ISSN:0975-9646

Mitigating Man in the Middle attack Using Vi-Fickle Algorithm

Vishnuganth.M[#1], Mohanraj.S[#2], Stanly Jayaprakash.J[#3]

[#3]*Head of the Department,*

[#]*Department of Computer science,*

Mahendra Institute of Technology,

Namakkal, TamilNadu, India

***Abstract*—Hectic world relies on Internet for communication purposes and are allied with one another via social network. In this consequence, Information security is the foremost need which has to be enriched. As the people made Internet to play a vibrant role in their life and anticipates high QoS, the complication also arises simultaneously. Network Eavesdropping is key threat which leads to the MITM attack. In MITM attack, Wi-Fi is the main target. Most of the people relies on Wi-Fi as they use smart devices for accessing Internet. MITM could target and succeed network eavesdropping in LAN, WLAN, HTTP, and HTTPS. This paper travels through Wi-Fi & its flaws and mitigation technique to prevent MITM.**

***Keywords*— Information security, MITM, BeEF, WLAN, Static & Dynamic algorithm.**

I. INTRODUCTION

With the escalation in the system of the internet there is an exponential upturn in the amount of the outbreaks. So there is a need of Information security in the network. With the initiation of internet today's domain is becoming more allied, so outsized number of persons, managerial, defense and government information is being communicated over the internet. Therefore there is a boundless standing of need of network security.

A. *Information Security attacks:*

Security outbreaks may be well-defined as any attempt that compromises the security of the data preserved by any party. These attacks are separated into various sorts. Some of the attacks are used to advance personnel data or system information. Further attacks are castoff to interfere with the planned role of the system. Certain attacks are used to chomp all the properties of the system unusably. Security attacks are classified as active and passive attacks. An active attack is that type of attack in which the attacker tries to alter the resources of the system or affects the operations of the system. A passive attack is that type of attack in which the attacker tries to make use of the data from the system, but does not affect the resources of the system.

1) Network Eavesdropping: Eavesdropping monitor the traffic and transmission of the information. The goal of the invader is to advance knowledge of data that is being transferred. There are many types of Eavesdropping attacks in that MITM is the key threat to data and information.

2) MITM & WLAN: MITM attacks that involve the monitoring and alteration of the data or involve the forming of the dishonest data stream. Some attacks are MITM and MITB (Man in the browser attacks).Where for these attacks, WLAN paves way easily. The security methods in WLAN system are weaker and hence considered as weaker than the LAN.

3) Smart devices: Smart devices such as Smart watches, Tablets, Smart phones, Smart glasses (GOOGLE GLASS) etc., are ruling the current world scenario and which also reduces the work complexity of people. Most of the smart devices works on android and also some other operating systems like iOS, Windows etc. Where these devices cannot access internet via LAN connection instead of they depend upon the WLAN and Mobile networks for network connection, which makes the attacker's work more easier as attacker could break the security of WLAN easily, he also could breach the security of the smart devices easily using some Backdoor attack, Trojan and BeEF.

II. PROBLEM DEFINITION

The most of the general public having smart devices where they trust on using Wi-Fi and in some cases it would be public Wi-Fi, which is not secure. Thus the usage of Wi-Fi paves way for the intruder, when people start performing any transactions or get into their private data or connecting to any of social networks, then their credentials and private data are no longer harmless. This is because of the deficiency of proper security implementations.

III. SSL SYMMETRIC V/S SSL ASYMMETRIC

In detection application of malicious attacks and intrusion, the main problem which arises is the complexity and the time efficiency. However the proposed system which is explained below must implement the key generation in the SSL which could be Symmetric or Asymmetric. In case of the Symmetric key there occurs the exchange of public key to both the end whereas in the Asymmetric concept it has to use public key for encryption and private key for decryption. Though the Asymmetric concept stands a bit ahead of Symmetric on the basis of security, but it is a complex and time in-efficient process. As, the proposed system provides very strong and unique security method it is processed with Symmetric key algorithm for efficient process.

IV. PROPOSED MODEL

The Vi-Fickle algorithm is being developed on the need of dynamic process in encrypting techniques. Vi-Fickle algorithm is named after its inventor 'Vishnu'-Vi and 'Fickle' means 'Changing frequently'. The process is to yield the mockup of the conception which would be

simulated with SSL Symmetric key algorithm for simpler reproduction. The basic idea is to afford more intricate security heightening which makes the undertaking of cryptanalyst even more challenging to decrypt the cipher text.

This encryption algorithm will keep on changing for every successful process completion. As it is processing with SSL Symmetric key, it would also protect the browser from unwanted redirection and doesn't allows the browser to download trustless file or malicious files.

