International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 1613–1619

Pragmatic Overview Of Security Issues Of Healthcare Management System And Its Countermeasures.

Minal D. Kalamkar[1]
Research Scholar, T.M.V., Pune
minaldk@gmail.com

Dr.Vikas Prasad[2]
Associate Professor, School of General Management,
National Institute for Construction Management & Research,
Balewadi, Pune 411 045, Maharashtra, India
drvikaspd@gmail.com

Abstract*:*
Over the past few decades, due todigital innovations, technology opened up myriads of opportunities in all sectors of business, even in the healthcare industry. With the increasing number of mobile users, everything is available at fingertips including healthcare services. There are many web applications and mobile applications related to healthcare services that are used to right from seeking consultation to prescription management etc. These applications with such facilities alsohave the potential risk of data breaches or meddling of Electronic Health Record (EHR). Although the research literature in this area is sparse, the aim of this research to consolidate all security issues that are faced while maintaining patient data through the healthcare management system(H.M.S.) and its countermeasures.
Keywords*: countermeasure, data breaches,electronic health record, healthcare management system, security.*

1.Introduction:

Gustav Wagner established the first organization for health informatics in Germany in 1949**.** In the early 1950s, technology entered the field of medicine worldwide. [1]

Healthcare Management system ismeant to assist healthcare providers to gather, store, and share patient information more efficiently and to enhance patient care**.**[2]

Whereas an electronic health record (EHR) is a digital version of a patient's medical record. In other words, an EHR is a collection of medical information about individual patients stored in an electronic manner, which may contain anything from a patient's information and social security number to the diagnosis of a patient with a certain disease. [3]

The recent explosion of technologies like the Internet of Things(IoT)and mobile health (mHealth) is used to collect real time data via wearable devices. The continuous stream of data can be captured by sensors, stored, and analyzed using the above mentioned technologies. These inventions yield new insights into the security issues associated with EHR.

Yet while digital innovations can be a boon, but it also takes one's attention to ensure that data maintained by H.M.S.is secure. Technology also has a dark side. The software needs toupdate to keep information functioning and safe. Non updatedsoftwareis prone to attack with a virus or malware. Personal information could be compromised by stealing cookies. Over time, a patient's information in the H.M.S hoards remarkable personal information including identification, symptoms, history of the disease, immunization records, digital reports, radiology reports,details of treatments, medication history, food habits, lifestyle details, genetic information, psychological information, physicians' subjective assessments of disease,personality, mental state, social security number, and billing information.[4]

Cyber-attack is a prime concernwhile dealing withthe security of H.M.S. As new exploits are discovered every day, we cannot fully overcome Cyber-attacks.[5]

ISSN: 2233-7857 IJFGCN

Theseattacks may result in gaining access to the hospital intranet in turnto compromise a large database of patient medical records.

1.1 Whyhealthcare is being a target?

Why hackers hack the information or system depends on their aim. A criminal hacker aims to steal financial information or someone's identity. It may be due to out of the excitement of doing something different or to know the internal structure of the system or working of the system whereas ethical hackers do it to find the vulnerabilities in the software. [6]

The healthcare sector became another target of cybercriminals due to the sensitive and critical informationaccumulatedby H.M.S. and its capacity to hold personal and financial information. Cybercriminals apart from their own interest are also selling the healthcare data in underground markets.[7]

EHR is having valuable assets as follow:

Medical data: To perform attacks like identity theft as it contains telephone numbers, social security numbers, credit card numbers, billing information

The service: Further, not being able to access a patient's health records could cause serious threats to patient safety.[8]

1.2 Common Vulnerabilities:

It is clearly seen from OWASP report, vulnerabilities like SQL injection, cross site scripting (XSS) are still in the top 10 positions. These vulnerabilities have great potential to breach the Healthcare Data. Out of which this study focuses on scripting attacks, XSS is one of them. There are 4 types of XSS: 1. Stored attack 2. Reflected attack 3. DOM based attack 4. Induced attack.

Types of XSS:

1 Stored or Persistent attack: This type of attack happens because of the exploitation of a vulnerability in the web applications by attacker.He injects the script that permanently resides on the server. When the user tries to access the web application, the malicious script gets executed that can steal the user's information

Generally, stored XSS attacks are performed on web applications like forums, comments and blog sites where input textis entered by the user and gets stored in the web application's database.[9]

2 Reflected attack or Non-persistent attack:

In this type of attack, hackers send malicious script embedded in an email or any web page residing on another server. When user clicks on the link, the payload gets injected in attacker's web server and the attack gets back to victim's browser. As it comes from a trusted server, the victim's browser executes the code. Thus,bypassingthe same origin policy. After executing a malicious script, an attacker gains the control of victim's system and can steal sensitive information.

3DOM attack:

In this type of attack, DOM structure of the victim's browser is modified by the original client-side script to execute client-side code in unexpected way. In this type of attack, web page doesn't get modified but DOM structure gets changed.

4 Induced attack:

This type of attack takes place when web server possesses HTTP response splittingvulnerability. The attacker manipulates server's HTTPresponse header and so the HTML content by finding an invalidated request parameter that is present in the HTTP response header.[10]

2. Security assessment:

This study involves the security issues of healthcare web applications for which 22papers
have been studied using keywords like healthcare security, healthcare application vulnerability, cyber-attacks on healthcare, chatbots, phishing, wifi, etc. After going through all papers,
questions have been categorized into security issues and its countermeasures. The questions have been designed to know what are the different ways or causes in which malicious scripts can be injected and

ISSN: 2233-7857 IJFGCN

executed by the hacker so as to acquire control of the victim's account along with their countermeasures. Considering the aim of the study, following research questions were formulated.

RQ1.
What are the security issues that are associated while using a healthcare management system?
This question helped to give an overview of the security issues associated with healthcare management systems.

RQ2.
What are the countermeasures that can be implemented to address the security issues concerned with the healthcare management system?

2.1 Literature Review: Using related literature review, the causes concerned with security issues involved in the usage of the healthcare management system and its countermeasures are recognized.

2.1.1The challenges in maintaining the security of HMS:
With upcoming technologies and inventions, each day the healthcare industry faces new challenges to protect patient data from various security issues.These security issues can be categorized into the following categories: Network, software, browser and other attacks that are related to user's awareness.
Network
Public Wi-Fiis not password secured hence these are at greater risks and can be easily get attacked by the hacker. Hence it is recommended to avoid the use of public Wi-Fi. [11]

Software
Considering the ubiquitous use of web application in every domain, web application security became a prime concern with the increasing number of threats in web development. The web application possesses a risk that exploits applications and systems vulnerabilities. Tragically, the vast majority of web engineers emphasize more the application usefulness and user interface(UI).[12]
In spite of implementing appropriate measures, the problem arises in the case of interoperability which involves third-party systems. Outdated healthcare systems lack in updated security measures.[13]
Generally due to web application's weak security is the main reason behind the scripting attacks. By overlooking sanitization, the user input is prone to XSS. These unsanitized inputs are used by the attackers to exploit the vulnerabilities in web applications. [14]
The attacker can execute JavaScriptfiles that are embedded in PDF files that can cause security issues on the victim's machines.
Though sharing documents between users is a part of HMS, but with this,the ability to inject malicious scripts or embedded executable could facilitate attackers to exploit the application's infrastructure.[15]
URL shortener makes the URL short and succinct. These services were launched in 2001. To hide the identity, phishers are using a short URL. With a short URL, it becomes difficult to make a judgment whether the URL is spam or not.Generally,phishing emails are targeted for banking and other financial frauds. Some well-known URL shorteners are bit.ly, goo.gl, is.gd, ow.ly.[16]
Software cracking is a term used for the modification of software to remove or disable features. Pirated software is nothing but cracked software and generally had the modified executable that can cause undesirable behavior.
Using a malicious script, the known vulnerability of the software can be exploited. Another form of malware is viruses that can delete the files or corrupt the hard disk [17]
Using compromised machines, it is possible to install malicious software or even hardware-based keystroke loggers to gather sensitive information like user credentials
Free software is referred to as freeware that may contain malware that can infect the system functionality. [18]

ISSN: 2233-7857 IJFGCN

The study [19] shows locations and names leak more from web sites than mobile applications moreover it was found that passwords were sent to the third parties without reason. Both mobile applications and web sites can reveal locations, gender, names, and email addresses.
Steganography is a method of communication by sending a hidden message. Stegware is the use of steganography that makes use of malware for furtive cyber-attack. A malicious script may be embedded within an image file by an attacker that can be executed to perform the attack.[20]
Attackers can create malicious chatbots that may trick the users to click the links or share personal information [21]

Browser
The browser histories enhance user experience. The browser histories can disclose the user activities and internal web server structurewhich is vulnerable to data theft. Depending on their usage and content, cookies could contain subtle information about users that can lead to session hijacking.The machines that have low web browser security settings cannot show warning when an SSL certificate seems to be suspicious.[22]
Make sure the browser setting is set to clear data when the browser is closed. Browser cache, browser histories are maintained by the browser to enhance the user experience. The browser histories reveal the user activities and internal web server structure. [23]

Awareness
The medical data must be protected from a data breach or any modifications. The information must be transferred securely and should be adhered to all ethical and legal restrictions. Assuring security certification of the web site is a means of guaranteeing that medical data are exchanged and processed appropriately. Certification ensures auditing and information security along with compliance to medical regulations like ISO 27000 series, HIPAA directions,and NABH.[24]
QR (Quick Response) codes are two-dimensional barcodes that are used to encode different types of information like URL encoding or mobile payments. QR codes are popular in the various domain because of their easy use but they also possess security risks that can be exploited by attackers. Thus, benign codes can get replaced by such malicious QR codes that can lead to phishing sites.[25]
Many web sites use Pop-ups to display information. A fake pop up can be used by a hacker for the attack so as to download the malicious software.

2.1.2 The Consequences:
The scripting attack uses the malicious script to exploit the vulnerability in the software to capture the personal information of the user, cookies, passwords can be hacked. Using phishing attack, the hacker can not only steal the patient's health and financial data but also intervene and modifyvital and sensitive medical information that can have extreme implications.

2.1.3 Recommendations:
In an untrusted host, two-factor authentication such as a one-timepassword (OTP) is used to protect users from passive password logging. [26]CAPTCHA is used to distinguish Human and bot which uses visual authentication and identification.
Password attack is performed by predicting possible password combinations until the correct combination is matched. Hence avoid passwords such as birth date, or names. Usedifferent passwords for multiple accounts. By using strong passwords and multiple factors authentication can be used to avoid password attacks like dictionary attacks, brute force attacks, or hybrid attacks [27]
Some tools can be installed like browser cache control, cache cleaner, desktop security, keystroke logger detection that can mitigate the security issues.
Antivirus and Intrusion prevention systems (IPS) can be installed to prevent network attacks, viruses, worms, Trojan horses, spyware, and other security threats. [28]

ISSN: 2233-7857 IJFGCN

Whenever installing free software, always go through the online reviews about the software, the software developer,and the organization that developed that software, along with the steps to uninstall it. [29]
Download freeware only from sources that can be confirmed as reputable and legit. It is not advised to install freeware from an organization that is unknown.
The study [30] shows that different password managers used to save passwords to device storage in an insecure manner. While login into any account, whenever the browser asks whether to save the password or not, do not select the "always allow" option otherwise the password will automatically be saved next time.
Considering software application security, the use of unlicensed software and old version software should be avoided. [32]
Whenever Pop up is shown by the website, it can be found if Pop up is fake or not just by noticing the URL of Pop up. Pop up blocker is recommended while browsing the web sites. It is recommended to update the software periodically. Software updates fix older version problems and increase the software's stability.
To protect, prevent, quarantine, and remove malware from the computer, antivirus software should be installed and it should be updated periodically. [31]
Do not open any attachments from spam emails or unknown sender.
Data recovery can be done by having data backups regularly to ensure data safety even after a security attack or hardware failure.
Do not plug in any external drives without security scanning that may be infected with malware that can damage the system.
Clear the browser cache. Don't share the passwords.
While using public Wi-Fi, turn off the file-sharing to avoid the chances of receiving the infected files with malware sent by the hacker. Moreover, one can be a victim of accessing a network using a fake Wi-Fi hotspot. Never make the payments using public Wi-Fi. Always check to forget the network after using public Wi-Fi.
Before performing any financial transaction or dealing with sensitive information, look for HTTPS appearing before the web site's address. To ensure security, it's better to use 2-factor authentications to access any account [33]

Summary:

This study is aboutthe overview of the state-of-the-art research related to security issues and their countermeasures while dealing with the healthcare management system. The various issues were found and categorized for which extensive literature review conducted.
The main goal of this work was to identify and consolidate the issues in the area of security along with their countermeasures. Finally,to propose the overall guidelines for maintaining the security of the medical data.

