IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

MAC Spoofing Detection and Prevention

Ananth Hegde[1]

Master of Technology, Information Technology, International Institute of Information Technology, Bangalore, India[1]

Abstract: As we all know, wireless networks are spread at each and every part of the world, starting from home to large organizations, governments, etc. The exponential growth in the deployment of wireless access networks (WLAN) makes them an attractive target for attackers. Wireless networks are vulnerable to identity spoofing attacks when a hacker/attacker can forge the MAC address of his wireless device to impersonate another device on the network. Unlike IEEE 802.11 data frames, management frames which carries MAC address are not encrypted, which makes source authentication difficult. Several techniques exists to detect MAC spoofing such as Sequence number analysis, Radio signal strength based detection, dynamically changing MAC etc. All of these techniques can wrongly classify malicious user to bean authenticated one. In this paper, we propose a reliable and robust algorithm based on smart antenna technology and shared key exchange techniques to detect and prevent MAC spoofing.

Keywords: Access Points, Dos, WLAN, CSI, MIMO.

I. INTRODUCTION

MAC Spoofing is a hacking technique of changing MAC address of a networked device to a different one. The changing of the MAC address allows the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer. Each network devices is Identified by unique address called MAC address which is burned into Network Interface (NIC) cards.

The MAC spoofing doesn't mean that we have wrote the new MAC on the chipset of the Ethernet card but the MAC Spoofing is the way to change MAC details from the hardware configuration structure of the operating system. When the OS is initially loaded, MAC address is picked from NIC card and Saves it in the registry key and there after it picks the MAC address from registry key. It is very easy to change the value of MAC address in registry key. There are many tools and commands available.

MAC spoofing becomes the biggest threat for cyber investigation agencies. To approach any target system the investigation agencies try to recover the IP address and the MAC address, where the IP address can be changed or spoofed easily as an option defined in every Operating Systembut at least the Investigation agencies can rely on MAC because it's a worldwide unique Address mounted on the Ethernet Chipset but this technology becomes the major threat and vulnerability for them to approach to the exact target system [1]. MAC spoofing is one of the root cause for DOS attacks, Man in the middle attack, DNS poisoning, ARP poisoning etc.

Authentication is essential in today's modern computer and communication systems. One of the widely used authentication technique is address-based authentication which assumes that the identity of source could be inferred based on the network address from which packets arrive. WLAN standards fails to address the authentication of 802.11 Management frames and NIC addresses, it is possible for adversaries to spoof the identity of legitimate WLAN nodes with the available of sophisticated tools which sniffs the authenticated packets over the air to steal MAC address. In case of wired Ethernet LAN users needs to have physical access to the port that the user is registered to. Otherwise the port security mechanism of the switch blocks the packets.

Rest of the paper is organized as fallows. Section II gives background on WLAN. Section III provides working principle of WLAN. Section IV presents vulnerabilities and attack scenarios. Section V gives overview of existing methods and its disadvantages. Section VI presents our approach. Section VII describes our system model and algorithm and section VIII concludes the topic.

II. BACKGROUND ON WLAN

In this section we describe WLAN infrastructure and its authentication process and different modes of operation

A. WLAN Infrastructure

In a typical WLAN infrastructure. All nodes communicate through central node (Access Points). Access Points can be connecting to another Access Points in a distributed manner. Access Point also serves as a gate way to access other networks.

B. WLAN Authentication Process

In a typical WLAN infrastructure. Every node in WLAN network starts communication after it is authenticated with Access Point (AP). Below are the steps performed by the node in authenticating itself with the Access Points.

- Node first sends authentication frame to Access Points. Access Points responds with the frame of type success.
- There may be multiple Access Points in the range of client, it may receive authentication response from more than one Access Point's, In order to associate with nearest AP (i.e. the one which has strongest signal) the node send association frame to the chosen AP. AP responds with the association response.
- Node starts communication with the access point.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

- Communication continues until node or AP sends a de authentication frame. Optionally, disassociation frame requesting to return back to authenticated unassociated state.

III. WORKING PRINCIPLE

The working principle of MAC authentication changes with respect to whether it is used alone (Mode 1: open authentication) or as a way to augment other authentication methods (Mode 2: two-factor authentication). Below, we assume that AP forwards the requests from the clients to an authentication server which checks the requests centrally. Using MAC authentication WLAN works in two phases a) Registration b) Operation.

