International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 7, Issue 3
March 2018

Secure Transmission against Pilot Spoofing and Phishing Attack

[1]Anusha Ramprasad, [2]Jayavarshini Thirumalai, [3]Jhon Sneha Arokia Sundaram,
[4]Manjana Karthikeyan
Valliammai Engineering College

ABSTRACT:*The openness of wireless and sensor networks offer tempting target for malicious attacks, especially vulnerable to spoofing attacks. Spoofing attack poses a serious threat as they represent a form of identity compromise. Malicious data attacks have raised widespread concerns on data integrity and security of cyber-physical systems. The process of transmitting the data packets with forged source address is known as IP spoofing. By altering the target addresses, attackers can easily change the target from one destination to another. Phishing attack is a method of tricking users into unknowingly providing personal and financial information or sending funds to attackers. It uses some form of electronic messaging such as email to provide a link to what appears to be a legitimate site but is actually a malicious site controlled by the attacker. Phishing is a hybrid attack combining both social engineering and technological aspects and combatting phishing attacks requires dealing with both aspect The phishing websites have been detected by analysing the URL site checker and malicious external links in the website which transmits the user data to an external server. This assures that even when the distribution of phishing URLs changes, the detector remains effective. The prevention of these two attacks can be attained using NA Algorithm.*

KEYWORDS:Electronic messaging, Site checker, Pilot spoofing attack, Phishing attack, NA .

I. 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 and phishing 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 phishing and eliminate them from the network.

II. SPOOFING

The pilot spoofing attack is one reasonably active eavesdropping activities conducted by a malicious user throughout the channel training phase. By transmission the identical pilot signals as those of the legal users such an attack can able to manipulating the channel estimation outcome, which may result in a huge channel rate for the adversary but a small channel rate for the legitimate receiver. The proposed system has an intention for detecting the pilot spoofing attack and minimizing its damages, a tendency to style a two way training based scheme is introduced. An effective detector exploits the interfering element designed by the adversary, followed by a beam forming assisted data transmission. In addition to the solid detection performance, this scheme is also able to get the estimations of each legitimate channel. The cookies are analyzed and MAC address is generated.

III. PHISHING

Phishing is a form of identity theft that occurs when a malicious Web site impersonates a legitimate one in order to acquire sensitive information such as passwords, account details, or credit card numbers. Though there are several anti-phishing software and techniques for detecting potential phishing attempts in emails and detecting phishing contents on websites, phishers come up with new and hybrid techniques to circumvent the

available software and techniques. Phishing is also known as brand spoofing or carding.The phishing attacker's trick users by employing different social engineering tactics such as threatening to suspend user accounts if they do not complete the account update process, provide other information to validate their accounts or some other reasons to get the users to visit their spoofed web pages.

IV. ATTACKER

An attacker is a skilled computer programmer who breaks or hacks a password code and gains remote access to a protected computer system. It also performs criminal actions such as alteration or stealing of data, or transfer of funds. In the existing system, the attacker spoofs the IP address of the victim and thereby either modifies or performs other illegal activities with the obtained information. They also gain access to the user's personal detail by the means of the phished link.

V. SECURITY MANAGER

Security managers are responsible for protecting their organization's computers, networks and data against threats, such as security breaches, computer viruses or attacks by cyber-criminals. It enhances security in an organization and is used to assess and implement security for parts of an IT setup, for networks. In the proposed system, if any spoofing activities take place, the security manager immediately blocks the IP address and MAC address of the attacker thereby protecting the data. Security manager also checks the link received by the user from an unknown sender. It compares the received link with the legitimate link in DNS server and if the link is a legitimate one, it will be added to the whitelist and user is granted access; else it will be added to the blacklist and the link gets blocked.

VI. COOKIE MANAGEMENT:

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. Unsecured Wi-Fi hotspots are particularly vulnerable, as anyone sharing the network will generally be able to read most of the web traffic between other nodes and the access point.

VII. 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. It is used to prevent packet sniffing.

VIII. MAC ADDRESS VALIDATION:

MAC address validation is a verification process performed on each incoming packet to prevent spoofing on IP based interface. When an incoming packet arrives on an interface, the validation table is used to compare the packet's source IP address with its MAC address. If the MAC address and IP address match, the packet is forwarded; if it does not match, the packet is dropped. To anticipate packet sniffing, an extraordinary procedure which utilizes arbitrary encryption is used. Random encryption gathers the MAC address of the machine and changes over the MAC address into scrambled arrangement and empowers session upkeep.

IX. LINK GUARD:

Link guard works by analyzing the differences between the visual link and the actual link. It also calculates the similarities of a URL with a known trusted site. In main routine link guard, it first extracts the dns names from the actual and the visual links. Then It compares the actual and visual dns names, if these names are not

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 7, Issue 3
March 2018

the same, then it is phishing. If dotted decimal IP address is directly used in actual dns, it is then a possible phishing attack. Analyze DNS and the related subroutines are depicted in Analyze DNS, if the actual dns name is contained in the blacklist, then we are sure that it is a phishing attack. Similarly, if the actual dns is contained in the white list, it is therefore not a phishing attack.

X. PATTERN MATCHING:

Pattern matching is designed to handle unknown attacks (blacklist/whitelist is useless in this case).phishing attacks, all the information we have is the actual link from the hyperlink (since the visual link does not contain DNS or IP address of the destination site), which provide very little information for further analysis. In order to resolve this problem, we extract the sender email address from the e-mail. Since phishers generally try to fool users by using (spoofed) legal DNS names in the sender e-mail address, we expect that the DNS name in the sender address will be different from that in the actual link. Second, we proactively collect DNS names that are manually input by the user when she surfs the Internet and store the names into a seed set, and since these names are input by the user by hand, we assume that these names are trustworthy. Pattern Matching then checks if the actual DNS name of a hyperlink is different from the DNS name in the sender's address, and if it is quite similar (but not identical) with one or more names in the seed set by invoking the Similarity procedure.

