Using Biometrics to Fortify E-learning Platforms Security

Spyros Kopsidas, University of Thessaly, Greece
Eleni Ioannou-Sougleridi, University of Thessaly, Greece
Dimitris Zisiadis, University of Thessaly, Greece
George Stamoulis, University of Thessaly, Greece

The Paris Conference on Education 2023
Official Conference Proceedings

Abstract
E-learning is here to stay. During the COVID-19 pandemic, more than 1.2 billion students were educated through online learning. Platforms such as Zoom, Webex, Skype, Microsoft Teams, Google Meet, etc. were among the most popular ones during that period. However, these platforms suffer from various vulnerabilities that make them susceptible to cyberattacks, including Man-in-the-Middle attacks (MitM), during which the communication between a student and a teacher is intercepted by a ghost user. In this study, we propose the implementation of VIPSec, a secure and elaborate protocol, that is also easy to use for young and inexperienced users such as children. Thus, online learning sessions could be secured from disruptors and the threefold of confidentiality, integrity, and availability of the sensitive nature of personal data of both students and educators is respected.

Keywords: E-learning, Security, VIPSec, Education, MitM, Zoombombing

iafor
The International Academic Forum
www.iafor.org

1. Introduction

The COVID-19 pandemic has brought upon dramatic changes in education. The digitalization of education that has been happening in the last years, became more prominent as the majority of students worldwide were affected by the pandemic. During the pandemic, more than 1.2 billion students in 186 countries were out of the classroom due to school closures [1]. As a result, many educational institutions had to adopt online learning methods to continue their teaching and learning activities. Teleconferencing platforms such as Zoom, Webex, Skype, Microsoft Teams, Google Meet, VooV Meeting, and Blackboard Collaborative Ultra were among the most popular ones in downloads during the COVID-19 pandemic [2]. These platforms enabled synchronous e-learning, which is a form of online learning where learners and instructors interact in real-time through audio, video or chat features [3]. Synchronous e-learning is different from asynchronous e-learning, which is self-paced and does not require simultaneous participation [4].

One of the most widely used teleconferencing platforms during the pandemic was Zoom. Zoom is a cloud-based video conferencing service that allows users to virtually meet with others, either by video or audio-only or both, while conducting live chats [5]. In 2020, it emerged as one of the most popular mobile apps globally with more than 500 million downloads [6]. Zoom was especially popular among educators and students, as it offered free accounts for schools and universities with unlimited meeting time and up to 100 participants per session [7]. Another teleconferencing platform that was extensively utilized for educational purposes was Cisco Webex. Webex is a suite of software products that provides video conferencing, online meetings, screen sharing, and collaboration tools [8]. Webex was widely utilized as the exclusive officially authorized software for such purposes in Greece [9]. Webex also offered free accounts for educators and students with unlimited meeting time and up to 100 participants per session [10].

These e-learning platforms are heterogeneous environments with different web-enabled applications. E-learning is a structured course or learning experience that is delivered electronically [11]. E-learning can be delivered through various media, such as web pages, audio files, video files, animations, simulations, games, and virtual worlds. The use of e-learning is not only cost-effective and cost-efficient but more importantly it removes the geographical obstacles often associated with traditional classrooms. Worldwide e-learning revenue is expected to grow to $325 billion by 2025 [12].

2. Synchronous Learning Security Risks

This sudden and unplanned influx of people using teleconferencing platforms has brought into light the insufficient existence of a normative and legislative base on e-learning and digital learning resources in general. Security is the Achilles heel of educational platforms. Since e-learning relies on the Internet for its execution [13], it entails additional security and privacy issues [14]. The weakness in design implementation, operation, or internal control could be exploitable by cybercriminals, who often target schools, where cybersecurity is not a priority. The greater number of current e-learning systems do not sufficiently meet fundamental security requirements [15]. As a consequence, some serious security incidents have taken place, such as Zoombombing.