A. Registration

In an organization or an institution, authenticated users MAC address is stored in a centralized server. For example in a universities all the students MAC address will be collected and registration is made in the server after verifying student's identity. Registration can be offline or online.

B. Operation (Mode 1)

Since MAC authentication is not specified as part of the 802.11 standard, we have a variety of options to implement it. Here, we prefer to explain the one implemented in Cisco and various other companies products. Upon receipt of a beacon from an AP, the wireless node sends its authentication frame. Upon receipt of this frame, the AP simply sends a response frame of type success because open authentication is used. Then, the node sends its association request frame. At this point, the AP asks to the authentication server whether the source MAC address on the frame is listed in its authorized address list. If it is, upon receipt of an accept response from the server, it responds to the node with an association success frame and switch to the authenticated associated state. Otherwise the node is rejected by sending a failure type of association response [2].

C. Operation (Mode 2)

In this case, registration phase is as same as Mode 1 but the procedure to give the access permission decision is expanded. For instance in case when there is a challenge response authentication based on a shared key (as in WEP), response to an authentication request would be of type challenge (not type success). The client returns back an encrypted challenge and only if this encrypted challenge is decrypted successfully by the server, the state is changed to authenticated-unassociated and a success message is sent. The rest of the operation is similar to the one explained in mode 1 [2].

IV. VULNERABILITIES AND ATTACK SCENARIOS

The IEEE 802.11 MAC-layer was especially designed to meet all requirements of a wireless network. In particular the ability to discover networks, and coordinate access to the radio medium. Today, we know that most link layer attacks on WLAN networks are DoS attacks based on these extended functionalities. These attacks mainly affect the availability of WLAN services - optionally for a dedicated target or the whole network. Sometimes, a DoS is only the first step in a more sophisticated attack that in the worst case could lead to the theft of authentication credentials like usernames and passwords. The next sections describe the vulnerabilities and the attack scenarios that might arise [3].

D. De-Authentication Attack

To join a wireless network a client has to choose an access point and authenticate itself to it before any further communication may start. This authentication protocol also includes a message that allows nodes to de-authenticate from each other with one single message. Unfortunately this message is in no way protected against spoofing. So anybody can send this message with a forged identity. As a consequence the attacked client will not receive further messages unless it re-establishes authentication. With one single de-authentication message the attacker provokes six messages for the re-authentication between the attacked client and the access point. If this attack is replayed periodically a victim could be kept from joining the network indefinitely.

E. Disassociation Attack

In an environment with multiple access-points available, each client may be authenticated with more than one access point if they overlap. The state of association was introduced to allow the access points to agree who has the responsibility for forwarding packets to the client. As with authentication, one single message allows the client or an attacker to disassociate. Exploiting this vulnerability is functionally identical to the de-authentication attack. The impact is slightly weaker due to the fact that the reestablishment of the association needs less effort than re-authentication.

F. Access Point Spoofing

Unlike the previous vulnerabilities the following two attacks do not directly rely on flaws in the IEEE 802.11 MAC layer specification but rather in completely faking the AP's identity. If an attacker is able to spoof the identity of an AP he might lure clients into connecting to the fake AP instead of the legitimate one. The attacker only needs to emit a stronger signal than the legitimate AP. In many cases, public WLANs use web portals for user authentication. The attacker now might redirect the client to a faked web portal and steal the client's username and password. Alternatively the attacker can implement active man-in-the-middle attacks against SSH and HTTPS sessions.

Now, let us see what is different when two-factor authentication is in place (mode 2). Similarly, the attacker needs to capture the traffic and learns some authorized MAC addresses first. However in this case it is not possible for him to wait till one of the authorized users quits. Because when a user quits, his communication returns back to the initial state where no frame is forwarded by the access point. To change the state back again to authenticated-associated, the attacker needs to authenticate himself successfully. Since the attacker does

not hold the credentials for this authentication, the MAC address he has captured is useless after the authorized user quits the session. Therefore, the attacker should act while the authorized user continues communication with the access point. Attacker can launch a DoS attack against the authorized user and cause his machine to crash. Before the crashed machine boots up, for a short period of time, the attacker has the capability to bypass the authentication by changing his MAC address with the MAC of the crashed machine and impersonates himself to the access point. As far as mode 2 is concerned, there are a variety of options available to deal with this attack. First of all, as explained in section III, if the authentication enables authenticated key exchange to exchange a key used to encrypt the rest of the communication, then this attack is totally avoided since the shared secret is not known by the attacker [2].