Reference:

1. Yadav, C. S. (2020). Digital Trends Revolutionizing Healthcare Industry. CLIO An Annual Interdisciplinary Journal of History, 6(5), 275-282.c
2. RobertHalf. Retrieved from https://www.roberthalf.com/blog/management-tips/3-things-to-know-about-healthcare-managementsystems#:~:text=Healthcare%20management%20systems%2C%20also%20known,and%20enable%20better%20patient%20care.
3. Austin, A., Smith, B., & Williams, L. (2010, May). Towards improved security criteria for certification of electronic health record systems. In Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care (pp. 68-73).
4. http://www.gescienceprize.org/medical-informatics-strengthening-the-bond-between-patientphysician-relationships/

ISSN: 2233-7857 IJFGCN

5. Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering, 9(3).
6. 18,29]Negi, Y. (2011). Pragmatic Overview of Hacking & Its Counter Measures. In Proceedings of the 5th National Conference, INDIACom, New Delhi, March (pp. 10-11).
7. M. R. Fuentes, Cybercrime and Other Threats Faced by the Healthcare Industry, Trend Micro, May 2018, [online] Available: https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf.]
8. 15,28]Smith, B., Austin, A., Brown, M., King, J. T., Lankford, J., Meneely, A., & Williams, L. (2010, October). Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. In Proceedings of the second annual workshop on Security and privacy in medical and home-care systems (pp. 1-12).
9. Malviya, V. K., Saurav, S., & Gupta, A. (2013, December). On security issues in web applications through cross site scripting (XSS). In 2013 20th Asia-Pacific Software Engineering Conference (APSEC) (Vol. 1, pp. 583-588). IEEE.
10. Sadana, S. J., &Selam, N. (2011). Analysis of Cross Site Scripting Attack. In Proc. International Journal of Engineering Research and Applications (IJERA) (Vol. 1, No. 4, pp. 1764-1773).
11. Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering, 9(3).
12. Hidayanto, A.N., Rinaldi, Handayani, P.W. and Louvan, S. (2013) 'How secure your applications are?: Analysis of web developers awareness to application security', Int. J. Innovation and Learning, Vol. 14, No. 1, pp.53–78
13. Yang, D. (2017). The Risk of Cyberattacks on EHR (Doctoral dissertation, Utica College).
14. Chhabra, S., Aggarwal, A., Benevenuto, F., &Kumaraguru, P. (2011, September). Phi. sh/$ ocial: the phishing landscape through short urls. In Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (pp. 92-101).
15. Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering, 9(3).
16. Leung, C. M. (2009, August). Depress phishing by CAPTCHA with OTP. In 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication (pp. 187-192). IEEE.
17. Wiseman, S. (2017). Stegware – Using steganography for malicious purposes. 10.13140/RG.2.2.15283.53289
18. Murugesan, S. (2019). The Cybersecurity Renaissance: Security Threats, Risks, and Safeguards. IEEE ICNL, Jan-Mar.
19. Schiller, E. I., & Luminita, D. C. C. (2012). SSL VPN security issues. Global Journal on Technology, 2.
20. Varlamis, I., Apostolakis, I., &Chryssanthou, A. (2010). Certification and Security in Health-Related Web Applications.
21. [26]Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., &Weippl, E. (2014, June). QR code security: A survey of attacks and challenges for usable security. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 79-90). Springer, Cham.
22. Leung, C. M. (2009, August). Depress phishing by CAPTCHA with OTP. In 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication (pp. 187-192). IEEE.
23. Mitz.(2014, April1). TIPS4PC. Retrieved from http://tips4pc.com/computer-software-tips/precautions-before-installing-software.htm

ISSN: 2233-7857 IJFGCN

24. Silver, D., Jana, S., Boneh, D., Chen, E., & Jackson, C. (2014). Password managers: Attacks and defenses. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 449-464).
25. Ghazvini, A., &Shukur, Z. (2016). Awareness training transfer and information security content development for healthcare industry. International Journal of Advanced Computer Science and Applications, 7(5), 361-370.
26. Baig A. (2018, October 19).GlobalSign. Retrieved fromhttps://www.globalsign.com/en/blog/staying-safe-using-public-wifi
27. Tilak, G. Usage of Visual Communication Design on Consumer Behaviour.

ISSN: 2233-7857 IJFGCN