Connector-Core-Concepts

[31] "Does Skype Use Encryption?" Microsoft, 2021, https://support.skype.com/en/faq/fa31/does-skype-use-encryption

[32] I. Arghire, "Vulnerability in Skype for Android Exposes User Data," January 4, 2019, https://www.securityweek.com/vulnerability-skype-android-exposes-user-data

[33] E. Hess, "Is Secure Video Conferencing Achievable? How To Improve Security for Your Video Conferencing App," Helical Inc., March 31, 2020, https://helical-inc.com/blog/is-secure-video-conferencing-achievable-how-to-improve-security-for-your-video-conferencing-app/

[34] "National Vulnerability Database," 2014/2018, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, https://nvd.nist.gov/vuln/detail/CVE-2014-1664

[35] "Protecting your online safety, security and privacy," Microsoft, 2020, https://support.skype.com/en/faq/FA34649/protecting-your-online-safety-security-and-privacy

[36] Federal Bureau of Investigation Internet Crime Complaint Center, https://www.ic3.gov/

[37] K. Shaw, "Do's and don'ts of video conferencing security," Computerworld, 2020, https://www.computerworld.com/article/3535924/do-s-and-don-ts-of-videoconferencing-security.html