- Enhanced protection
- Warns on malicious sites
- Blocks malicious file downloads
- Assures secure transaction
- Improved protection against cryptanalyst
- High QoS with high security

A. *Vi-Fickle Algorithm*

In this model, the key generation concept is based on producing unique keys for the life time with unique keys for each day in a lifetime of the process. The formula involves the process of both encryption and decryption process of Cipher text and Plain text.

$$C_p = K+E_e(P_l),$$

$$P_l = [K-E_e(P_l)]\ Dd,$$

Where $K= C_1 + S_{1....s}\ , C_2 + S_{1....s}\ \dots\ C_n + S_{1....s.}$

TABLE I

REPRESENTATIONS OF NOTATIONS USED IN THE MODEL

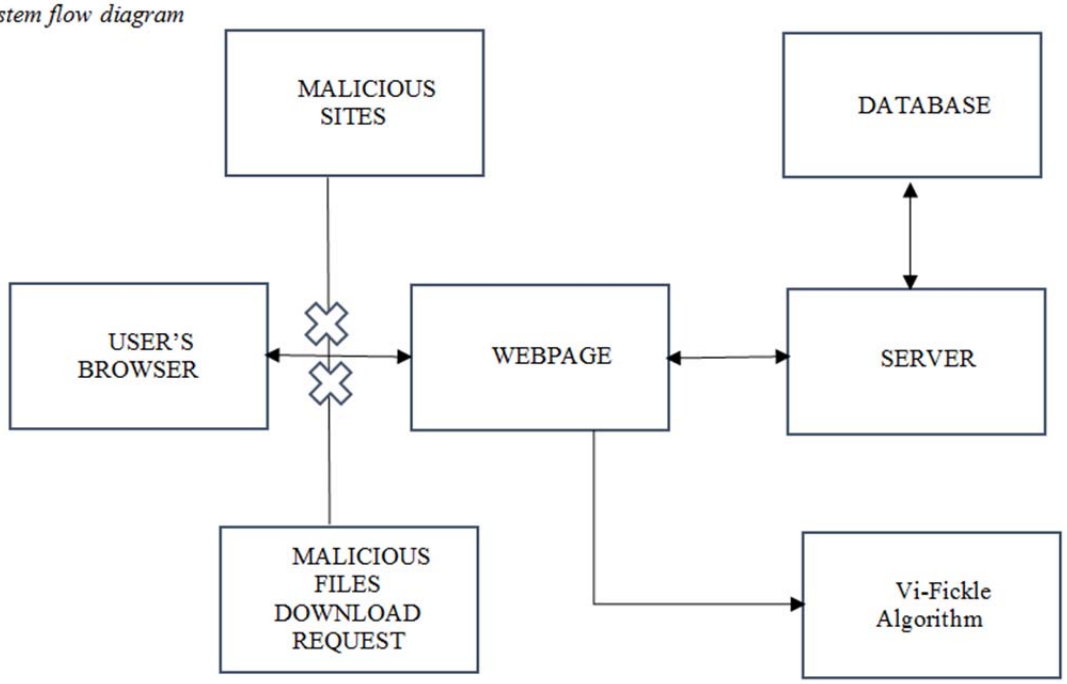
Notations	Descriptions
E_e	Encrypted text
C_p	Cipher text
D_d	Decrypted text
P_l	Plain text
s	No of combinations (S).
n	No of combinations (N)
K	KEY
E	Encryption logic
N	String (Key)
S	Subset (N)
D	Decryption logic

B. *Overview of the Algorithm*

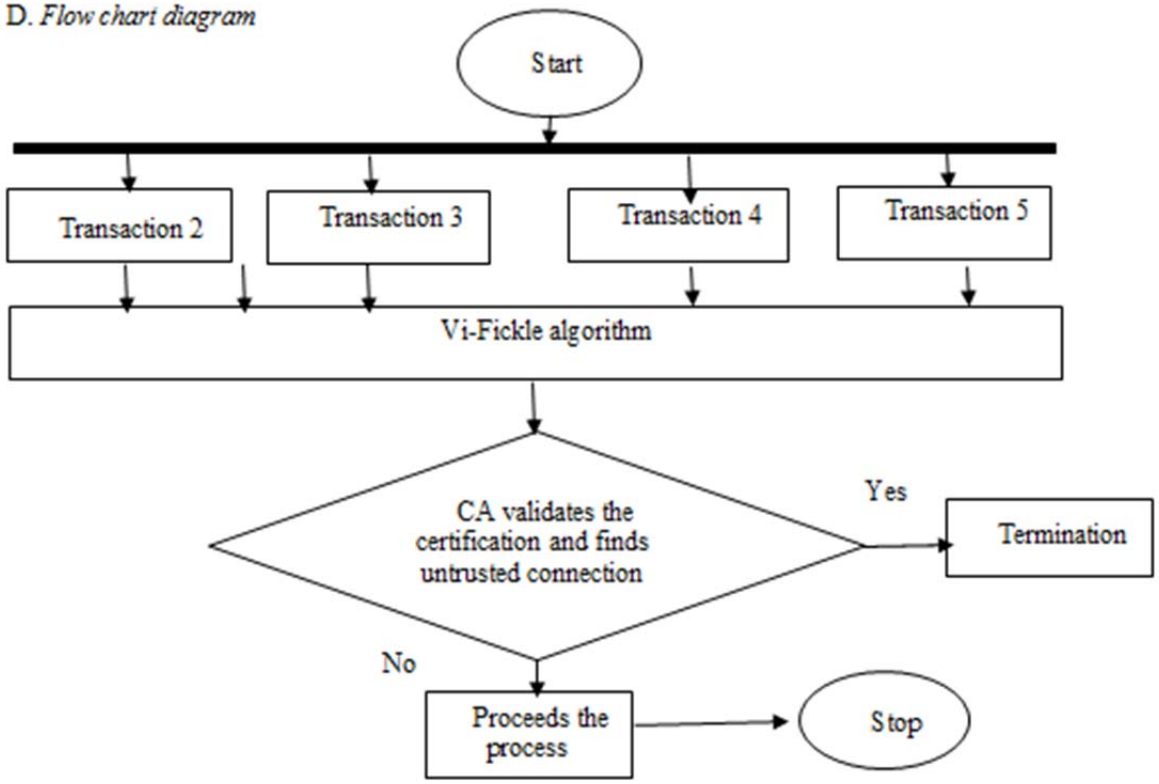
- Step 1: Generate String(N) and combinations (KEY)
- Step 2: KEY with Subset combination [$(K= C_1 + S_{1....s}\ , C_2 + S_{1....s}\ ,\dots, C_n + S_{1....s}\ )$]
- Step 3: Convert plain text to encrypted text [$(E_e(P_l))$]
- Step 4: Convert as Cipher text [$C_p = K+E_e(P_l)$]
- Step 5: Decryption process to get back the Plain text [$P_l =[\ K-E_e\ (P_l\ )]D_d\ ]$

