OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Mini-review

Improving Security of Patient Health Information Regarding Wireless LAN Networks

David A Walker*

Department of Engineering, Northwestern University, Evanston, USA

ABSTRACT

The objective of this article is to report the results of data collected to search for solutions towards advancements in strengthening hospital wireless network security. Patient data breaches cost hospitals billions of dollars annually. The analysis of the data collected for this qualitative exploratory historic case study indicated that hospitals are searching for solutions to protect patient data from wireless network breaches, and the results of the analysis are available for review. This article presents results of the data collected and reviewed for this qualitative exploratory historical case study, as well as the results of the analysis of the data.

Keywords: LAN Networks; Databases; Data transcripts; WEP protocol; Biometric Technology; Facial recognition

INTRODUCTION

The themes discussed will outline possible solutions that could be incorporated to help increase security on hospital wireless LAN networks. Biometric technology for authentication via fingerprint and retinal scan, and facial recognition technology for smart devices are examined. Chapter 4 presented the findings of the themes from the data analysis. Finally, the article discusses the summary of the findings and the conclusion to the chapter.

DATA COLLECTION RESULTS

The data compiled for this research study came from a collection of articles, peer- reviewed journals, and scholarly literature written regarding the wireless protection of hospital patient health information over the past ten years, from 2006 to 2016 and posted on the collegiate, scholarly web databases. Throughout this qualitative exploratory historic case study, the information was compiled regarding patient data breaches and addresses how breaches affect hospitals. In the reviewing of articles, journals, and scholarly research for contributing information necessary for the research, this qualitative exploratory historic case study conducted keyword searches. By applying keywords in the search parameters on online research databases, over 2,500 scholarly journals and prior research articles were examined for this qualitative exploratory historic case study in an attempt to retrieve data relevant to the research performed for this qualitative exploratory historical case study. After compiling the articles and journals necessary for this qualitative exploratory historic case study, commonalities arose. Presented below are the themes of the study.

DATA ANALYSIS AND RESULTS

When analyzing the data for this qualitative exploratory historic case study, the information was gathered from online scholarly resources. The objective for analyzing the data for this qualitative exploratory historic case study was to examine security processes previously instituted. The information regarding security processes implemented previously can be used to search for improvements that would allow hospital personnel to work more efficiently towards the prevention of wireless data breaches in hospitals [1]. Reviewing the scholarly online data resources produced common themes that possibly render solutions to the hospital data breaches. Of the articles and journals reviewed for this qualitative exploratory historic case study, 49% referenced the WEP, WPA and WPA2 security protocols as early solutions to wireless data breaches. The data analysis for this qualitative exploratory historic case study did not include interview transcripts or any transcript analysis.

Data transcripts are derived from group and one-on-one interviews with personnel having information specifically connected to the topic being examined for a study. The personnel interviews gathered for a research study can be in

Correspondence to: David A. Walker, Department of Engineering, Northwestern University, Evanston, USA, E-mail: dwalker6282@gmail.com

Received: November 5, 2020; **Accepted:** November 20, 2020; **Published:** November 27, 2020.

Citation: Walker DA (2020) Improving Security of Patient Health Information Regarding Wireless LAN Networks. J Inform Tech Softw Eng. 11:246.

written, video or audio format. To include recorded (audio or video formatted) interviews in a research study, any audio or video files compiled for use in a study; need to be transcribed into written form. The sensitivity and protection of electronic patient information did not allow the gathering and use of data transcripts for this qualitative exploratory historical case study so prior relevant research journals and articles were used.

Scholarly journals and peer-reviewed articles referenced in this qualitative exploratory historical case study were reviewed and compiled according to the relevance to the study, into primary and secondary data reference points. Information deemed not relevant for inclusion was not used but set aside. After reviewing and sorting by relevance, the scholarly journals and articles researched for this qualitative exploratory historical case study, themes were formulated. The themes realized for this article have been composed from the information gathered during the analysis of the articles and journals researched online.

