Journal of Advances in Science and Technology

Vol. III, No. VI, August-2012, ISSN 2230-9659

DIFFERENT KIND OF ATTACKS ON WLAN

www.ignited.in

Journal of Advances in Science and Technology
Vol. III, No. VI, August-2012, ISSN 2230-9659

Different Kind of Attacks on Wlan

Amandeep Kaur

Research Scholar of CMJ University, Shillong, Meghalaya

Abstract - Different types of attacks and threats are categorized in to two main parts. These type of attacks are considered to be general in context for every WLANs and will described further in detail with their drawbacks and solutions.

1. Logical Attack

2. Physical Attack

A logical attack always relates with the software, system and the sensitive data flowing in the network. In this type of attack the target of the intruder is to find the code and software or any drawback in the network which will help the intruder to access the network and altered the sensitive data easily. The main target of this attack is to find the sensitive data flowing in the network. If the attacker is successful, then this attack will produce lot of problems for the network as well as for all the networks that is in connection with. Some logical attacks are defined below with their mitigation techniques.

MAC addresses are sent over the medium when communication has to start between the node and the AP. When any node tries to establish a connection with AP (access point) it must be authenticated through its MAC address of Wireless NICs to make the connection more secure. In the normal process of authentication the MAC addresses are forwarded in the clear text form and any attacker can pick the address of any authenticated user while using different tools like kismet. It will create a data base of legal wireless nodes and also their MAC addresses.

----------♦----------

INTRODUCTION

The attacker passively sniffs every packet of the victim. He keeps storing the cipher text along with the corresponding IV. Whenever the same IV repeats, he has two cipher texts for the corresponding IV. As shown in the figure he has C31,0 and C31,1 for K 31.

C31,1 □ C31,0 = P31,1 □ P31,0

Using classical techniques it is possible to find a and b from a □ b. Thus the attacker can get the knowledge of P31,0 ,P31,1 and K31 provided he has patience and resources to do it.

IV	Ciphertext
IV0	C0, 1
....	....
IV31	C0,31
....	....
IVN	C0,N

Table. A Decryption Dictionary

This passive attack is used to find the secret key, k. The attack is based on the premise that some weak IVs exist, i.e. they reveal information of a byte x of k. The following facts/assumptions are used:

- The first byte of plaintext is known, it happens to be 0xAA for ARP and IP packets. We thus know the first byte K1 of the key stream K.
- K1 is enough to find the byte x of k.
- All the bytes of k prior to x have been deciphered correctly.

The probability of finding byte x of k correctly is more than 0.05.

We illustrate here, with an example, the working of the attack:

1. We take a packet and keep its IV.

2. There can be two cases

If it is not a weak IV we dump it.

If it is a weak IV, we find that it helps us in finding 6th byte of k

3. We calculate the value of 6th byte (Function key Guess of it RC4.c of Air snort, 5).

We find out that this weak IV w.r.t 6th byte of k calculates k6 to 0x67. We keep this Value of k6 in a

table because the calculated value 0x67 may be wrong.

4 Such a table keeps filling. After sufficient entries, we find that the calculated value 0x67 of k6 is correct because it occurred the maximum times.

5 After finding all the bytes of k, we make a try on all the packets, used above, by decrypting them and checking whether indeed, CRC(M) is consistent for all of them.

Byte No. of k	Value	Value	Value	Value	Value	Value
....	....	....	....	....	....	....
6	0x67	0xab	0x37	0x67	0x67	0x20
....	....	....	....	....	....	....

Table. Working of Airsnort

The actual number of packets needed to crack the WEP key was not checked by us, but reports say that it can be done in a matter of a few hours for 40-bit secret key and a matter of days for 104-bit secret key.

MESSAGE MODIFICATION

This active attack is used to change a particular part of the message M that is known to the attacker, along with its position in the packet. This field can be an email ID, HTML form.

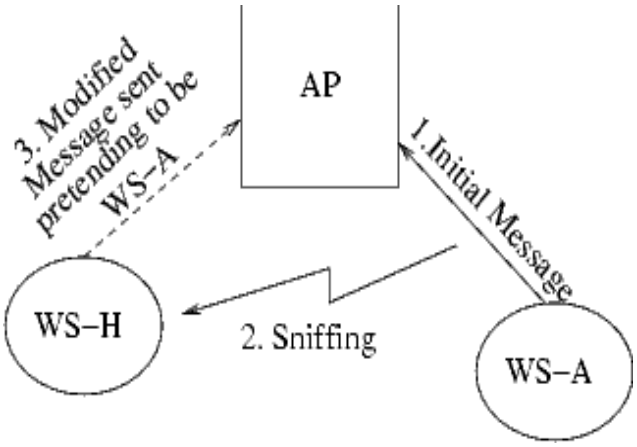

Fig : Message Modification

The attacker doesn't need to have the knowledge of key stream K or the secret key k for the attack. The attack is based on the fact that CRC(M) is an unkeyed function of M.

