International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 5(I); May 2018; Page No. 12811-12815
DOI: http://dx.doi.org/10.24327/ijcar.2018.12815.2266

Research Article

A RESEARCH PAPER ON SECURITY OF WIRELESS NETWORK

Kirti Kaushik and Nidhi Sewal

Department of Computer Science and Engineering, of DPGITM, Maharshi Dayanand University, Haryana, India

ARTICLE INFO

Article History:

Received 9th February, 2018
Received in revised form 26th
March, 2018 Accepted 17th April, 2018
Published online 28th May, 2018

Key words:

WLAN, Wireless LAN, Security, IEEE802.11

ABSTRACT

Over the past few years, the IEEE 802.11 standard has been the focus of a large amount of research with respect to its security architecture and mechanisms. Our own research has shown a huge deficiency in the 802.11 standard with regard to security, as well as deficiencies in 802.11 network implementation and deployment. Furthermore, while several technologies have been (and continue to be) developed to either augment or replace the standard's flawed portions, the difficulty of managing wireless networks has created a complex situation for network administrators even when they use the latest technologies. Like most advances, wireless LAN poses both opportunities and risks. The evolution of wireless network in few years has raised many serious security issues. In this Paper to fix security loopholes a public key authentication and key-establishment procedure has been proposed which fixes security loopholes in current standard. The public key cryptosystem is used to establish a session key securely between the client and Access point. A client -Agent based Rouge Access point detection system was developed to counter the threat of Rouge Access points in wireless LANs and are difficult to handle at the protocol level. Hence a centralized RAP was developed for organization where the area is quite large to cover manually or form a single location. An algorithm was also developed to detect Evil-Twin Access points, which cannot be detected by traditional methods. The algorithm works on fact that the evil-twin is placed at a distance from the good-twin to prevent direct detection.

INTRODUCTION

WLAN standard and security services is IEEE 802.11 become top priority in installation of wireless technology-based information infrastructure because of its economic feasibility and high ability over several wireless technologies available today such as microwave, Wi-Fi or IEEE 802.11 and Wi-MAX. Apart from the low cost, IEEE 802.11 technology is relatively easy, quick to install, and operating on an unlicensed frequency of 2.4 GHz which can be built independently by the individual or organization without reliance on operator. A Wireless LAN always uses the electromagnetic waves to transmit the data signals from one end to another end in the network and it is implemented on the physical layer. IEEE 802.11 wireless LAN has two types of network architectures:

1. Ad-Hoc Network
2. Infrastructure Network

IEEE group started work on IEEE 802.11 project in year 1997, in order to design a Medium Access Control (MAC) and Physical layer (PHY) which provides benefits to wireless connectivity to fixed stations, portable stations and moving station within the specific boundary of the network. The initial standard includes three Physical layers, FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) and Infrared. Later on two other transmission technologies were included OFDM (Orthogonal Frequency Division Multiplexing) and HR-DSSS (High Rate Direct Sequence Spread Spectrum).

IEEE802.11 MAC layer consists of Channel Access Mechanism. IEEE802.11 MAC provides two channel access controls, DCF (Distributed Coordination Function) and PCF (Point Coordination Function). PCF provides contention free channel access and aims at supporting real-time traffic. DCF works based on CSMA/CA (Carrier- sense Multiple Access with Collision Avoidance) with the consideration of the complexity in wireless environment; for example, stations can not listen to the channel for collisions while transmitting.

IEEE 802.11 Specifications

The 802.11 Standard is a group of networking standards that cover the physical layer specifications of technologies from Ethernet to wireless. IEEE 802 is subdivided into 22 parts that cover the physical and data-link aspects of networking. The better known specifications include 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth/ZigBee, and 802.16. All the 802.11 specifications use the Carrier Sense Multiple Access and

Corresponding author:* **Kirti Kaushik
Department of Computer Science and Engineering, of
DPGITM, Maharshi Dayanand University, Haryana, India

Ethernet protocol with Collision Avoidance (CSMA/CA) for path sharing. The original modulation used in 802.11 was phase-shift keying (PSK). Another schemes, such as complementary code keying (CCK), are used in some of the newer specifications. The latest modulation methods provide higher data speed and reduced vulnerability to interference.

