ISSN:2229-6093

B Eshwar et al, International Journal of Computer Technology & Applications,Vol 8(2),282-290

Secure Packet Transmission Against Pilot Spoofing and Phishing Attack

B. ESHWAR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING CHENNAI

e-mail: eshwarbillakanti1609@gmail.com

GVS .RUPESH

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING CHENNAI

e-mail:rupeshrupee690@gmail.com

ABSTRACT

The pilot spoofing attack is one kind of active eavesdropping activities conducted by a malicious user during the channel training phase. By transmitting the identical pilot (training) signals as those of the legal users, such an attack is able to manipulate the channel estimation outcome, which may result in a larger channel rate for the adversary but a smaller channel rate for the legitimate receiver. With the intention of detecting the pilot spoofing attack and minimising its damages, we design a two-way training-based scheme. The effective detector exploits the intrusive component created by the adversary, followed by a secure beam forming-assisted data transmission. In addition to the solid detection performance, this scheme is also capable of obtaining the estimations of both legitimate and illegitimate channels, which allows the users to achieve secure communication in the presence of pilot spoofing attack.

Phishing attacks were highly concentrated in targeting at a few major Websites. In this project, the machine learning based phishing detection using only lexical and domain features, which are available even when the phishing Web Pages are inaccessible. We then select an optimal set of features in our phishing detector, which has achieved a detection rate better than 98%, with a false positive rate of 0.64% or less. The detector is still effective when the distribution of phishing URLs changes.

Key words: Spoofing, Phishing, eavesdropping, validation.

ISSN:2229-6093

INTRODUCTION

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network.

LITERATURE SURVEY:

Keerthy K Murali, Abhisha Devi C M

The convenience of wireless network is very high. But we must realize the fact that they are very unsecure. For example wireless networks are susceptible to identity based attack such as spoofing attacks. Conventional cryptographic schemes are the techniques for the secure communication in the presence of third parties called adversaries but it require huge infrastructure and computational overhead. However, as the internet grew and computers became more advanced, high quality encryption techniques became well known around the globe. This paper describes survey on pilot spoofing attack detection in wireless networks. Spoofing attack is one kind of active eavesdropping conducted by a malicious user, in which one person or program can successfully falsify the data of another for illegitimate advantage. One of the best examples of spoofing attack is pilot spoofing attack. The pilot spoofing attack could also weaken the received signal strength at the legitimate receiver if the eavesdropper utilizes large enough power

T C Deepthi, Jenelin S S

The Pilot spoofing attack is a kind of eavesdropping conducted by malicious users while transmission takes place between a legitimate transmitter and a legitimate receiver. Here the eavesdropper spoofs the legitimate transmitter on the estimation of Channel State Information (CSI) by sending the identical pilot signal as the legitimate receiver, in order to obtain larger information rate in the data transmission phase. The pilot spoofing attack would reduce the strength of the received signal at the legitimate receiver when the eavesdropper utilizes large enough power.So, an Energy Ratio Detector(ERD) is proposed to help the legitimate users to detect and locate such attacks. This Energy Ratio Detector detects the existence of pilot spoofing attack by exploring the asymmetry of received signal power levels at the legitimate transmitter and thelegitimate receiver when there exists a pilot spoofing attack

Yong Zeng and Rui Zhang

This paper studies a new active eavesdropping technique via the so-called spoofing relay attack, which could be launched by the eavesdropper to significantly enhance the information leakage rate from the source over conventional passive eavesdropping. With

this attack, the eavesdropper acts as a relay to spoof the source to vary transmission rate in favor of its eavesdropping performance by either enhancing or degrading the effective channel of the legitimate link. The maximum information leakage rate achievable by the eavesdropper and the corresponding optimal operation at the spoofing relay are obtained. It is shown that such a spoofing relay attack could impose new challenges from a physical-layer security perspective since it leads to significantly higher information leakage rate than conventional passive eavesdropping.