V. EXISTING METHODS

In this section we brief about some of the existing approaches and its drawbacks.

G. Sequence number analysis

One way to avoid the attack is based on sequence number field of 802.11 frame headers. The sequence number field is 12-bits long and incremented by one for each no fragmented frame. Although the attacker has the ability to change the MAC address, same thing is not true for the sequence number. Without the ability to access the firmware source code of the wireless card, the attacker cannot alter the sequence number to an arbitrary value. Hence, when the attacker hijacks the authorized connection, the frame he sends would not have a sequence number incremented by one. For instance the lastframe the authorized user sends might have a sequence number of 433 whereas the frame the attacker sends very likely might have a sequence number something other than 434. This anomaly is the hint for the AP to recognize that there is something wrong. Analysing the sequence number pattern, the access point can identify and mark the activity from the concerned MAC address as the spoofed MAC activity. Can we do the same kind of sequence number analysis for mode 1? The answer is unfortunately no. Remember that the attacker instantiates a new connection to the AP in this case. The only thing the AP can do here is to store the sequence number of the previous session and match it with the sequence number of the first frame in the new connection. However the probability that the wireless card has sent frames to another AP in the meantime is not negligible therefore calling the gap in the sequence numbers a spoofed MAC activity carries the significant risk of being a false positive. (One might think that to avoid false positives, the sequence number analysis mentioned above can also be done centrally on the authentication server but this is not a practical solution since all AP-s now should continuously inform the server about the sequence numbers of the frames they receive.) [4].

H. Radio Signal Strength Detection

The assumption in this method is that attacker is like to be attacking from different position or place it is quite impossible that at the receiver that both the signals from authenticated user and attacker match. But with the help of sophisticated tools the attacker can study the authenticated users signal strength and adjust his signal strength to match the authenticated node signal [4].

VI. OUR APPROACH

One of the key features of high speed WLAN such as 802.11n is the use of MIMO (Multiple Input Multiple Output) antenna technology. The MIMO channel is described with fine granularity by Channel State Information (CSI) that can be utilized in many ways to improve network performance. Many complex parameters of a MIMO system require numerous samples to obtain CSI for all possible channel configurations. Our approach is based on utilizing CSI in MIMO based WLAN to prevent MAC spoofing. CSI alone cannot prevent MAC spoofing, so we include second factor authentication to completely prevent MAC spoofing.

I. Channel State Information (CSI)

Channel State Information describes the current condition of the channel, and consists of the attenuation and phase shift experienced by each spatial stream to each receive antenna in each of the OFDM subcarriers. CSI is determined in the 802.11 hardware by analysing received packets using training sequences in the packet headers [5]. Many implementations of 802.11n require successful decoding of a data packet to obtain CSI. In addition, it is required to send a packet using n transmit antennas over a bandwidth W, and receive it over m receive antennas to obtain the complete m × n × W CSI data structure. m is thenumber of transmitter, n is number of receivers and W is number of OFDM subcarriers [6]. CSI is a very high dimension data m × n × W. It is very difficult for an attacker to capture CSI information of an authenticated user. One of the main property of CSI is its rapid spatial decorrelation, i.e. if an attacker attacks slightly from different position compared to authenticated user then attacker CSI information doesn't match with authenticated user. Correlation coefficient of two CSI matrix tends to zero rapidly. In this model attacker and authenticated user are assumed to be located in spatially separated position.