Zoombombing, a term that was popularized in 2020, is associated with and derived from the Zoom video conferencing software program, but it also applies to other video conferencing

platforms [16]. Zoombombing is a form of cyberattack where an uninvited person joins a Zoom meeting and disrupts it by sharing inappropriate or offensive content, such as pornography, hate speech, or violence. Zoombombing has caused significant issues for schools and educators due to the minimal security implemented in teleconferencing platforms. Some organizations have even banned the use of Zoom altogether due to security concerns [17]. Zoombombing can be prevented by using some security features available on teleconferencing platforms, such as password protection, waiting rooms, host controls, and encryption [18].

The security issues of e-learning have been brought to light due to its exponential growth and its dependency upon the Internet [19]. Password-protected online classrooms are not secure since session hackers usually target browser or web application sessions, and meeting disruptors search the Internet frequently for publicly posted meeting IDs, that are being shared carelessly or the use of the same meeting link more than once. These security issues have made parents skeptical towards online learning platforms. Since 2018 there is a General Data Protection Regulation (GDPR) being applied in the EU that focuses on the protection of data privacy. Educational e-platforms should comply with the GDPR regulation. In 2021, Zoom was found to be violating the GDPR by the Data Protection regulatory agency in Hamburg, Germany, since it was transmitting data collected in the EU to the United States [6]. Children's data are sensitive and require to be secured from disruptors, as their interception might lead to phenomena such as cyberbullying, which affects the general well-being of a student. In addition, there is also the issue of copyright and ownership of the authors of educational content. When disruptors access digital content without authorization, they can make unauthorized use of it, and have a financial interest in authors' lecture notes [20].

Modern-day e-learning systems can often be connected with the user's social media accounts in several ways. Most of the online platforms offer the Social Login option that allows users to log in using their social media credentials such as Facebook or Google. Some online learning platforms have social sharing buttons integrated, allowing thus users to share their progress, achievements, or course content on their social media profiles. However, this poses an additional risk for students, because someone who penetrates into the online learning system, may be able to identify the young students, through their social media accounts. It is therefore vital to secure the digital classroom from the prying eyes of disruptors.

Online learning should rely on trust. Most young students tend to trust all sources of information and accept them as true [21]. Therefore, the importance of the content is fundamental, and it should be protected against unauthorized modifications. This trust can be built by having secure educational platforms [20].

Security issues are caused by users' poor knowledge of security measures, improper behaviors, and lack of education [22]. It is difficult for children to evaluate the risks posed to information, to appreciate security priorities, and to take responsibility for the implementation of controls. Therefore, security is critical for the protection of learners and teachers from unauthorized threats. Security refers to protection from malicious or accidental misuse of resources [23] [24]. In cybersecurity, threats are potential negative actions or events that may result in unauthorized information disclosure, theft, or damage to hardware, software, or data [25]. Threats include [26]:

- Data tampering: altering or modifying data without authorization.
- Network eavesdropping: intercepting or listening to network traffic.
- Unauthorized access to administration interfaces: gaining access to system settings or functions that are restricted.
- Disclosure of confidential data: revealing sensitive or personal information to unauthorized parties.
- Attacker exploits an application without a trace: exploiting vulnerability in an application without leaving any evidence.
- Man-in-the-Middle attacks (MitM attacks): intercepting and modifying network communication between two parties.
- Poor key generation or key management caused by weak encryption: using weak cryptographic algorithms or keys that can be easily broken or compromised.

3. Man-in-the-Middle Attack

Man-in-the-Middle (MitM) attack A Man-in-the-Middle (MitM) attack, one of the oldest forms of cyberattacks, is a cyberattack in which the communication between two parties is intercepted [27]. MitM attacks include:

- Session hijacking: taking over an active session between a user and a server.
- Replay attack: capturing and retransmitting data at a later time.
- IP spoofing: forging an IP address to impersonate another party.
- Eavesdropping attack: listening to network traffic without modifying it.
- Bluetooth attacks: exploiting vulnerabilities in Bluetooth devices or protocols.

During a typical MitM attack in an educational platform, the communication between a student and a teacher is intercepted. The disruptor then sends fake information to each party, i.e., by modifying an online quiz or exam, impersonating the teacher, or redirecting the student to a phishing website to steal their login credentials.

