JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE

Volume-2,Issue-6 (June-2019)
ISSN (O) :- 2581-6934

A Comparative Review of Wireless Security Encryption Systems Methods

Sandeep kumar Vishwakarma [1] , Prof. Amit chouksey [2]

[1 2] GGCT, Jabalpur

Abstract: ***Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs. These features came with expensive price to pay in areas of security of the network. This paper distinguishes and outlines these security concerns and their answers. Extensively, security worries in the WLAN world are arranged into physical and legitimate. The paper outlines both physical and consistent WLANs security issues pursued by a survey of the primary advancements used to defeat them. It tends to coherent security assaults like manin-the-center assault and Denial of Service assaults just as physical security assaults like rouge APs. Wired Equivalent Privacy (WEP) was the primary coherent answer for secure WLANs. Hiwever, WEP endured numerous issues which were incompletely settled by IEEE802.1x convention. Towards flawlessness in verifying WLANs, IEEE802.11i developed as another MAC layer standard which forever fixes the greater part of the security issues found in WEP and other transitory WLANs security arrangements. This paper audits all security arrangements beginning from WEP to IEEE802.11i and talks about the quality and shortcoming of these arrangements.***

Keywords: WLAN, remote LAN, security, IEEE802.11.

1. Introduction

Remote Local Area Networks (WLANs) succeeded inproviding remote system access at adequate information rates. The Institute of Electrical and Electronics Engineering (IEEE) have set measures and particulars for information correspondences in remote condition, IEEE802.11 is the driving innovation standard for WLANs [1]. WLANs are conveyed as an augmentation to the current fixed/wired LANs and because of the way that the idea of WLANs are unique in relation to their wired partners, it is critical to raise the security of WLANs to levels nearer or equivalent to the wired LANs. As a rule IEEE802.11 can work in two system topology modes, Ad hoc and Infrastructure modes. This paper examines WLANs in foundation mode. In the framework topology, remote stations (STAs) impart remotely to a system passageway (AP) which is associated with the wired system, this setup shapes a WLAN. The foundation of associations among STAs and AP experiences three stages; examining, verification and affiliation [1]. In examining stage, the STA can either listen latently to AP signals and naturally endeavors to join the AP or can effectively demand to join an AP. Next is the verification stage, the STA here is confirmed by the AP utilizing some confirmation systems portrayed later in the paper. After effectively verifying, the STA will send an affiliation solicitation to the AP, when affirmed, the AP adds the STA to its table of related remote gadgets. The AP can relate numerous STAs yet a STA can be related to one AP just at once. Figure 1 demonstrates the three stages in WLANs.

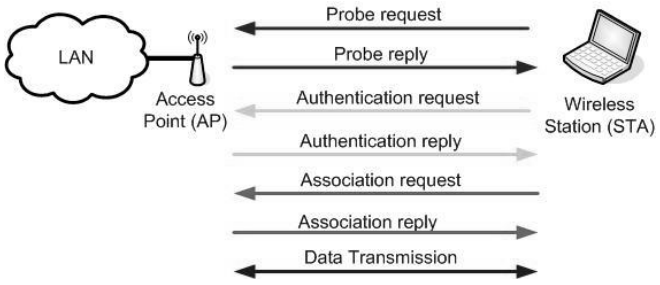

Fig. 1 The three phases undergone through WLAN for the establishment of connections between STAs and AP

These are testing, verification and affiliation A rupture of the security of the WLAN will inevitably hurt the security of the wired LAN. There are numerous issues with respect to the security of WLANs like utilizing Radio Frequency (RF) as a mechanism of transmitting data and the way that all messages are communicated to wherever the inclusion of that WLAN can reach [1]-[2]. The spread of wireless transmissions can't be blocked or secured a room so there is a major danger of spying and Man-in-the-center Attacks [3]. The circumstance is diverse in wired LANs where basic servers can be secured an uncommon room and information transmission is done by links that can be checked and controlled to some degree. When managing WLANs it is vital to remember three security objectives, Authentication to the WLAN, