International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 No: 3 March 2020

A Survey on various Security Issues in Health Data in Web Applications

P. Maragathavalli[1], M. Seshankkumar[2], V. Dhivakaran[3], S. Ravindran[4]
Department of Information Technology, Pondicherry Engineering College, Puducherry, India
[1]marapriya@pec.edu, [2]seshank98@pec.edu, [3]dhivakaran17299@pec.edu, [4]segarravindran@pec.edu

Abstract: The health data in web application faces various Network security threats such as Man-in-the-Middle Attack (ARP spoofing, mDNS spoofing and Evil Twin), SQL injection, Denial of Service (Dos) and the prevention from these threats are discussed in this paper. ARP Spoofing, mDNS spoofing comes under IP spoofing, it is a way used to gain unauthorized get entry to to machines, wherein an attacker illicitly impersonates another device by way of manipulating IP packets. A Man-in-the-Middle attack (MITM) is accomplice degree attack wherever the offender in secret relays and possibly alters the communications between two parties who believe they're without delay human movement with one another. Using these attacks the health data can be stolen and modified. To overcome these networks security issues various methodologies like HTTP/1.0, HTTP/2.0, SSL, and HTTPS. The advantages and disadvantages are discussed in this paper.

Keywords: Network Security, IP Spoofing, Security Threats, Man-In-The-Middle attacks, Web Authentication.

1. INTRODUCTION

Nowadays, every health care organization supplies an enormous amount of information to doctors, pharmacies, and patients online via the web. While printed information is static, web-based content is dynamic and updated promptly. However, websites and web servers are exposed to various network security threats. Any server connected to an online network will not only suffer from internal threats caused by employees of health care organization as a result of misuse of network resources, but are also vulnerable to a range of outside threats. Man-In- The-Middle (MITM) Attacks is one among the most important and most dangerous network security threats in web application. In MITM a malicious actor inserts themselves into a conversation between two people and where the attacker is able to get information that is sent and received between server and client. MITM has many types like ARP spoofing, mDNS spoofing and Evil Twin and other web security issues are SQL injection, Denial of Service (DoS).

ARP spoofing also usually referred to as ARP cache poisoning is one of the Local Area Network network techniques where attackers send spoofed Address Resolution Protocol (ARP) to one or more target hosts. This issue is one of the grand challenges that need to be addressed in the security enterprise. Many malware attackers use static or dynamic methods to communicate Command and Control to the centralized server. All is set at static process. This is, the malware will permanently have both a fixed IP address and a fixed domain name. Thus if a malware has been detected, a simple rule is used to rectify the issue. ARP spoofing is often used as the first move in bigger attacks, where the attacker's ultimate aim may be to achieve a man-in - the-middle role between two hosts or to trigger a denial of service (DoS) against one or more hosts. The Address Resolution Protocol is unsafe to spoofing because there is no authentication for all these messages and therefore any host will emit ARP requests or responses to another host. This approach has been known for 20 years, and remains an area of concern in the security community, analyzing and mitigating strategies to identify it. Although ARP spoofing is typically addressed in connection with wired LANs, it may be more dangerous and easier to execute — in wireless ad hoc networks where hosts are allowed to exit and enter regularly, the physical communication medium is readily accessible and no central security co-ordinating body exists; recognizes the catastrophic effects of ARP poisoning on ad hoc networks.

Often known as the Multicast Domain Name Scheme, mDNS is the same as DNS, but it is performed on a Local Area Network (LAN) using ARP spoofing as broadcast. It renders it a perfect target for spoofing attacks the native name resolution framework is intended to build very easy network device configuration. Users need not be aware of

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 No: 3 March 2020

which address should be communicated with; the system itself resolves. It protocol is used by entertainment services, because they are usually on trusted networks. When an app needs to know a certain device's address, it is simple for an attacker to respond with fake information. Since devices keep a neighborhood cache of addresses, the victim can currently see the attacker's device as sure for a period of the time.

An evil twin, within the context of network security, may be a villain or faux wireless access purpose (WAP) that seems as a real hotspot offered by a legitimate supplier. In associate degree evil twin attack, associate degree listener or hacker fraudulently creates this villain hotspot to gather the non-public knowledge of unsuspecting users. The most sensitive data might be stolen by phishing or spying on a connection.

SQL Injection (SQLi) may be a form of associate degree injection attack that produces it potential to execute malicious SQL statements. These statements management a information server behind an online application. Attackers will use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of net, an internet, an online page or web application and retrieve the content of the complete SQL information. They can also use SQL injection for modifying and deleting the records in the database.

A denial-of-service attack may be a security event that happens once associate degree offender prevents legitimate users from accessing specific pc systems, devices, services or other IT resources. Denial-of-service (DoS) attacks usually flood servers, systems or networks with traffic in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them

To prevent these attacks in a web application, encryption mechanism with strong wireless access points should be used. It eliminates the unwanted users from joining the network. A weak coding mechanism will permit associate degree offender to brute-force his means into a network and start man-in-the-middle offensive. Thus the encryption mechanism should be stronger. The techniques used to prevent these network security threats are SSL, HTTPS, HTTP/1.0, HTTP/2.0 and TLS. Their drawbacks are mentioned in the literature survey table.

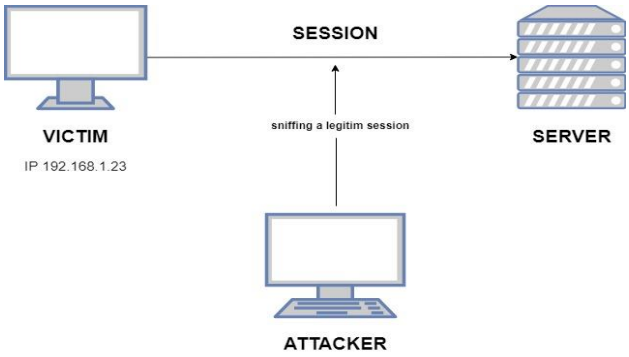


Figure 1. Man-In-the-Middle attack scenario

Fig 1 demonstrates MITM attack where a attacker illegally monitoring the communication between a client and a server where the information is to be sent. The attacker can also change the information that is transmitted between the server and client.

2. LITERATURE SURVEY

Table 1. Survey on Network Security Types in Web Application

Sl. No.	Name of the Journal, Year	Title of the Paper	Technique / method / algorithm	Data set used	Parameters used	Results	Limitations
1	IEEE Translations and Content Mining, IEEE Access, 2019	An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4.0 Supply Chain	TLS Protocol	Existing Array dataset	Communication overhead	Reduces communication overhead by 50%	Server side security is not considered

2	IEEE Translations and Content Mining, IEEE Access, 2019	Questioning Key Compromise Attack on Ostad-Sharif et al.'s Authentication and Session key Generation Scheme for Healthcare Applications	Session Key	Existing Healthcare dataset	Authentication	Increases the level of authentication	Only key compromise attack is considered
3	IEEE Translations and Content Mining, IEEE Access, 2019	Security-Aware Department Matching and Doctor Searching for Online Appointment Registration System	Public Key Encryption	Electronic Health Record (EHR)	Communication Overhead	Decreases Communication Overhead	Data transmission is not considered
4	IEEE Translations and Content Mining, IEEE Access, 2019	A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images	Watermarking Scheme	Medical Image	Computational Overhead	Decreases Computational Overhead	Only image data is considered
5	Smart Innovation in Communication and Computational Sciences, Springer, 2018	Analysis of Hypertext Transfer Protocol and its Variants	HTTP/1.1, HTTPS, HTTP/2.0	Existing Array dataset	Load time, Computational overhead	Decreases the load time of a site and Improves its performance parameters.	More Computational overhead
6	Multimedia Tools and Application, Springer, 2018	XSS-secure as a service for the platforms of online social network-based multimedia web application	XSS-Secure using HTTP response	URL from Google	Response time	Reduces response time	Security metrics are not considered
7	Information System and Technologies, Springer, 2018	Implementation of Web Browser Extension for Mitigating CSRF Attack	SRF Detector performs based on HTTP request	URL from Google	Time Complexity	Reduces load time by 0.21 s.	Server side security is not secure

In most of the papers mentioned above they used a single validation to check the man in middle attacks. The attacker can steal the information easily. The existing mechanisms such as SSL protocol, HTTPS protocols and TLS protocol provide only partial security against such attacks and these mechanisms also use only single validation to check these attacks (i.e.) protection of information sent from only client-to-server it considered; not server-to-client. So the attackers can easily hack the password of users and steal the health care very easily. The security can be improved by giving double validation before transmitting the health care data. By giving

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 No: 3 March 2020

additional security, parameters such as confidentiality, integrity and privacy can be improved and communication overhead can be reduced.

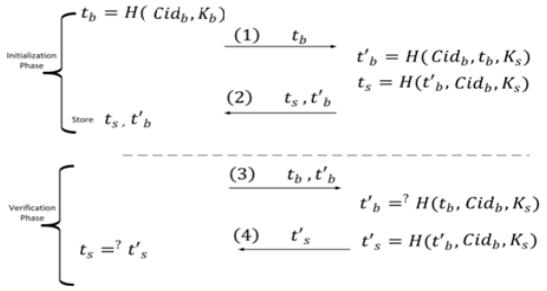
3. PROPOSED WORK

In this proposal, a new methodology is used in Transport Layer Security (TLS) Protocol along with two symmetric hashing techniques namely modified MD5 and SHA-1. The TLS protocol is used to establish a connection between two parties in a secure way. The main objective of this protocol is to provide privacy and data integrity between two communicating entities over the Internet. The major advantage of this mechanism is to improve the efficiency of network security protocol against MITM attacks and reduce the communication overhead in web applications. The proposed mechanism consists of two phases: Initialization and Verification.

Initialization: The purpose of this phase is to make a preparation for the client authentication.

Verification: The verification phase takes place upon every subsequent TLS connection to the server which occurs within the same browsing session.

Both the steps are clearly explained in module description.



Initialization and Verification Phase

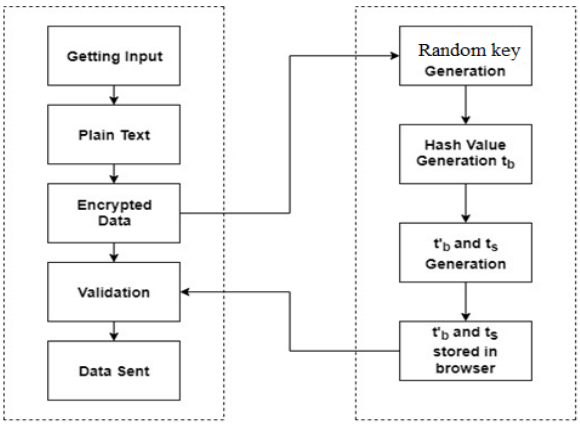
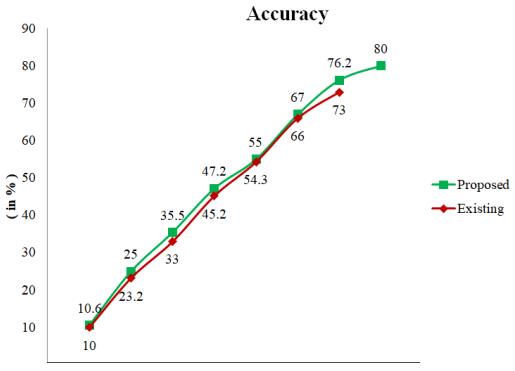
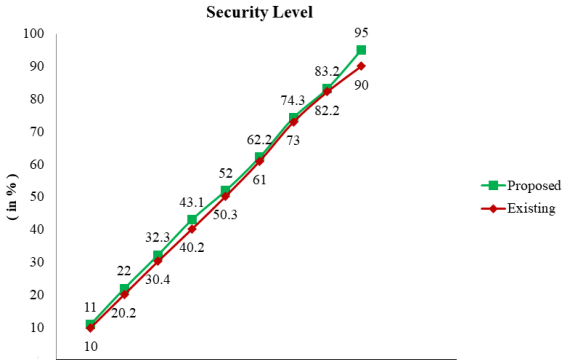


Figure 1.1. Proposed System Design

4. RESULTS



Accuracy



Security Level

5. CONCLUSION

From the survey we conclude that each method have their own advantage and disadvantage. It is clear that SSL is not sufficient to keep against desktop conciliation attacks. It is also moderately well understood that, for high value applications, SSL is still not sufficient to defend against societal production attacks on health care data, as proof by the miserably high success of such societal production attacks on health care data. HTTPS has more computational complexity than HTTP. HTTP/2.0 has more computational overhead. Further security can be provided in network in web application, which can make the network communication more secure and faster.

REFERENCES

[1] Alireza Esfahani, Georgios Mantas, Jose Ribeiro, Joaquim Bastos, Shahid Mumtaz, Manuel A. Violas, A. Manuel De Oliveira Duarte and Jonathan Rodriguez, "An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4.0 Supply Chain", IEEE Translation and Content Mining, *IEEE*

Access, ISSN: 2169-3536, Vol. 7, Apr 2019, pp.58981-58989.

[2] Awais Ahmad, Mudassar Ahmad, Muhammad Asif Habib, Shahzad Sarwar, Junaid Chaudhry, Muhammad Ahsan Latif, Saadat Hanif Dar and Muhammad Shahid, "Parallel query execution over encrypted data in database-as-a-service (DaaS)", The Journal of Supercomputing, Springer, ISSN: 1573-0484, Vol. 75, Iss. 4, Mar 2019, pp.1-19.

[3] Nayanamana Samarasinghe and Mohammad Mannan, "Another look at TLS ecosystems in networked devices vs. Web Servers",Computer and Security, Elsevier, ISSN: 0167-4048, Vol. 80, Sep 2018, pp.1-13.

[4] Ru Zhang, Gongshen Liu, Jianyi Liu and Jan P. Nees, "Analysis of Message Attacks in Aviation Data-Link Communication", IEEE Translation and Content Mining, IEEE Access, ISSN: 2169-3536, Vol. 6, Feb 2018, pp.455-463.

[5] Mohammed Awad, Muhammed Ali, MaenTakruri and Shereen Ismail, "Security vulnerabilities related to web-based data",TELKOMNIKA (Telecommunication, Computing, Electronics and Control),ISSN: 1693-6930, Vol. 17, No. 2, Apr 2019, pp.852-856.

[6] Aakanksha, Bhawna Jai, Dinika Saxena, Disha Sahni and Pooja Sharma, "Analysis of Hypertext Transfer Protocol and Its Variants",Smart Innovation in Communication and Computational Sciences, Advances in Intelligent Systems and Computing,Springer, ISBN: 978-981-10-8971-8, Vol. 670, Jan 2019, pp.171-188.

[7] Mohammed Abdulridha Hussain, Zaid AlaaHussien, Zaid Ameen Abduljabbar and Sarah Abdulridha Hussain, "Boost Secure Socket Layer against Man-In-The-Middle Sniffing Attacks via SCPK", in Proceedings ofThe IEEE International Conference on Advanced Science and Engineering(ICOASE), ISBN: 978-1-5386-6696-8, Oct 2018, pp.295-300.

[8] Mohammed Abdulridha Hussain, Zaid AlaaHussien, Zaid Ameen Abduljabbar and Sarah Abdulridha Hussain, "Boost Secure Socket Layer against Man-In-The-Middle Sniffing Attacks via SCPK", in Proceedings ofThe IEEE International Conference on Advanced Science and Engineering(ICOASE), ISBN: 978-1-5386-6696-8, Oct 2018, pp.295-300.

[9] J. David Brown and Triciz J. Willink, "A New Look at an Old Attack: ARP Spoofing to create loop in AD Hoc Networks", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Book Series (LNICST), Springer, ISBN: 978-3- 319-74439-1, Vol. 223, 20th Jan 2018, pp.47-59.

[10] M. Satish Kumar and B. Indrani, "A Study on Web Hijacking Techniques and Browser Attacks", International Journal of Applied Engineering Research, ISSN: 0973-4562, Vol.13, No. 5, 2018, pp.2614-2618.

[11] Nikolas Karapanos and SrdjianCapkun, "On the Effective Prevention of TLS Man-in-the-Middle-Attacks in the Web Applications", 23rd Security Symposium {USENIX} Security 14, ISBN 978-1-931971-15-7, Aug 2014, pp.671-686.

[12] S. Kumari, P. Chaudhary, C. Chen and M. K. Khan, "Questioning Key Compromise Attack on Ostad-Sharif et al.'s Authentication and Session key Generation Scheme for Healthcare Applications", IEEE Translation and Content Mining,IEEE Access, ISSN: 2169-3536, Vol. 7, Mar 2019, pp.39717-39720.

[13] Luona Yin, Aiqing Zhang, Xinrong Ye and Xiaojuan Xie, "Security-Aware Department Matching and Doctor Searching for Online Appointment Registration System", IEEE Translation and Content Mining,IEEE Access, ISSN: 2169-3536, Vol. 7, Mar 2019, pp.41296-41308.

[14] X. Liu, Jieting Lou, Hui Fang, Yan Chen, Pingbo Ouyang, Yifan Wang, Beiji Zou and Lei Wang, "A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images", IEEE Translation and Content Mining, IEEE Access, ISSN: 2169-3536, Vol. 7, Jun 2019, pp.76580-76598.

Author Biography

Dr. P. Maragathavalli

She received her B.E degree in CSE from Bharathidasan University, M.Tech. degree in CSE from Pondicherry University and PhD degree in CSE from Pondicherry University. She is working as Assistant Professor in the Department of Information Technology; Pondicherry Engineering College. She is a Life member of ISTE.

M. Seshankkumar

He is pursuing his B.Tech. degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

S. Ravindran

He is pursuing his B.Tech. degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

V.Dhivakaran

He is pursuing his B.Tech. degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.