Security Considerations in a Mobile Learning Environment

Michael Sletten
Department of Education Policy, Organization and Leadership
University of Illinois, Urbana-Champaign 1
310 South Sixth Street Champaign IL 61820
USA
{authorof01@gmail.com}

ABSTRACT: *In 2021, education using a mobile phone has become an immensely popular means of delivering and accessing learning content. Learners and instructors have become unbound from their desktop and laptop machines and now enjoy the portability and ubiquitous nature of mobile phones in their educational endeavors. Within the mobile learning platforms, there are five elements that are involved—the user, the mobile device, the wireless network, the learning management system, and the computer network(s) that host the wireless networks and/(or) the learning management system. Each of these five areas are susceptible to security threats and therefore must be hardened to become more resilient to attacks.*

Keywords: Mobile Security, Mobile Learning, Network Security

Received: 19 January 2021, Revised 15 February 2021, Accepted 20 February 2021

DOI: 10.6025/isej/2020/7/2/58-63

1. Introduction

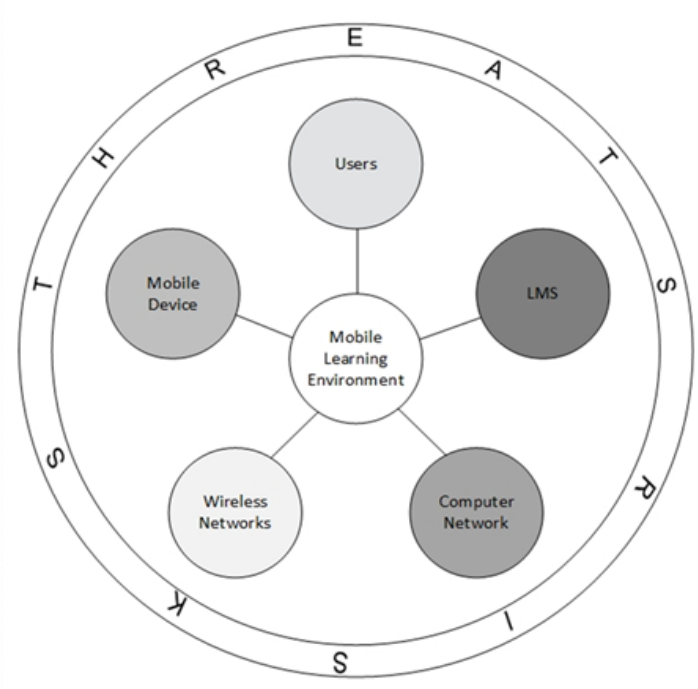
Since the beginning of face-to-face learning until now in 2021, there have been many changes in how education takes place. In 2001, the first experiments involving mobile phone usage in a learning environment came from a research group at Stanford who were trying to "fill in gaps of time–to create a bubble of learning that you carry with you but may only access for periods of 30 seconds or 10 minutes at a time." (Brown, 2001, p. 1). This research, along with technological developments of mobile phones, has created an environment in which learners and instructors can now access educational content via their mobile phone ubiquitously, provided that they have access to the Internet. The Mobile Learning has been widely adopted across U.S. in the year 2020. (ReportLinker, 2020), which is an immense amount of growth within a twenty-year period. This has all occurred since the Stanford researchers first explored the potential of the mobile phone for learning purposes.

Within the mobile learning environment, there are five specific areas: the learner, the mobile phone, the wireless network, the learning management system, and the computer network(s) that host the wireless network *and/(or)* the learning management system. Each of these five areas present security challenges that can affect areas such as encryption of data (at rest, in flight, in process), mobile device health and physical security, wireless and computer network security, and securing learning management systems. This includes the protection of all user data, course data, and information. The work will explore the five

elements of a mobile learning environment and discuss each one while providing recommendations and potential solutions for each element.

2. The Five Elements In A Mobile Learning Environment

It is important to show the five elements in a mobile learning environment because they help illustrate distinct components within the that mobile environment. Each of these must be differently addressed from a security standpoint. The five elements are illustrated in the diagram below.



Adapted from "The Five Elements of a Mobile Learning Environment" (Sletten, 2020, p. 55)

As illustrated above, each of these five elements are connected to the central point called the mobile learning environment. The mobile learning environment continues to be surrounded by risks and threats which present themselves in diverse ways and means.

The user element includes the students, instructors, and any other personnel (i.e., administrators, instructional designers, learning management administrators, etc.) who are involved in the mobile learning environment. Users are an incredibly important part of the mobile learning platform and one of the most difficult elements to secure, as it is challenging to control everything a user can and cannot do on their phone. Security measures can be configured on the device to limit or control functionality. User security awareness training may be required for users, but there still exists a level of autonomy that the user can exercise which opens up potential security issues.