XI FIGURE:-

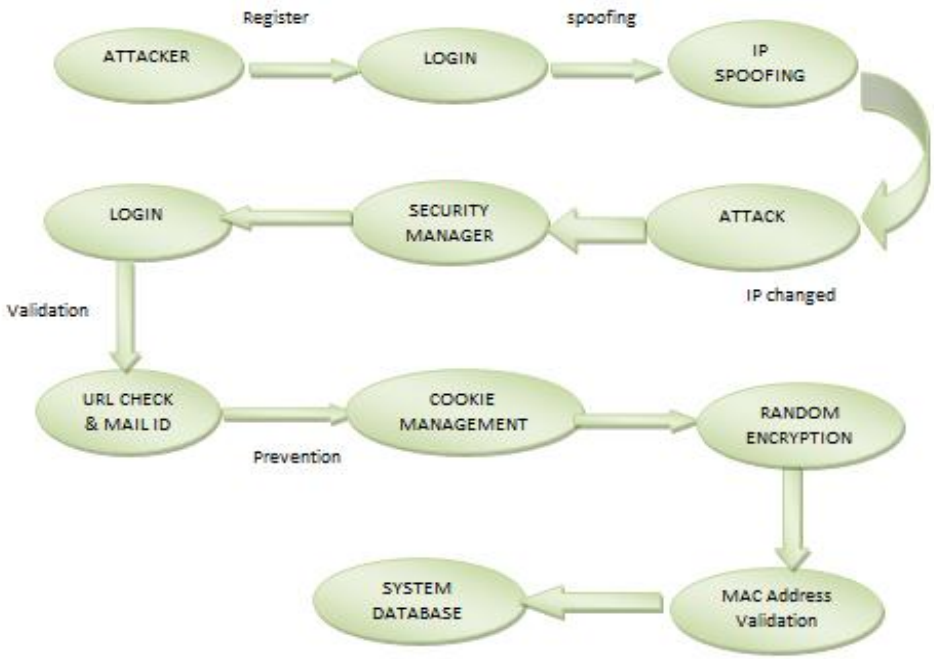


FIG:ARCHITECTURE DIAGRAM FOR SPOOFING

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 7, Issue 3
March 2018

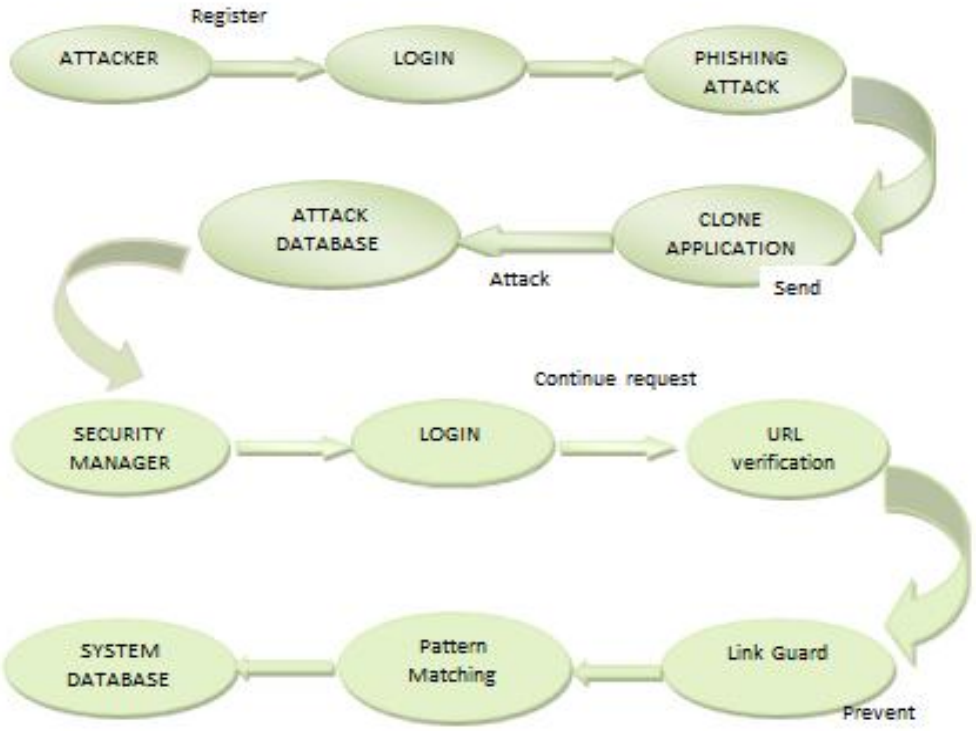
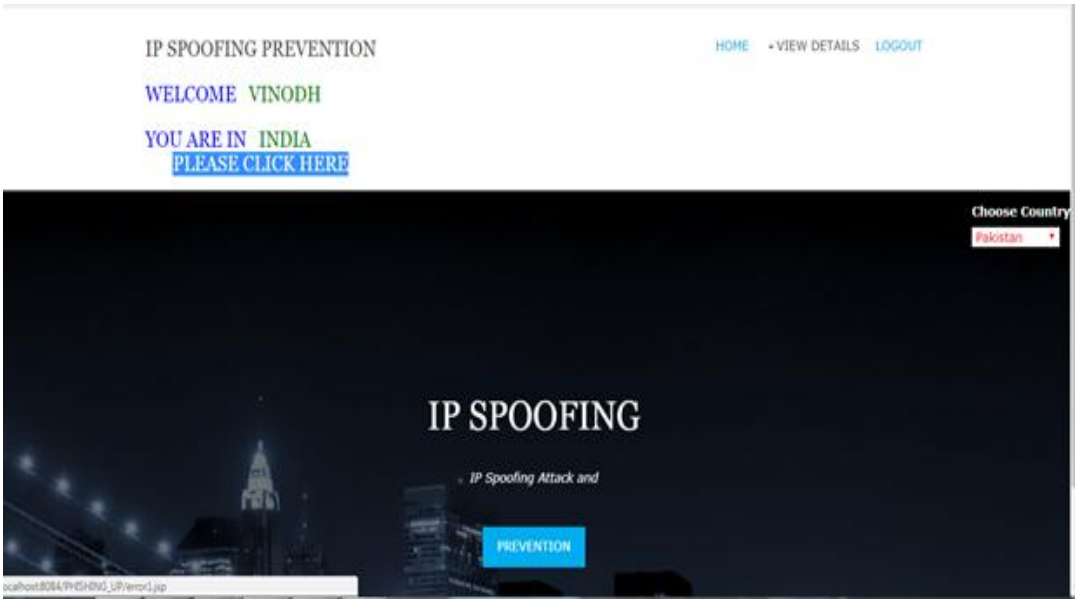
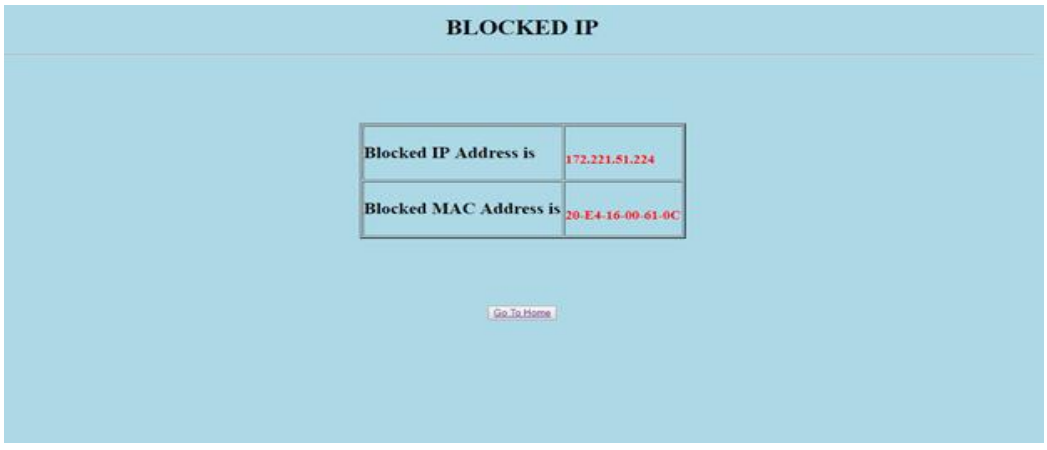