Project Zero, a team at Google, has discovered a way for cyber attackers to compel a victim to connect to a MitM server without any user intervention, thereby enabling the attacker to intercept and alter client update requests and responses. This allows them to send a malicious update to the victim, automatically downloading and executing, giving the attacker remote code execution (RCE) capabilities. Project Zero has stated that the only prerequisite for executing this attack is the ability to send messages to the target through Zoom chat [28].

Regarding Cisco Webex, multiple vulnerabilities have been reported, that could allow an authenticated, local attacker to gain access to sensitive information [29]. Disruptors can take advantage of these vulnerabilities by intercepting traffic between the affected user and an endpoint using MITM techniques and then impersonating the endpoint with a forged certificate. Depending on the configuration of the endpoint, an attacker could access call controls, modify presented content or view presented content modify any content being presented by the victim or have access to call controls. Successful exploits also allow the disruptors to gain access to sensitive information, including meeting data and recorded meeting transcriptions.

It is important to take precautionary measures to prevent MitM attacks before they occur, since they can be prevented or detected by authentication and tamper detection. The most

effective way to do so is encryption. Encryption is one of the techniques used for confidentiality, in order to ensure that information and data are not disclosed to any unauthorized person or entity [30]. Weak encryption mechanisms allow a disruptor to brute force his way into a network and begin MitM attacking. All cryptographic systems are secure against MitM attacks, through the use of mutual authentication. Mutual authentication is a process in which both parties verify each other's identity before exchanging data [31]. Mutual authentication can be achieved by using digital certificates, public key cryptography, or shared secrets [32].

4. Enhancing E-learning Security With VIPSec

A novel method called Voice Interactive Personalized Security (VIPSec) [33] [34] has been proposed. VIPSec is a method for enhancing the security of synchronous e-learning systems by using biometric-based authentication and voice verification. VIPSec is especially suitable for use in multi-party teleconferencing systems, as it offers several benefits over other security methods, such as:

Easiness of Use: VIPSec does not require the users to remember or enter any passwords or PINs. The users only need to speak to authenticate themselves and verify their peers. This makes it convenient and user-friendly for the participants, as they do not have to deal with complex or cumbersome authentication procedures. VIPSec also does not require any additional hardware or software installation. The users only need a device with a microphone, which is a common feature of most laptops, tablets, and smartphones. This makes it compatible and accessible for the participants, as they do not have to acquire or install any special equipment or software.

Device Independence: VIPSec does not depend on any specific device or platform. The users can use any device that supports voice communication and has a secure channel to exchange the token. This makes it flexible and adaptable for the participants, as they can use their preferred or available device to join the session. VIPSec also does not store any user data or keys on the device, so the users do not have to worry about losing or compromising their device. This makes it secure and resilient for the participants, as they do not have to risk exposing their data or keys to attackers.

Strong Encryption: VIPSec provides end-to-end encryption of the session data using a secret key derived from the token. The secret key is unique for each session and each pair of peers. The secret key is also based on user-specific biometric features, which are hard to forge or copy. The secret key is never transmitted over the network, so it cannot be intercepted or stolen by attackers. This makes it robust and reliable for the participants, as they can ensure the confidentiality and integrity of their data during the session.

Scalability and Deployability: VIPSec only requires minimal resources from the user devices and no additional support from the network. VIPSec does not rely on a central bridge circuit to mix and distribute the speech signals of the participants. Instead, each participant receives and decrypts the speech signals of all the other participants and mixes them locally on their device. This eliminates the security weakness of having a central bridge that works with clear speech and cipher keys for all of the participants. VIPSec also does not rely on a public key infrastructure (PKI), which can be costly and complex to maintain and secure. VIPSec can be easily integrated with existing synchronous e-learning systems without affecting their performance or functionality. This makes it scalable and deployable for the

participants, as they can use it with any number of peers and any existing system without any additional overhead or hassle.