MESSAGE DECRYPTION

There are two methods of decrypting the message by active attacks.

1. IP Redirection

2. Reaction Attack

IP REDIRECTION

This attack is an extension to message modification. The attacker modifies the destination IP in the IP header of the packet. By doing this, the attacker sends a packet from WEP encrypted zone to No WEP Zone, where he holds a machine.

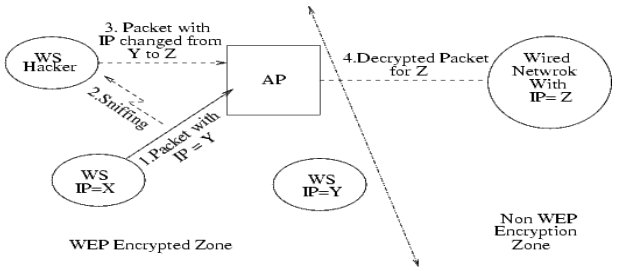

Fig: IP Redirection

To do this he has to make changes in the IP Header Checksum. In most cases the initial IP Checksum is not known although the attacker is assumed to have the initial destination IP address. So the attacker keeps sending packets with various values of checksum till he gets the packet across to his machine in No WEP Zone.

We did a simulation of this attack. The number of packets required, as a function of initial and final destination IPs, before getting a hit is open for interpretation.

REACTION ATTACK

This attack only works for TCP Packets. If TCP checksum is valid w.r.t. to the checksum, an ack is sent, otherwise the packet is dropped silently. This attack is based on the receiver's willingness to decrypt arbitrary cipher text and feed them to another component of the system that leaks a tiny bit of information about it's inputs. The attack is rightly called reaction attack as it works by monitoring the recipient's reaction to our forgeries.

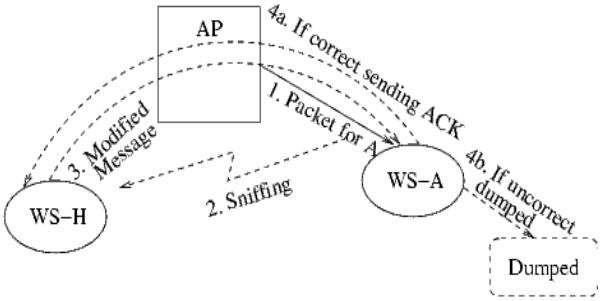

Fig: Reaction Attack

We have coded a simulation that verifies the property of TCP checksum that if bits Pi and Pi+16 are complements of each other then putting

complemented values into each, Pi and Pi+16 doesn't affect the TCP checksum. Thus, the attack works in following fashion:

1. Take complements of Ci and Ci+16.

2. Make appropriate changes in the CRC checksum (this is not to be confused with the IP or

TCP checksums) of message, CRC (M), and send the packet to the recipient.

3. There are two cases:

1. ACK received: Pi and Pi+16} were complements of each other.

2. No ACK: Pi and Pi+16 were same.

We didn't test the actual effectiveness of this attack.

TOOLS AVAILABLE FOR ATTACKING WLANS

These are few of the tools that are available for attacking the WLANs:

1. Airsnort (Linux) - cracks the WEP key.

2. WEP Crack (Linux) - cracks the WEP key.

3. Net Stumbler (Windows) - finds the network parameters like, SSID, Channels, MAC Addresses, Type of Encryption used, Vendor of the card, tells the default secret key of the vendor can be used with a GPS for locating APs.

4. Kismet (Linux) - a WLAN sniffer.

5. Thc-Wardrive (Linux) - for war driving.

6. dsniff (Linux) - counterpart of NetStumbler.

7. dstumbler (FreeBSD) - counterpart of NetStumbler.

This type attempts to describe the prospective of security issues faced during the transfer of data between the WLAN users. The current study is provided to identify the impact of security problems in WLAN. Currently WLAN faces several security threats and attacks due to its nature because the information is broadcast into the air through which one can break the security of WLANs having little understandings about the network.