Mobile devices, such as a mobile phone, have become an increasingly popular means of delivering and accessing online learning content. Technological developments in electronics have created miniaturized electronic components found in mobile phones along with the ability to connect to the Internet wirelessly. This has made using a mobile phone quite desirable for instructors and learners. Without this level of portability and connectivity, the ubiquitous nature of mobile learning would not be possible. However, "mobile devices are vulnerable to the common security threats such as thief (sic) of the devices, infections via applications, misappropriation of data, interception of communication, Bluetooth intrusions, viruses, payment fraud, automatic data transmission and tracing" (Ismail, 2016, p. 4). Overall, it is these dangers that present risks and vulnerabilities that must be addressed to ensure a more secure mobile device and mobile learning environment.

Wireless networks such as cellular wireless connections or hosted Wi-Fi on a computer network are the primary means by which mobile phone users connect to the Internet. In either case, it is of utmost importance to ensure that connection to these networks is secured and encrypted. As noted by Friedman & Hoffman, "there are several methods hackers can use to intercept wireless communications between laptops, handheld devices, cell phones and other mobile devices." (Friedman & Hoffman, 2008, p. 173). These methods include the use of free, legally obtainable software such as Wireshark, which enables the collection of wireless and wired data transmissions. If encryption standards such as SSL/TLS as well as a virtual private network (VPN) are not being used for the connection, then the data transmissions can be potentially exposed to anyone with the means and motivation to eavesdrop on a user's session. It is also important to ensure that the Wi-Fi access points are correctly installed and secured, considering various physical and configuration settings such as disabling Wi-Fi Protected Setup (WPS), installing the Wi-Fi access points at an elevated level from the ground, and using MAC address filtering. There are additional considerations when securing a Wi-Fi network which will be addressed later in this paper.

The learning management system must also address security as it holds a large amount of data from students, faculty, and other personnel. This information can fall under the protection of FERPA or PII laws at a state or Federal level, reinforcing the need for having a secure learning management system. No learning management system is perfect. For example, in 2019, it was reported that eighteen-year-old Bill Demirkapi broke into Blackboard's Community Engagement Software:

"Demirkapi found a series of common web bugs in Blackboard's Community Engagement software and Follett's Student Information System, including so-called SQL-injection and cross-site-scripting vulnerabilities. For Blackboard, those bugs ultimately allowed access to a database that contained 24 categories of data, everything from phone numbers to discipline records, bus routes, and attendance records—though not every school seemed to store data in every field." (Greenberg, 2019).

SQL-injection and cross-site-scripting are dangerous vulnerabilities for any customer using web-based interface; especially those that allow for the user to access secure data and/or stores secure data that may be legally protected. Learning management systems store this data in databases and they must be encrypted and backed up. This requires a regular backup schedule via a virtual private network connection during data backup and recovery processes.

Computer networks that host Wi-Fi networks and/or learning management systems need to be secured in a mobile learning environment. Computer networks present multiple attack surfaces and opportunities for security violations to take place in the hardware, software, and infrastructure. If Wi-Fi networks are not properly configured on a separate network, such as a virtual local area network (VLAN), then the computer network can be exposed to an attack if the Wi-Fi network is compromised. When a computer network is hosting a learning management system, it is critical that all the data is encrypted and backed up on a regular schedule using secure channel communications via a virtual private network connection.

Risks and threats in any of the Five Elements of a Mobile Learning Environment will never be 100% be eliminated, mitigated, or patched. Only through supporting a level of constant vigilance and diligence about security, can there be hope of supporting security within the mobile learning environment.

3. Recommendations

In the world of security, there is a concept known as the CIA triad which stands for Confidentiality, Integrity, and Availability. The first, Confidentiality, "is a necessary component of privacy and refers to our ability to protect our data from those who are not authorized to view it." (Andress, 2014, p. 6). The second, Integrity, "refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner. This means the unauthorized change or deletion of our data or portions of our data, or it could mean an authorized, but undesirable, change or deletion of our data." (Andress, 2014, p. 6). Lastly, Availability, "refers to the ability to access our data when we need it." (Andress, 2014, p. 7). The following recommendations all relate back to the CIA triad.

The user is one of the more challenging areas to secure. This is because there is a level of autonomy that each user enjoys when on their device. A user can access many different resources and places on the Internet, some of which may be unsavory or unadvised. Going to one of these types of locations on the Internet could result in those websites or resources installing something on the user's mobile phone (malware, virus, etc.) and/or collecting data from them that was unauthorized.