Consequently, VIPSec can be a useful method for enhancing the security of LMSs, as it can address some of the common security challenges that LMSs face, such as:

Account Breaches: LMSs store sensitive information about learners, instructors, courses, and assessments. If an attacker gains access to a user account, they can steal or tamper with this information, or impersonate a legitimate user. VIPSec can prevent account breaches by using biometric-based authentication and voice verification. VIPSec does not require passwords or PINs, which can be forgotten, stolen, or guessed. Instead, VIPSec uses the user's voice or face as a unique identifier that is hard to forge or copy. VIPSec also uses liveness detection to ensure that the user is alive and present at the time of authentication, and not using a recorded or synthesized voice sample.

Data Interception: LMSs transmit data over the network, such as voice, video, text, and files. If an attacker intercepts this data, they can eavesdrop on the communication, or modify or delete the data. VIPSec can prevent data interception by using end-to-end encryption of the session data using a secret key derived from the token. The secret key is unique for each session and each pair of peers. The secret key is never transmitted over the network, so it cannot be intercepted or stolen by attackers. VIPSec also does not rely on a public key infrastructure (PKI), which can be vulnerable to man-in-the-middle attacks or other compromises.

Denial-of-Service Attacks: LMSs depend on the availability and performance of the network and the servers to deliver the learning content and services. If an attacker launches a denial-of-service attack, they can overload the network or the servers with malicious traffic, causing them to slow down or crash. This can disrupt the learning process, affect the user experience, or damage the system. VIPSec can prevent denial-of-service attacks by using a challenge/signature token to establish the session. The token is a random string of characters that is encrypted with a user-specific key derived from their biometric features, such as voice. The token is then sent to the other peer through a secure channel. The token acts as a filter that blocks any unauthorized or malicious requests from reaching the network or the servers. VIPSec also uses voice verification to confirm the integrity of the token and the identity of the peers. VIPSec can ensure the availability and performance of the LMS by preventing unauthorized or malicious traffic from accessing the system.

5. Conclusions

VIPSec is a valuable security technology that can help to enhance the security of synchronous e-learning systems. VIPSec can help to prevent Zoombombing, protect user data, improve user experience, and foster a more secure learning environment. As a result, VIPSec is a valuable security tool that can help to make synchronous e-learning systems more secure and user-friendly.

In addition to the benefits mentioned above, VIPSec can also help to:

Foster a More Secure Learning Environment. By making it more difficult for unauthorized users to join synchronous e-learning sessions, VIPSec can help to create a more secure learning environment for students and teachers.

Reduce the Risk of Data Breaches. By protecting user data from unauthorized access, VIPSec can help to reduce the risk of data breaches. This is especially important for organizations that collect sensitive data about their employees or students.

Improve Compliance With Data Privacy Regulations. By using VIPSec to protect user data, organizations can help to demonstrate compliance with data privacy regulations such as GDPR and CCPA.

Overall, VIPSec is a valuable security technology that can help to enhance the security of synchronous e-learning systems. VIPSec can help to prevent Zoombombing, protect user data, improve user experience, and foster a more secure learning environment. As a result, VIPSec is a valuable security tool that can help to make synchronous e-learning systems more secure, more user-friendly, and of course, more reliable, and trustworthy for online education and collaboration.

References

[1] OECD (2021). *The State of School Education: One Year into the COVID Pandemic*, OECD Publishing, Paris.

[2] Trueman C. (2020). *Pandemic leads to surge in video conferencing app downloads. Needham*, Computerworld.

[3] Synchronous learning. (2023, March 10). In *Wikipedia.* https://en.wikipedia.org/wiki/Synchronous_learning

[4] Mayadas, F (March 1997*). "Asynchronous learning networks: a Sloan Foundation perspective"*, Journal of Asynchronous Learning Networks, vol. 1(1).

[5] Zoom Video Communications (2023, July 24). *In Wikipedia. https://en.wikipedia.org/wiki/Zoom_Video_Communications*

[6] Zoom (software) (2023, July 24). *In Wikipedia.* https://en.wikipedia.org/wiki/Zoom_(software)

[7] Zoom. (2023). *COVID-19 Support.* Retrieved July 27, 2023 from https://zoom.us/docs/en-us/covid19.html

[8] Cisco. *About Us*. https://www.cisco.com/c/en/us/about.html

[9] Cisco Webex. (2023, March 23). In *Wikipedia*. https://en.wikipedia.org/wiki/Cisco_Webex

[10] Webex, *Essentials: Education Overview*, Essentials | Education Overview, Retrieved July 27, 2023 from https://www.webex.com/webexremoteedu.html

[11] Nichols, M. (2008*). E-Learning in context*. E-Primer Series, vol. 2869(1), pp. 1-2.