SPOOFING OF MAC ADDRESS

MAC addresses are sent over the medium when communication has to start between the node and the AP. When any node tries to establish a connection with AP (access point) it must be authenticated through its MAC address of Wireless NICs to make the connection more secure. In the normal process of authentication the MAC addresses are forwarded in the clear text form and any attacker can pick the address of any authenticated user while using different tools like kismet. It will create a data base of legal wireless nodes and also their MAC addresses. The intruder can simply spoof the MAC address of any node and use that MAC address to gain access to WLAN. This stealing of nodes with MAC addresses that are authenticated via AP is also possible. It can create a main security violation. To eliminate this condition the network engineer must be notified of any stolen user or lost node to remove the MAC addresses of those from the list which are allowed to access the AP in the WLAN.

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS)

The availability of a network is significant for crucial services. In the WLAN network, the transfer of a data must be guaranteed with a high success rate while providing prompt first - response services. DoS and DDoS are used to lose the availability of different services of a network.

DoS attacks are considered to be a most common type of security attacks, very complex in nature and difficult to mitigate fully, but it can be controlled up to some extent. The target of the DoS attacks is to restrict the legal client from accessing the network. DoS attack makes the services ineffective for the legal client. DoS attacks can be implemented by using Flood attack, SYN attack and Ping of death attack.

Distributed DoS is considered to be a common category of DoS. The target of the Distributed DoS is to attack on the Server by sending lot of irrelevant request to the network Server and network Server becomes slow after sometime and unable t provide the services to the legal user. The most important way to protect from DoS and DDoS attack is to locate the source of the attack and then block that traffic from that source. There are three common mitigation techniques for DoS and DDoS.

- Anti-spoof feature.
- Anti-DoS feature.
- Traffic rate limiting.

The DDoS attacks are a series of DoS attacks which are more harmful than DoS in the network.

WLAN allows these intruders to begin easily inside WLAN network. Therefore, WLAN network has to face many challenges and has to discover different kinds of tools to protect it from these attacks. This type of attacks can be blocked through authentication, authorization, and accounting server.

REFERENCES

- Prasad, A. R., WLANs: Protocols, Security and Deployment, Ph.D. Thesis, Delft University Press (DUP), Delft, The Netherlands, December 2003.
- Prasad, N. R., Adaptive Security in Heterogeneous Networks, Ph.D. Thesis, University of Roma "Tor Vergata," Rome, Italy, April 2004.
- Prasad, N. R., and A. R. Prasad (eds.), WLAN Systems and Wireless IP for Next Generation Communications, Norwood, MA: Artech House, January 2002.
- Black, U., Internet Security Protocols: Protecting IP Traffic, Upper Saddle River, NJ: Prentice Hall, 2000.
- Stallings, W., Cryptography and Network Security: Principles and Practice, Upper Saddle River, NJ: Prentice Hall, July 1998.
- Anand R. Prasad & Neel R. Prasad. 2005. 802.11 WLANs and IP Networking Security, QoS and Mobolity. Artech house Universal personal communication Series.
- AvHarold F. Tipton & Micki Krause. 2009. Information security management handbook.
- Auerbach Publications.
- Arinze Nwabude. 2008. Wireless local area network (WLAN): security risk and counter measures. Blekinge Institute of Technology.
- Hara & A. Petrick. 1999. IEEE 802.11 Handbook, A designer companions. IEEE Presss.
- Wi-Fi Protected Access: Strong, Standard based, interoperable security for today‟s Wi-Fi
- networks. Retrieved june 28 2005. Online available http://www.wifialliance.com/opensection/pdf/whitepaper_Wi-Fi_Security4-29-03.pdf
- Wi-Fi Protected access 2. Retrieved june, 28 2005. Online available: http://www.wi-fi.org/opensection/protected_access.asp
- Sebastin Bohn & Stephan Grob. 2006. An automated system interoperability test bed for WPA and WPA2. IEEE Xplore White paper. July 2008.
- WLAN Security Today: Wireless more secure than wired. Siemens Enterprise Communications.
- White paper. July 2008. WLAN Security Today: Wireless more secure than wired. Siemens Enterprise Communications.
- Ahmed M. Al Naamany, Ali Al Shidhani & Hadj Bourdoucen. 2006. IEEE 802.11 Wireless LAN Security Overview. Department of Electrical and Computer Engineering, Sultan Qaboos University. Oman.
- ISS Technical Paper Internet Security System, Wireless LAN Security 802.11b and Corporate Network. Barfiled Road, Atlanta.
- F. Cao & S. Malik, 2005. Security Analysis and Solutions for Deploying IP Telephony in the Critical Infrastructure, Critical Infrastructure Assurance Group Cisco Systems, Inc.
- Patrick C.K & M. Vargas. 2006. Security Issues in VOIP Applications. Hung University of Ontario Institute of Technology Oshawa, Canada.
- Joon S.Park & Derrick Dicoi. 2003. WLAN Security: Current and Future.