One of the best ways to help users become more aware of their mobile phone usage and increase their level of understanding is to provide all users in a mobile learning environment with security awareness training on a regular basis. As noted by Wilson & Hash, "Users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities." (Wilson & Hash, 2003, p. 5), which makes user training crucial. Security awareness training could be delivered and accessed through a mobile device. Topics that might be included in this training could include how to use anti-malware and antivirus software on their mobile phone, email phishing/spam frauds, and how to best secure their data including making regular backups. Frequency of training should be anywhere from one to four times per year, due to the ever-changing nature and varying types of security threats that exist and are newly created.

Mobile phones need to be secured because they are the primary means by which users access their learning content. The technology of phones has changed significantly over the last twenty years and phone sizes, shapes, cameras, and microphones all make for an interactive user experience. Potential dangers present themselves in the form of theft, eavesdropping via the built-in microphone, unauthorized use of the camera by an application or virus, and unauthorized access to the device and/or the data it holds.

Mobile phones can be configured by the individual user or the organization that owns the device. For some users, it is a challenge to install and configure different antivirus and anti-malware applications and learn how to configure different settings on the device itself. From an organization's standpoint, they could employ the use of Mobile Device Management (MDM) software. This allows the administrator of the Mobile Device Management software to create a policy for each type of mobile phone that connects to their system (e.g., Android or Apple) and allows them to set minimum requirements for joining the network. These minimum requirements can include operating system version, patching level, anti-virus/anti-malware software installation and scanning, and authentication requirements. Mobile Device Management software will be discussed in further detail later in this section.

Recommendations for securing a mobile device include the use of two-factor authentication. Two-factor authentication requires a username and password along with something else such as a PIN number or a biometric factor such as face recognition or a fingerprint. Second, there should be anti-virus and anti-malware software applications installed, updated, and used on a regular basis such as once per week for each. The prevalence of malware and viruses throughout the digital world now call for this recommendation. Third, the remote wipe feature should be enabled on the mobile device. Remote wipe is a feature that allows the device owner to wipe their phone clean of all information and data stored on it in the event the device is lost or stolen. Lastly, it is highly recommended to use a virtual private network (VPN) for end-to-end encrypted communications. A virtual private network creates a private, encrypted tunnel from the mobile device to the endpoint that the device is connecting to. This provides a much higher level of security during communication. It is recommended that users to avoid using commercially free virtual private network software because those tend to collect data and keep records of your sessions.

Mobile phones can connect to the Internet through either a Wi-Fi connection (wireless access points that are hosted on a computer network) or via their own built in wireless antenna to their service providers cellular base antenna stations. This is what we see in may public places. Setting up Wi-Fi on a computer network requires special considerations to ensure that it is secured. It first starts with the physical security of the Wi-Fi access points. It is imperative that Wi-Fi access points should be placed at a height above 10 feet when possible. The distance off the floor deters people from accessing the equipment and height can also aid in the signal performance of the Wi-Fi access point itself.

Another security consideration for Wi-Fi access points is to disable the Wi-Fi Protected Setup (WPS) button that is usually present on many devices. An unauthorized use of the Wi-Fi Protected Setup feature could disrupt and completely reset that Wi-Fi access point, therefore denying access to users who connect to it. In addition, "Users should be aware that during the two-minute setup period which follows the push of the button, unintended devices could join the network if they are in range. "(Wi-Fi Alliance, 2021)". This means that if someone wanted to join a Wi-Fi network and had access to a Wi-Fi access point that has WPS enabled, all they would have to do is press the WPS push-button and try to join the Wi-Fi network.

Enabling the use of Wi-Fi Protected Access (WPA) 2 with Pre-Shared Key (PSK) or WPA3 with Simultaneous Authentication of Equals (SAE) is also highly recommended. WPA3 is preferred because "The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further

network interaction." (Wi-Fi Alliance, 2021). Another benefit of WPA3 is that "WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data." (Wi-Fi Alliance, 2021). If WPA2 is employed, the Pre-Shared Key should be changed every thirty days. In addition, if an organization is large enough, the use of a RADIUS (Remote Authentication Dial-In User Service) server should be employed to supply the user authentication service. Other security configuration considerations in the Wi-Fi environment include using:

- **Authenticated encryption:** 256-bit Galois/Counter Mode Protocol (GCMP-256)

- **Key derivation and confirmation**: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)

- **Key establishment and authentication:** Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.