VII. SYSTEM MODEL

In this section we describe working model of our approach and algorithm

J. Attack Model

Throughout the discussion, we introduce three different parties: Alice, Bob and Eve. As shown in Fig. 1, they are assumed to be located in spatially separated positions. Alice is the legal client with NT antennas, initiating communication by sending signals to Bob. As the intended receiver, Bob is the legal access point (AP) with NR antennas. Their nefarious adversary, Eve, will inject undesirable communications into the medium with NE antennas, in the hopes of impersonating Alice. In this working model Alice and Bob share authentication key which is used to authenticate initially. After initial authentication Bob determines CSI of Alice through

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

training signals sent by Alice. Once the CSI information of Alice is captured Bob determines correlation coefficient of CSI matrix with every incoming data. If both CSI match, its correlation coefficient will be one in ideal case. Now if Eve injects any packets his CSI information doesn't match with the stored CSI information with Bob. When Bob calculates the correlation coefficient, it tends towards zero. Bob suspect packets from Eve and asks for second factor authentication. Second factor authentication is provided by shared key. Since Eve is not an authenticated user, he fails in providing authenticated key and his packets will be rejected. What if Alice suddenly moves to different location suddenly? In this case his CSI information suddenly changes and Bob suspects packets from Alice and ask for second factor authentication. Since Alice is an authenticated user he can provide shared key and Bob reconstructs CSI information from Alice and rest of the procedure repeats. Second factor authentication is put in place in order to make authenticated user flexible to move around.

K. Algorithm

Page numbers, headers and footers must not be used.

- Node first sends authentication frame to Access Points. Access Points responds with the frame of type success.
- Shared key is exchanged between authenticated node and Access Point before data communication
- Node sends training signal to access point so that access point constructs CSI matrix of size m × n × W.
- For all the subsequence data packets from the node the access point constructs CSI matrix and matches it with that of the stored CSI by performing correlation.
- If correlation coefficient is less than threshold packet is suspected to be spoofed and second factor authentication is initiated by access point.
- As shared key is present only with the authenticated node, it can provide shared key to authenticate itself. If it is an attacker node then packets are rejected (Note: shared key is present only with unauthorized node)
- As shared key is present only with the authenticated node, it can provide shared key to authenticate itself. If it is an attacker node then packets are rejected (Note: shared key is present with unauthorized node)
- Access point requests for training signal and recalculates CSI and stores it.
- Above procedures repeats.

L. Threshold

Correlation coefficient threshold can be set as per the requirement. For any communication of the correlation coefficient lea than threshold will be treated as suspicious one. To make authenticated user to move around AP spatially threshold has to be set less than 1. Lesser the thresh hold more authenticated user can move around. As the thresh hold becomes low network becomes less secure giving attacker provision to launch attack from those position used by authenticated user. Threshold can be adjusted based on the criticality of the communication.

M. Performance

CSI is a very high dimension data of the order m × n × W. Time complexity of the correlation of two CSI matrix is O(m3) assuming m=n=W. Based on the criticality of the security this matrix can be reduced. More dimensionality of CSI implies more difficult for user to spoof it, hence more secure and vice versa.

VIII. CONCLUSION

In this paper we presented algorithmic approach based on smart antenna technology (MIMO) and second authentication factor. Algorithm is very robust and reliable and works for both in mode 1 and mode 2 type of operation explained in section III. In order to increase the performance, threshold and dimension can be varied considering criticality of communication security.

REFERENCES

[1] AnupGirdhar, Dr. SushilaMadan "MAC Spoofing A Biggest Threat for Cyber Crime Investigation".

[2] Kemal Bicakci, Yusuf Uzunay "Pushing the Limits of Address based Authentication," World Academy of Science, Engineering and Technology. Vol 2, Jun. 2008.

[3] Guenther Lackner, Udo Payer, and Peter Teufl, "Combating Wireless LAN MAC-Layer Address Spoofing with Fingerprinting Methods, "International Journal of Network Security". vol. 9, No. 2, pp.164–172, Sept 2009.

[4] Zhiping Jiang, JizhongZhao, Xiang-Yang Li, JinsongHan, Wei Xi "Rejecting the Attack: Source Authentication for Wi-Fi Management Frames using CSI Information".

[5] Riccardo Crepaldi, Jeongkeun Lee, Raul Etkin, Sung-Ju Lee, Robin Kravets. "CSI-SF: Estimating Wireless Channel State Using CSI Sampling & Fusion" .

[6] Liang Xiao, Larry Greenstein, Narayan Mandayam. "MIMO-Assisted Channel-Based Authentication in Wireless Networks" Wireless Information Network Laboratory (WINLAB), Rutgers University.

BIOGRAPHIES

Ananth Hegde is a student of International Institute of Information Technology, Bangalore. Pursuing final year M. Tech in Information Technology. His research interest includes Network Security, Machine Learning, Software Engineering and Embedded Systems.