The actual process of the Vi-Fickle algorithm is that it creates unique keys on the basics of given string, where both the combinations and subsets of the string is used for the unique key generation. The lifetime of the key is calculated using the length of the string and as the first achievement is gaining unique keys for entire life time from the combinations of the string and then for providing more uniqueness the subsets are created which are used on the 24 hour basis which basically makes the unique key as even more unique and dynamic and then the encryption & decryption logic which is used along with the key to convert cipher to plain and vice versa from the given input.

C. *System flow diagram*



D. *Flow chart diagram*



V. CONCLUSION

In the last two eras there has been a remarkable intensification in the rate of the attacks over the internet. One of the supreme donor to this rate is the Man in the Middle Attacks. The Vi-Fickle algorithm will be very tricky and difficult to decrypt and hence it keeps away the data from the cryptanalyst and as it uses SSL Symmetric key technique, hackers cannot perform MITM. This project also gives a clear vision on the vulnerabilities and threats in the WLAN and also usage of smart devices and also creates awareness on common attacks. By using this concept lots of spell is saved and we could able to detect the malicious things in a petite extent of time. The items that are non-harmful are permissible to go through without blocking them.

REFERENCES

[1] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici,S. Dolev, and C. Glezer. Google Android: A Comprehensive Security Assessment. IEEE Security & Privacy, 8(2):35 –44, Mar. 2010.

[2] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?" IEEE Computer, vol. 41, no. 5, 2008.

[3] J. Anderson, J. Bonneau, and F. Stajano. Inglorious Installers: Security in the Application Marketplace. In Proceedings of the 9th Workshop on the Economics of Information Security, 2010.

[4] J. Bickford et al., "Rootkits on Smart Phones: Attacks, Implications and Opportunities," in Workshop on Mobile Computing Sys. and Appl. (HotMobile'10). ACM, 2010.

[5] Egele, M., Kruegel, C., Kirda, E., Vigna, G.: Pios: Detecting privacy leaks in iOS application. In: Network and distributed System Security Symposium (2011).

[6] E. Rescorla, "HTTP Over TLS‖," IETF RFC 2818, www.ietf.org/rfc/rfc2818.txt Last Accessed on February 3, 2010

[7] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol‖," IEEE Security and Privacy, vol.7, Jan-Feb. 2009, pp. 78-81, doi: 10.1109/MSP.2009.12

[8] D. Kristol and L. Montulli,"HTTP State Management Mechanism‖," IETF RFC 2965, www.ietf.org/rfc/rfc2965.txt Last Accessed on February 3, 2010

[9] J. Katz and Y. Lindell, "Introduction to Modern Cryptography: Principles and Protocols" Chapman & Hall/CRC Press, 2007, ISBN: 978-1584885511

[10] X. Liu, J. M. Kovacs, C.T. Huang, and M. G. Gouda, "A Secure Cookie Protocol‖," In Proceedings of 14th Computer Communications and Networks, San. Diego, California, USA, 2005

[11] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50

[12] Computer and Network security by ATUL KAHATE

[13] Fundamentals of Computer Security, "Basic Cryptographic Algorithms" in www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms

[14] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

[15] "Introduction to Public-Key Cryptography", an article available at developer.netscape.com/docs/manuals/security/pkin/contents.htm