- **Robust management frame protection:** 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)" (Wi-Fi Alliance, 2021)

The learning management system holds a vast amount of confidential and legally protected data such as user and course information, grades, and data that must always remain secured. Therefore, it is recommended that the learning management administrators institute a policy that requires a minimum of two-factor authentication to access the LMS. This can be achieved using a username/password along with a verification code that is texted to the user's mobile phone which had been previously registered and verified to LMS administration. The use of encryption during all data transmissions is highly recommended. A regular backup schedule should be created and enforced, along with testing the backups to ensure that the backups have the correct data, and it is accessible when need be. Security can also be enhanced using a virtual private network connection for all data communications that occur within the learning management system. Patching the system should occur when the learning management system vendor recommends it and there are no known issues with the security updates they provide. It is advisable to back up the system data prior to installing any updates and verify the backups prior to installation.

The computer networks that host the learning management system and/or the Wi-Fi network need to be configured in a way that supports security on many levels. As noted by Shonola & Joy, "The server sub-framework is developed to protect the mobile learning host systems from various threats and attacks." (Chova et al., 2014, p. 3338). This sub-framework should employ the use of virtual private network connections, backups, updates, and a VLAN for the Wi-Fi network. A VLAN is a virtual local area network and is created logically within the environment. It is very secure and helps to protect what is inside and what is outside of it (the rest of the computer network) from attacks if they happen. Added security steps can include locking up the computer equipment in rooms that require two-factor authentication and employ the use of CCTV cameras to record who is trying to access the equipment room.

Regular data backups should be scheduled and tested using a virtual private network connection. The use of Mobile Device Management (MDM) software should be considered to manage the mobile devices that join the network, "MDM provides control over employee-owned devices, mitigate risk from stolen or lost devices, segregate data from personal and corporate (Irimia & Rãdulescu, 2019, p. 3). MDM software allows the computer network administrators to create a policy of which type of mobile devices can join their network and which ones cannot. Lastly, regular security audits using penetration testing and security assessment tools should be conducted by qualified penetration testers. Based on those results, the systems should be changed to support a more secure environment.

4. Future Work

Regarding future work, we plan to expand recommendations on how mobile devices can store and send data securely that prevents or deters data theft. An effective security awareness training program for users in the mobile learning environment would add value for students, instructors, and other personnel. Future research can also explore how to secure Wi-Fi networks, learning management systems, and computer networks more effectively, so they all integrate and function securely. Lastly, a research should be conducted to investigate what types of data a social media application should retain. For example, can a

website retain FERPA or PII data? That research can also include the creation of a software program that tracks and records all activities of every social media applications installed on a mobile device, which can then be further analyzed.

5. Conclusion

It is critical to secure a mobile learning environment because the data and information that passes through the five elements are legally protected a lot of times. That is a concern for all parties involved if any of the five elements are not secured. Security considerations in a mobile learning environment take on many different forms depending on which of the five elements of a mobile learning environment is being examined. Some recommendations are realistically achievable by many users and organizations, such as user training, the use of anti-virus and anti-malware software, as well as encryption and a VPN for securing data and communication transmissions. Due to the complexity, cost, or level of skill needed to implement them, other recommendations will be difficult to achieve.

References

[1] Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). Syngress.

[2] Brown, E. (2001). Speaking of computers. *Mobile learning explorations at the Stanford learning lab*, (55).

[3] Chova, L. G., Martínez, A. L., Torres, I. C., Shonola, S. S., Joy, M. (2014). Security framework for mobile learning environments. *In*: ICERI 2014: Conference proceedings.

[4] Friedman, J., Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, 7, 1590180.

[5] Greenberg, A. (2019, August 9). *Teen hacker finds bugs in school software that exposed millions ofrecords*. Wired. https://www.wired.com/story/teen-hacker-school-software-blackboard-follett/

[6] Irimia, D., & Rădulescu, R. (2019). Mobile device management in the context of byod. https://www.researchgate.net/publication/333263130

[7] Ismail, M. I. (2016). A review of the challenges and issues in mobile learning. *International Journal of Enhanced Research in Educational Development (IJERED)*, 4 (2) 1-6.

[8] ReportLinker. (2020, August 18). *Global mobile learning industry*. GlobeNewswire News Room. https://www.globenewswire.com/news-release/2020/08/18/2080347/0/en/Global-Mobile-Learning-Industry.html

[9] Sletten, M. A. (2020). *Security in a mobile learning environment* (Doctoral dissertation). University of Illinois, Urbana-Champaign

[10] Wi-Fi Alliance. (2021, January 1). *How does Wi-Fi protected setup work? | Wi-Fi alliance*. *https://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work*

[11] Wilson, M., Hash, J. (2003). *Building an information technology security awareness and training program: Computer security* (800-50). National Institute of Standards and Technology/Technology Administration/U.S. Department of Commerce.