- 802.1- LAN/MAN bridging and management. Covers the lower sub-layers of OSI Layer 2, including MAC-based bridging (Media Access Control), virtual LANs and port-based access control.
- 802.2- LLC or Logical Link Control specification. The LLC is the top sub-layer in the data-link layer, OSI Layer 2. Interfaces with the network Layer 3.
- 802.3- "Granddaddy" of the 802 specifications. Asynchronous networking uses "carrier sense, multiple access with collision detect" (CSMA/CD) over coax, twisted-pair copper, and fiber media. Current speeds range from 10 Mbps to 10 Gbps.
- 802.4- Disbanded
- 802.5- The token-passing standard for twisted-pair, shielded copper cables. Supports copper and fiber cabling from 4 Mbps to 100 Mbps. Often called "IBM Token-Ring."
- 802.6- "It incorporates and supersedes published standards 802.1j and 802.6k. Superseded by 802.1D-2004."
- 802.7- Withdrawn Standard. Withdrawn Date: Feb 07, 2003. No longer endorsed by the IEEE.
- 802.8- Withdrawn PAR. Standards project no longer endorsed by the IEEE.
- 802.9- Withdrawn PAR. Standards project no longer endorsed by the IEEE.
- 802.10- Superseded **Contains: IEEE STD 802.10b-1992.
- 802.11- Wireless LAN Media Access Control and Physical Layer specification. 802.11a, b, g, etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified.

Security in IEEE 802.11 Networks

Various security solution measures of network performance that reflects the network's transmission quality and service availability for IEEE 802.11 standard like WEP, CCMP, etc and which one is considered to be best in which environment.

Wired Equivalent Privacy (WEP) – WEP is a first security technique that is used in IEEE 802.11 standards. WEP provides the security to WLAN like the wired LAN. WEP helps to make the communication secure and provide the secret authentication scheme between AP and the end user which is going to access the WLAN. Basically WEP implemented on initial Wi-Fi networks so that the user can not access the network without the correct key. WEP uses symmetric key encryption that ranges from 64 to 128 bit long encryption key. Usually, the same encrypted key is used for all the nodes in the network and manually forwarded to each node means WEP is unable to provide the key management function. WEP is using the shared key authentication method in which the user needs two things in order to access the WLAN, one is SSID and second is WEP key generated by the AP. The IEEE 802.11 standard defines the three different parameters for the WEP i.e. access control, data privacy and data integrity.

CCMP- CCMP is an encryption algorithm of IEEE 802.11i. CCMP performs in a particular mode of operation that is AES. In other words the mode of operation is known as the algorithm, whose purpose is to change the cipher text to plaintext and vice versa. The main purpose of using the encryption technique is to provide the confidentiality to data and hence it is proved that previous encryption technique is failed to provide the data integrity. In order to provide the integrity to data, a new message authentication code is appended with the original message. The message authentication code is useful for keyed cryptographic function in order to generate the integrity value (ICV).

In IEEE 802.11i standard is divided the CCMP in to two parts:

- Counter mode “CTR-Mode”. The counter mode is used in AES to encrypt the data
- Cipher block chaining- MAC mode “CBC-MAC Mode”. CBC-MAC mode is used to create a MIC code that provides integrity to data.

Parameters studied- Following parameters are undertaken in order to compare the results which are obtained to determine the Security of IEEE 802.11 Wireless Local Area networks under WEP and CCMP Security Protocols.

- Throughput (bit/sec): The total number of bits (in bits/sec) sent to the higher layer from the MAC layer. The data packets received at the physical layer are sent to the higher layer if they are destined for this station.
- Average Jitter: Jitter is defined as a variation in the Delay of received packets.
- Average End-to-End Delay: It indicates the Length of time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It represents the total Delay between creation and reception of an application packet.

Security Analysis

The complete analysis of authentication has been done considering possible threats. Since the management frames are not protected in a WLAN, an adversary is capable of interfering with initially step of AP discovery and IEEE 802.11 association and authentication. Spoofed security capabilities and topological views of the network can be sent to a supplicant on behalf of an authenticator by an adversary. Once this occurs, the supplicant will be forced to use inappropriate security parameters to communicate with the legitimate authenticator, or associate with a malicious AP, if no further protections are used, an adversary can forge association requests to the authenticator with weak security capabilities, which might cause problems. Fortunately these threats are eliminated in IEEE 802.1X authentication if a strong mutual authentication is implemented. The main purpose of authentication is to prevent an intruder from modifying, and forging authentication packets.