Theme one

After Finding Vulnerabilities with WEP and WPA, Increasing Security on Wi-Fi Protected Access (WPA2) is a Solution

Theme one indicates possible advancements in WEP security, including the Wired Equivalent Privacy (WEP) protocol created. IT experts designed the WEP protocol to transmit data between devices while preventing any unauthorized access to the data [2]. Of the 2,500 articles and journals researched for this qualitative exploratory historic case study, 19% (475 documents) focused on the security issues associated with WEP [2]. WEP technology instituted a beginning to solutions in security for wireless networks and would later be improved upon to increase the level of security provided. A minimal number of facilities applied WEP technology, less than 32% on average [2,3].

The information returned during the literature review indicated the reason for the low percentage of usage was because even though WEP could protect against some intrusions, WEP technology was easily breakable [3]. WEP was an early solution and was vulnerable because of the ease in breaking through the security. Because security of WEP was fragile, experts upgraded their platforms to increase security properties of the protocol [3]. The need to increase the security of protocols used for wireless networks initiated the creation of WPA.

WI-FI protected access 1: From the articles and journals researched for this qualitative exploratory historic case study, 22% (550) of the articles discussed Wi-Fi Protected Access, or WPA as an improved solution over WEP [3]. Experts considered WPA a more effective security solution for wireless networks [2].WPA utilized stronger wireless encryption and amended the flaws seen with WEP [3]. WPA offered stronger user authentication than WEP. Stronger user authentication meant stronger security for the network. The journals and articles referenced in this qualitative exploratory historic case study indicate the importance of the security aspect of implementing WPA [3]. Hospital organizations introduced and preferred WPA as a solution over WEP with regard towards protecting patient data. Technologists have implemented improvements in WPA with the introduction of WPA2 [3].

WI-FI protected access 2: Improving security solutions is a significant topic for hospitals with regard to protecting wireless data, with 28% of the research articles referenced in the study (700 documents) covered WPA2 as a viable security solution and a significant improvement over WEP and WPA [4] wrote that organizations tend to focus on protecting the information transmitted across the network. Security protocols such as WPA and WPA2 implement encryption to facilitate the security level attained [4]. WPA2 improved upon the security capability of WPA by using much stronger encryption. Wi-Fi Protected Access II (WPA2) improved the encryption process of WPA by applying an encryption method called Advanced Encryption Standard (AES). Realizing the security benefit of WPA2 on wireless networks, hospitals began to favor WPA2 over WPA and definitely over WEP.

The topic of solutions in wireless security presented in this qualitative exploratory historic case study represents the most significant percentage of referenced works used for this research, at 49%, and addressed the issue of wireless network security for hospitals. The implementation of security solutions on wireless networks is of significant concern for hospital leadership and personnel. According to the articles referenced in this qualitative exploratory historic case study, many hospitals have the same concern and are working to improve solutions implemented on the networks. The main reason for the necessity of improved solutions is data breaches that affect patient health information.

Theme two

Biometric Technology is a Solution that will Offer an Added Layer of Protection for Wireless Network Authentication.

Biometric modalities can be implemented to facilitate solutions for secure authentication logins and user identification .Biometric technology is a security solution used to ensure that person(s) connecting to the hospitals' wireless networks are who they say they are Modes of identifying an individual through biometric scanning consists of swiping a fingerprint, scanning the retina of the eye, voice recognition, and scanning of facial features. Of the articles researched for this topic, 5% of the documents referenced biometrics. Biometrics offers available options for authentication to wireless networks and wireless devices in the form of voice, facial, and fingerprint recognition, as well as retinal scanning. A biometric form of identification security works very well, as no two persons would have the same identifying features.

Biometric authentication solutions are already being implemented in some mobile devices and smart devices. Many desktops and laptops being built are implementing fingerprint scanners for keyless authentication. Keyless authentication technology is a solution introduced in smartphones and tablets. Another solution for wireless security is the implementation of facial recognition software [5]. Facial features are unique to each person, even twins, and would serve well for identifying and providing security for the individual and the data.

Theme three

Facial Recognition Software as a Solution for Smartphones connecting to the Hospital Networks.

Another biometric solution for hospital wireless networks and the protection of patient data is facial recognition software [5]. Facial recognition software is available today as a viable solution that provides recognition capabilities for over 5 billion smartphones [5]. Facial recognition software runs 100% on modern smartphones. Implementing biometrics would work very well as the answer to securing data and curbing the breach occurrences and issues that hospitals have experienced since the introduction of the mobile devices.