Shyam Jadhav, Yogesh Katke, Vaibhav Joshi, Sagar Thore

Wireless network are openness in nature and it is easy for spoofing attacker to launch wireless spoofing attackers which causes threat for data security and impact performance of a network. In conventional security cryptographic authentication is used to verify the nodes which are not desirable because of network overhead requirement. In this paper I use special information, that is a physical property associate with each node, which is very hard to falsify, and it does not depend on cryptography. This physical property can used for detecting spoofing attacker present in the network, determining the number of attacker when multiple adversaries masquerade as the same node identity as that of other node and localizing multiple adversaries. Then the problem of determining the number of attackers as multiclass detection problem is formulated. Cluster-based mechanisms are developed to determine the number of attackers.

PROPOSED METHODOLOGY

1. **EXISTING SYSTEM**:

Most of the existing works on physical-layer security have assumed the theoretical setup with passive eavesdroppers only. In practice, the eavesdropper could launch proactive attacks to enhance their eavesdropping performance, a technique known as active eavesdropping.

We are having the system which can secure the data against phishing at one of the levels and we don't have a highly secure system to detect Phishing URL's.

2 PROPOSED SYSTEM:

In this project, we are trying to propose a new system model which will guarantee a system where the attacker couldn't hack the user's data.

The techniques implemented in this system are too simple and strong for the user and hard for the hacker to break.

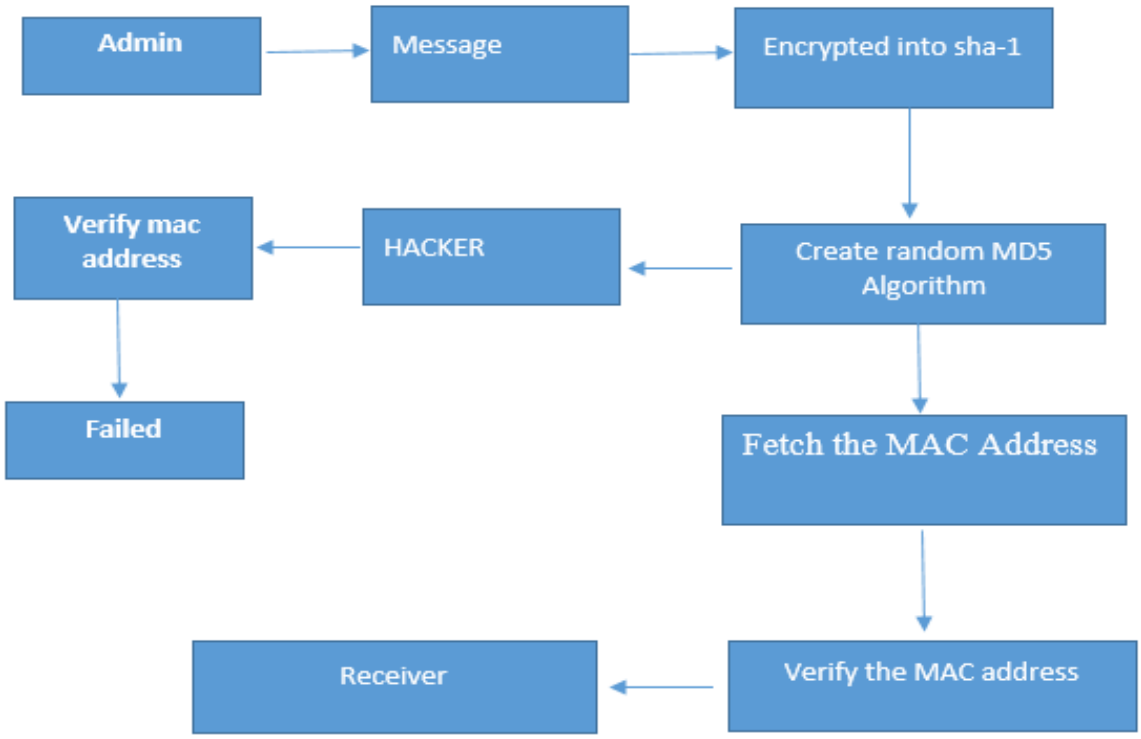
We propose fundamentally modified pilot signal design and estimation process, the former suggested to transmit two random phase-shift keying (PSK) symbols as the pilot signal and tried to detect the pilot spoofing attack based on the phase difference of