If PSK is used instead of PMK, then the AP and the supplicant can authenticate each other by verifying shared key (PSK or cached PMK) and active and passive eavesdropping and message interception can be eradicated. Session hijacking can be possible even if a strong authentication mechanism is implemented. However, it does not pose any threat more than eavesdropping, because the adversary can disconnect a station by forging de-authentication or disassociation messages and hijack the session with AP on the behalf of the legitimate station. In this case, the adversary can only accept packet which are encrypted using PTK, so he can't know what is inside the packet.

Man in the middle attack can be launched, if mutual authentication mechanism not appropriately implemented. The vulnerability is a weakness of the specific mutual authentication protocol instead of 802.11i and so the mutual authentication should be implemented carefully. The adversary can forward credentials between the AP and the station; but since the authentication packets cannot be used further like in replay attack, so an adversary can't cause more damage than eavesdropping, he can only relay the packets.

From the above discussion, the complete RSNA process seems to be secure for authentication process. Since the adversary could interfere with IEEE 802.11 authentication and association step, it might be able to fool the authenticator and the supplicant, and prevent completion of the RSNA. In addition, some implementations might also allow a reflection attack in the 4-way handshake protocol. Although the link between the authenticator and the authentication server is assumed to be secure, dictionary attacks will still be a threat for the shared secret in Radius. When a 256-bit PSK is used instead of PMK, this PSK could be derived from a passphrase, which makes the PSK vulnerable to dictionary attacks. For eliminating this vulnerability, a good passphrase or a 256-bit random value should be chosen carefully.

Countering the Threats

Threat of Rogue Access Points in Wireless LANs

Client based RAP detection

The RAP Detector can be deployed in an organization with a large number of wireless users, which are scattered all over the organization The RAP Detector will be useful for such organizations as it will require little additional infrastructure and can be easily deployed as most organizations already have a DHCP server on which the RAP Detector can be deployed. The RAP detector can be configured to notify the system administrator about suspicious Access Points, which can be investigated to confirm their purpose.

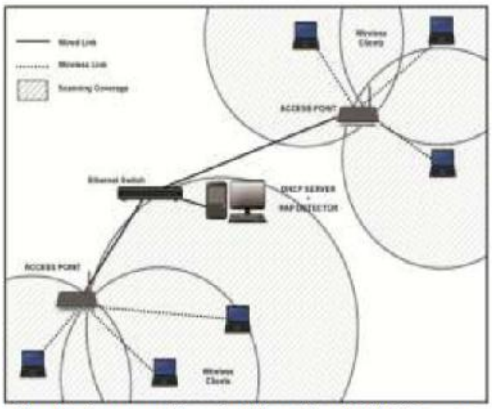

Fig Deployement Senerio Client Based RAP Detector

Basic system architecture

As shown in figure wireless nodes are scattered all over the organization. The shaded region depicts the area that can be scanned for rogue Access Points. The details of all the Access Points present in the area will be available at a central location (DHCP Server). Periodic scans can be scheduled that a more comprehensive coverage can be established. This can be done without manual intervention hence enhancing the security of the organization.

As shown in figure the complete system consists of three major components; a DHCP server, a Master Agent program having the database of all authentic APs and many wireless nodes (Laptops used by the members of the organization). These Laptops act as client agents. They will execute a small program it all times which will listen for a query from the Master Agent and then send a list of Access Points in its vicinity to the Master Agent. These lists are then consolidated and a list of all detected Access point is generated. This list of detected Access Points is then analyzed for anomalies. It is compared with the database of known Access Points. Also an algorithm to detect Evil-Twin Access Points is run to detect Evil-Twins in the list of detected Access Points.