FIG:ARCHITECTURE DIAGRAM FOR PHISHING

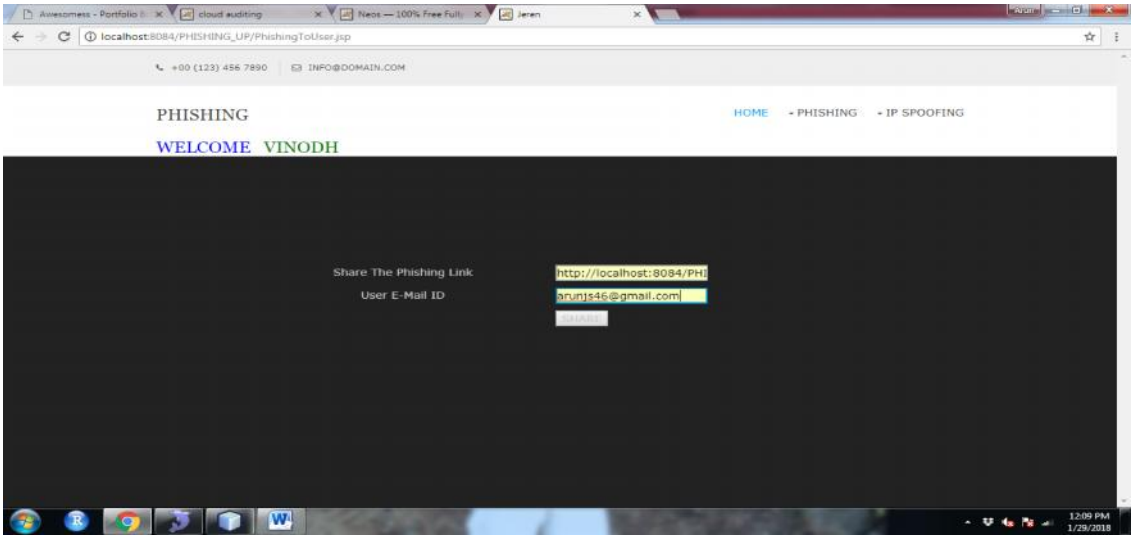
XII RESULT:

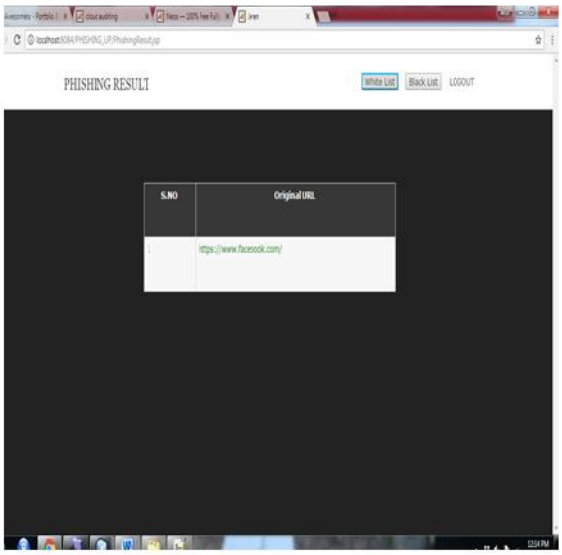
International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 7, Issue 3
March 2018

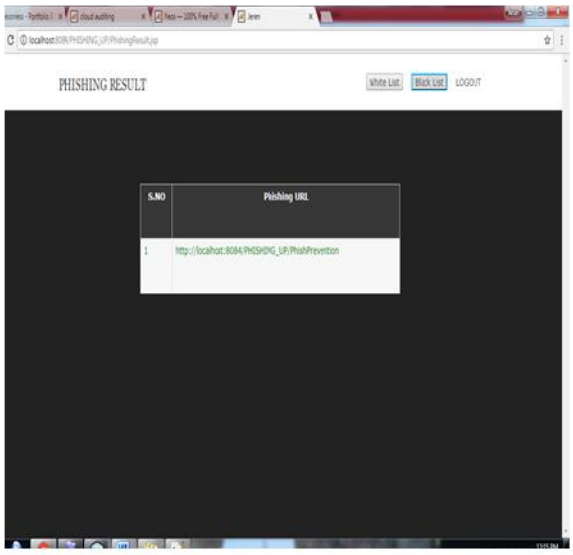




International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 7, Issue 3
March 2018







REFERENCES

[1] Keerthy k Murali, “A study on pilot spoofing attack detection,” IJRCCE.,vol.4,issue 7, July 2016.
[2] Yong Zeng and Rui Zhang, “Active eavesdropping via spoofing relay attack,”,2015.
[3]Ram Basnet. SrinivasMukkamala and Andrew H.Sung, “Detection of Phishing attacks:A Machine Learning approach,”,2008.
[4] XiaowenTian and QianLiu“Random-Training-Assisted Pilot Spoofing detection and secure transmission,”, IEEE Trans. Inf. Theory,Sep.2016
[5] AlwarRangarajan, RajendranSugumar, and ChinnappanJayakumar, “Secure verification technique for defending IP spoofing attacks,”,The international Arab journal of information technology,Vol.13,March.2016