those two symbols. Later a new discriminatory channel estimation method and claimed to be secure from the pilot spoofing (contamination) attack by randomly choosing the newly designed stochastic pilot signals.

We are trying to address some of the huge issues like, Title Based Crawler to crawl all the URLs matching with the Title name, Implementing URLs Scanning Method using Different types of Scan Engine Like AVG, Norton's, McAfee to Detect the Phishing URLs.

ISSN:2229-6093

SYSTEM ARCHIECTURE:

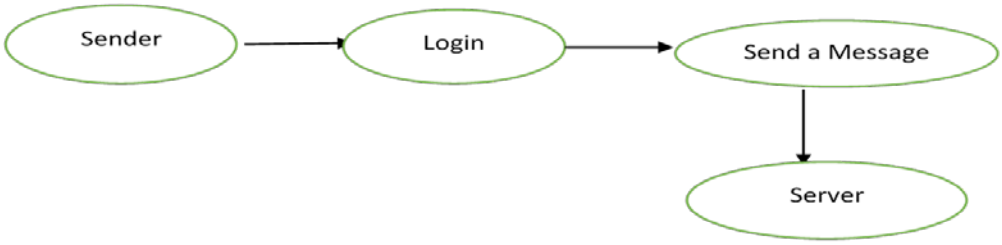


ISSN:2229-6093

MODULES FOR PILOT SPOOFING ATTACK:

Cookie Management :-

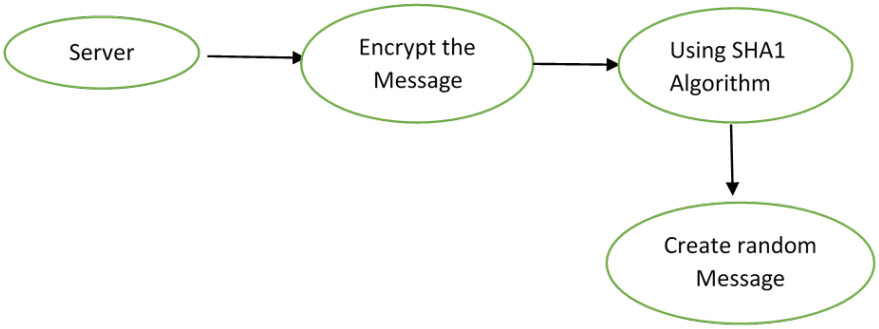
Where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie. Many web sites use SSL encryption for login pages to prevent attackers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows attackers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this data includes the session cookie, it allows him to impersonate the victim, even if the password itself is not compromised.



RANDOM ENCRYPTION:

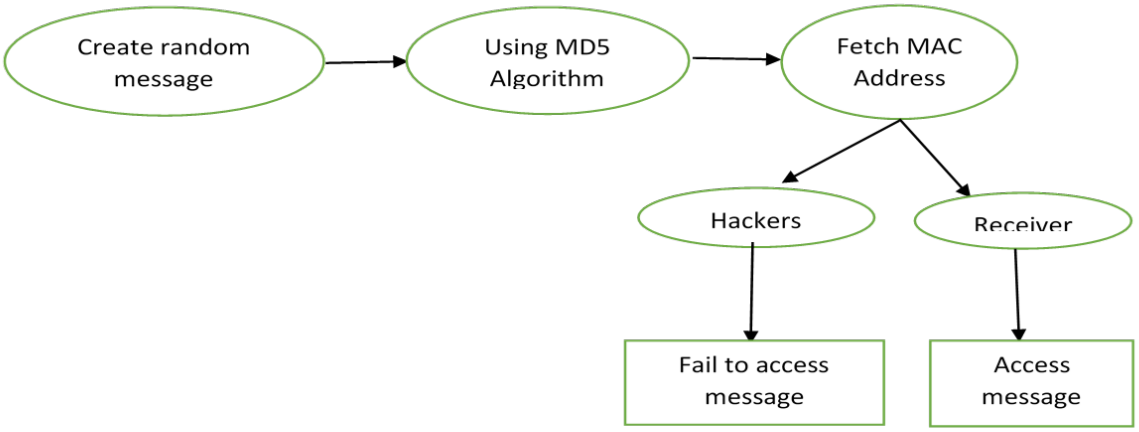
A Random encryption, or just cookie for short, is a token or short packet of data passed between communicating programs, where the data is typically not meaningful to the recipient program. The contents are opaque and not usually interpreted until the recipient passes the cookie data back to the sender or perhaps another program at a later time. The cookie is often used like a ticket – to identify a particular event or transaction.

ISSN:2229-6093



MAC ADRESS VALIDATION:

To prevent packet sniffing, a special technique is proposed under which, using random encryption to prevent this packet sniffing. Random encryption is not like a normal encryption which gets the MAC address of the machine and it convert the MAC address into some encrypted format and with enables the session maintenance .



MODULES FOR PHISHING ATTACK:

EXPLORE THE WEB PAGE SOURCE CODE:

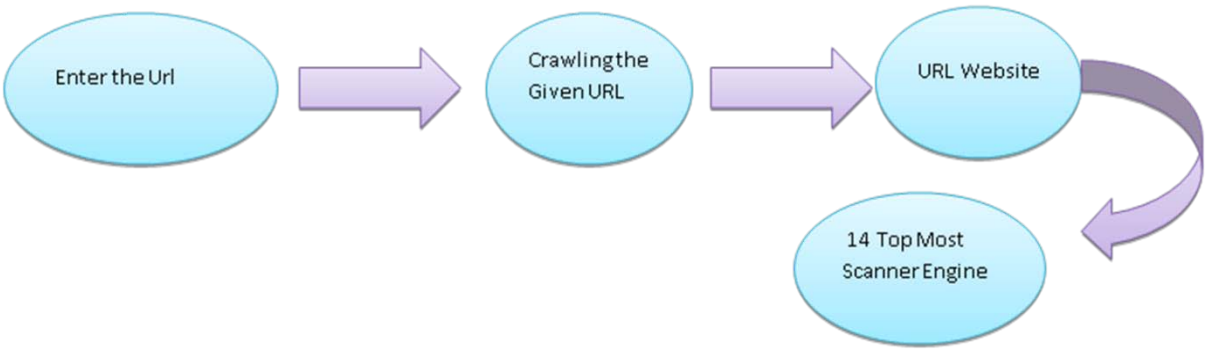
The search engine where we can search the URL of particular website, which needs to scan, and will call the Anti-Malware engines to perform the operations.

ISSN:2229-6093

SCAN THE INBUILT URL'S:

Scans the given URL according to Anti-malware engines in Explore module, are to be called, in which URL has filtered and, finds the vulnerable links if available in those pages.

Advantage is able to scan twenty different malware engines together, so we can catch the vulnerable links easily



FINALIZE WITH REPORT:

We conclude that the given URL with rating is injected or not by the scan results and, can block the link if it is injected.

CONCLUSION:

In this study the phishing url's and spoofing attack are avoided using sha1and md5 algorithms, few techniques which detects phishing links with the help of html, php, sql server.

REFERENCES:

1] W. Stallings, Cryptography and Network Security: Principles and Practice, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.

[2] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[3] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[5] S. fieShae and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2007, pp. 2466–2470.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[7] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," IEEE Wireless Commun. Lett., vol. 3, no. 4, pp. 357–360, Aug. 2014.