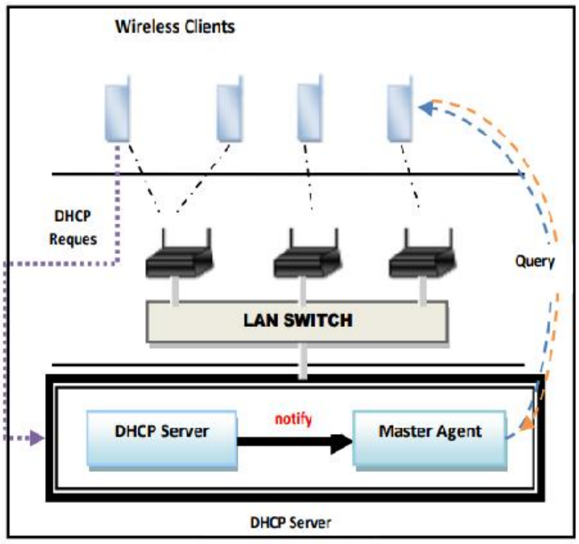

Fig Architecture of RAP detection system

Algorithm for Detecting Evil Twin Access Points

Evil Twin Access points are access points that have the MAC address of a legitimate Access Point installed by the organization. They spoof the MAC address to masquerade as a legitimate Access Point. These Access points are very difficult to detect. Most commercial Access points have methods to detect Evil twin Access Points if they are in the range of the Access Point they are trying to masquerade. This is easy as an Access point can detect if another Access Point in its range has the same MAC address. Hence most Evil Twin access points are placed outside the range of their authentic twin. This fact is used to detect the Evil Twin Access Point. To detect twin the algorithm analyzes the context of each Access Point. It checks that all the clients that detect a particular Access Point are located in the same locality. This is to be expected since two clients that are located far off should not detect an Access Point. Two clients located far-off can detect the same Access Point only if the Access Point has a twin located at a distance.
The pseudo-code for the algorithm is given in figure:

```
1. For each AP in AP List[]
2. For each CLIENTi that detected A
```

3. For each CLIENTj that detected AP (i != j)
4. Compare APs detected by CLIENT i and CLIENT j
5. If both lists completely mismatch Flag CLIENTi and CLIENTj as ABNORMAL.
6. IF ABNORMAL clients for AP> Threshold i. AP has twins
7. END

The Experimental Scenario

To test the RAP detection system, it was tested in a hostel LAN with two clients and a master agent. For experimental purposes the two clients were located at opposite ends of the building to provide maximum coverage. The IP addresses of the clients were manually entered in the database. Some of the Access Points were manually entered into the database of known APs. The two clients were placed at a distance to provide maximum coverage. Query packets were sent to the clients at regular intervals to the clients.

The Master-Agent gathered and processed the response front the different clients and built a list of Access Points in the building. The Access Points entered manually were flagged as Authentic Access Point whereas the Access Points that were not present in the database were flagged as Rogue Access Points. The System was kept running for a period of 30 minutes during which it provided real-time information about all the Access Points in the building. The following parameters were collected about the Access Points in the building:

- MAC ID of the Access Point
- List of clients that detected the Access Point
- Last time when the Access Point was detected.

RESULTS

Results of RAP Detector

The RAP detector was test in a building with 25 Access points and only two client agents. The two client agents were able to provide information about almost all the access points in the building. Only one Access Point was outside the range of both the clients. 17 Access points were added to the database of known Access Points and hence were detected as authentic APs whereas the rest were flagged as Rogue Access Points. The list of all detected access points was built within a time period of 1 minute. The clients were queried at an interval of 10 seconds and the replies were received almost instantly. In comparison the manual auditing took 30 minutes to scan the building and compare the results with the list of known Access points. Table shows the various results obtained from the experiment.

Result of RAP detection in the Experimental setup

Parameter	Value
Total Access points	25
Known Access points	16
Total Access points Detected	24
Rogue Access points Detected	8

It was very clear from the experiment that in organizations where manual scanning for Rogue Access Points is time consuming, such a centralized client-based RAP detector is very useful. As our system requires almost no additional hardware installation, it can be easily installed in organizations and can provide with real-time, centralized RAP detection.

Simulation Results for detection of Evil Twin Access Points

To simulate the performance of the Evil-Twin Access point detection algorithm it was tested in a virtual environment. Since it was not feasible to deploy such a large number of clients and access points the algorithm was tested on a virtual grid of l000xl000. Although Access Points operate in a 3-D space, a 2-D space was used instead for simplicity. The positions of 20 Access Points were randomly generated in a coordinate grid of 1000x1000. Various numbers of client positions were generated. The number of clients varied from 20 to 100.Out of the 20 Access Points two was twins. The algorithm was then used to detect the twins.