One of the issues mobile devices experienced was the security of mobile applications. The flaw regarding the lack of security for mobile applications on the mobile devices would allow non-authorized personnel to access PINs and passwords and cause a severe breach with mobile applications. Even though the focus was on the applications that use PIN numbers, the breach of mobile applications could be a problem with other devices and other applications as well. Bromwich and Bromwich stated that problems with mobile devices could thwart the efforts of the security procedures and policies implemented to help protect the data on wireless networks.

Mobile devices could have a flaw that would allow hacks into the system to gain access to the wireless network, making it possible to glean data from the host network without the approval or knowledge of the network management team. Bromwich and Bromwich used the article as an attempt to examine the issues and gain knowledge into what could be a significant issue for wireless network managers. The remediation of breach vulnerabilities on smartphones and mobile devices helps hospitals to ensure that customers can safely navigate the wireless networks.

With facial recognition software having many beneficial capabilities and requiring specific safeguards set before implementation and use, the recognition software is a solution worth exploring and examining [5]. The facial recognition software would require specific parameters for network users to enter as a secure sign-on process. With information stored in the biometric key, it would easy for an employee to track down the user's identity should a breach of hospital data occur [5]. The principal reason for the need for improved security comes in the form of breaches that affect patient health information. Also, visitors would still seek to connect to the wireless network while waiting for services.

Visitors should be able to access the guest network when visiting the hospitals and either waiting for procedures, are family members, or are in the hospital for an extended stay after a procedure. Locking down the wireless networks does not mean that visitors would not be able to access the network. If malicious activity continues against the networks, the network administrator can lock down the wireless network. This process will log and retrieve the sign-on and access activity of the offending individuals. Biometrics would aid security officials in the process of tracking down individuals that seek to gain unauthorized access to patient data. Another solution to protecting the patient data on wireless networks involves having the ability to hide the networks from unauthorized access completely.

SUMMARY OF FINDINGS

This qualitative exploratory historic case study presents three themes that serve as possible solutions to hospital data breaches. The information was compiled in this qualitative exploratory historic case study to examine the protection of hospital electronic patient data. The security of patient data is essential, according to the regulations and policies of HIPAA .The information supports the statement that breaches of hospital wireless networks regarding patient data happen more frequently than previously realized, and solutions are needed. Solutions in the form of biometric and facial recognition options, and improving the updates necessary for the wireless protocols, are available for the protection of patient data on wireless networks.

DISCUSSION AND CONCLUSION

This article presented the results of the data collection process, and discussed the information compiled regarding patient data breaches in hospitals and the current processes implemented to stop the breach attacks. This qualitative exploratory historical case study reviewed over 2,500 journals and peer-reviewed articles for information pertinent to the topic of hospital wireless LAN security of electronic patient health information. In the reviewing of articles, journals, keyword searches were performed. Also presented are the results of the data analysis performed, which resulted in three specific themes. The themes covered the WEP, WAP, WPA2 wireless security protocols, the frequency, and costs of wireless data breaches. The themes are also covered possible wireless network solutions in the form of biometric authentication. Finally, this article discussed the summary of the findings, stating that the security of patient health information is essential for hospitals, and that solid solutions need to found, upgraded and implemented to protect the data pertaining to patients health, identity and well-being.

REFERENCES

1. Mandal A, Asthana AK, Aggarwal LM. Experience of wireless local area network in a radiation oncology department. J Cancer Res Ther. 2010;6(2):148-151.
2. Heslop L, Howard A, Fernando J, Rothfield A, Wallace L. Wireless communications in acute health-care. J Telemed Telecare. 2003;9(4):187-193.
3. Misra S, Sarkar S. Priority-based time-slot allocation in wireless body area networks during medical emergency situations:an evolutionary game-theoretic perspective. IEEE J Biomed Health Inform. 2015;19(2):541-548.
4. Almashaqbeh G, Hayajneh T, Vasilakos AV, Mohd BJ. QoS-aware health monitoring system using cloud-based WBANs. J Med Syst. 2014;38(10):121.
5. Choi JM, Choi BH, Seo JW, Ryu MS, Yi W, Park KS. A system for ubiquitous health monitoring in the bedroom via a Bluetooth network and wireless LAN. Conf Proc IEEE Eng Med Biol Soc. 2004;2004:3362-3365.