[12] Tamm, S. (2023, January 11). *What is the Definition of E-Learning?*. E-student. https://e-student.org/what-is-e-learning/

[13] Alwi, N.H.M., Fan, I.S. (2010). *E-Learning and Information Security Management*. International Journal of Digital Society (IJDS), vol. 1, pp. 148-156.

[14] Neal, L. (2003). *Expectations of Privacy: Data Collected In Class Should Not Be Misused*, e-Learn, vol. 2003(9), Art. No. 1.

[15] Moneo J.M., Caballe S., Pneot J. (2012). *Security in Learning Management Systems*, eLearning Papers, Catalonia, Spain, Retrieved from www.elearningpapers.eu

[16] Zoombombing (2023, July 17). *In Wikipedia.* https://en.wikipedia.org/wiki/Zoombombing

[17] Wakefield, J. (2020, April 2). *Zoom boss apologises for security issues and promises fixes.* https://www.bbc.com/news/technology-52133349

[18] PCMAG. *How to Prevent Zoom-Bombing.* Retrieved 2023, July 27 from https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing

[19] Alwi, N. H. M., Fan, I. S. (2010*). Threats analysis for e-learning, International Journal of Technologically Enhanced Learning*, vol. 2(4), pp. 358371.

[20] Weippl, E. R. (2005). *Security in e-learning*, Springer publication.

[21] Graham, L., Metaxas, P. T. (2003). *Of Course It's True, I Saw it on the Internet, Critical Thinking in the Internet Era*, Communications of the ACM, vol. 46(5), pp. 70-75.

[22] Adams, A., Blandford, A. (2003). *Security and online learning: To protect or prohibit. Usability Evaluation of Online Learning Programs*, Ghaoui, Claude ed. Usability Evaluation of Online Learning Programs. UK: IDEA Publishing, pp. 331–359.

[23] Hina, S., Dominic D.D. (2016). *Information security policies: investigation of compliance in universities*, 2016 3rd International Conference on Computer and Information Sciences (ICCOINS). Piscataway: IEEE, pp. 564-569.

[24] Neumann, P. G. (1994*). Computer related risks*. Addison-Wesley Professional.

[25] Computer security (2023, July 24). In *Wikipedia.* https://en.wikipedia.org/wiki/Computer_security

[26] Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., Munikan, A. (2003). *Improving Web Application Security: Threats and Countermeasures*, Microsoft Press.

[27] Man-in-the-middle attack (2023, July 25). In *Wikipedia.* https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[28] Seals, T. (2022, May 25). Zero-Click Zoom Bug Allows Code Execution Just By Sending a Message, *DARK Reading*. https://www.darkreading.com/application-security/zero-click-zoom-bug-allows-remote-code-execution-by-sending-a-message

[29] Cisco Security Advisory (2021, July 15). *Cisco Intelligent Proximity SSL Certificate Validation Vulnerability*. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-proximity-ssl-cert-gBBu3RB

[30] Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, ISBN 978-1-119—09672-6.

[31] Mutual authentication (2023, June 14). In *Wikipedia.* https://en.wikipedia.org/wiki/Mutual_authentication

[32] *Improving Web Application Security: Threats and Countermeasures*, 1st Edition, Microsoft Press, (2003). ISBN: 0735618429.

[33] Kopsidas, S. et al, *Voice Interactive Personalized Security Protocol: Definition and Security Analysis*, IEEE Conference Publication, IEEE Xplore https://ieeexplore.ieee.org/document/4371621/

[34] Kopsidas, S. et al*, Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification*, IEEE Conference Publication, IEEE Xplore https://ieeexplore.ieee.org/document/4178383/

Contact email: spyros@uth.gr