For each client-set size the simulation was performed 100 times and the results were noted. The accuracy was calculated as follows:

Accuracy = (Number of Times Evil-twins were correctly detected) x 100
Total number of simulations

False Positive Rate = (Number of times other Access Points were wrongly detected) x 100 Total number of Simulations

A very high rate of success was observed. The algorithm detected the Access Point with twins with a high success rate. The results for various client-set sizes are shown in figure It was observed that accuracy increased with increasing number of wireless client- agents. With 20 clients the accuracy was 54% while with 100 clients it increased to 81%. Although some false positives were detected it was very low and always remained under 2%. As is clear from the results the accuracy for the algorithm is quite high whereas the false positive rate remained very low throughout all client-set sizes.

CONCLUSIONS

Security is very important in Wireless LANs since they operate in a broadcast medium.

From the obtained results the following can be concluded about the public-key based authentication scheme:

1. The authentication scheme will successfully stop DOS attacks by providing a secure key-establishment mechanism.
2. Both unicast and multicast management frames will be protected from eavesdropping and modification since they will be signed with the public key of the Access Point.
3. Insider Attacks will be stopped by providing each client with a secure session key.
4. Public-key based authentication mechanisms are feasible in wireless LANs without introducing much delay in the authentication procedure. It was seen from the results that while EAP (Extended Authentication Procedure) takes about 2.5 ms, a session key establishment will take around .4 ms with 10 concurrent clients.

The Client-Agent based Rogue Access Point detection system was tested and the following conclusions can be drawn from the results:

1. The client-agent based RAP detection system will be able to provide real time RAP detection capabilities in organizations that have a set of trusted wireless clients.
2. As the results show using the proposed system, even with a small number of trusted clients a very large area

can be covered and monitored. In our experiment with only 2 wireless clients an area of 100 sq meters was covered.

3. The Evil-Twin detection algorithm also performed well under the simulation environment. It showed 81% accuracy when the number of clients is 100. The false-positive rate was as low as 1%.

Future Scope

There is obviously scope for improvement and future work. The possible improvements to our work can be:

1. Although the proposed authentication scheme has been shown to mitigate existing attacks, it should be evaluated by formal evaluation method and predicate logic for the sake of completeness.
2. It was shown that public-key cryptosystem is feasible in Wireless LANs by simulating it on machine with CPU speed comparable to Access Points. As future work the mechanism should be implemented on an actual Access Point and tested for feasibility.
3. The RAP detection system only detects Rogue Access Points. A counter attack system can be incorporated into the Rogue Access Point system to block detected RAPs in the future. This can be done using SNMP to block the port where the Rogue Access Points are connected.

References

1. Les Owens, "Wireless Network Security: 802.11, Handheld Devices and Bluetooth", National Institute of Standard and Technology. November 2002.
2. IEEE Standard for local and metropolitan area networks, “Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, Medium Access Control (MAC) Security Enhancements”. ANSI/IEEE STD 802.11i, 2004 Edition.
3. Nikita Borisov, Ian Goldberg and David Wagner. "Intercepting Mobile Communications: The insecurity of IEEE802.11", 7th Annual International Conference on Mobile Computing and Networking. July 2001.
4. EEE-SA. (2007). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Communications Magazine
5. A. Mishra and W.A. Arbaugh, An Initial Security Analysis of the IEEE 802.1X standard, tech. report CS-TR-4328, Dept of Computer Science, Univ. of Maryland, 2002.
6. ISO/IEC 8802-11 ANSI/IEEE Sta. 802.11, Wireless LAN Medium Access Control and Physical Layer Specifications, draft amendment, Int’l Org. for Standardization/ IEEE, 2003.
7. J.R. Walker: An Analysis of the WEP Encapsulation, IEEE 802.11 Task Group E IEEE 802.11/00- 362, Oct. 2000,http://grouper.ieee.org/groups/802/11/ Documents/DocumentHolder/0-362.zip.
8. Stanley Wong, “The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards”, GSEC Practical v1.4b, 2007.
9. Muddassar Farooq, “Defence Against 802.11 DoS Attacks Using Artificial Immune System”, Springer-Verlag Berlin Heidelberg, pp. 95-106, 2007.
10. Chris Wullems, Kevin Tham, Jason Smith and Mark Looi, “A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANs”, 3rd IEEE Wireless Telecommunication Symposium (WTS) May 2004.

How to cite this article:

Kirti Kaushik and Nidhi Sewal (2018) 'A Research Paper on Security of Wireless Network', *International Journal of Current Advanced Research*, 07(5), pp. 12811-12815. DOI: http://dx.doi.org/10.24327/ijcar.2018.12815.2266

****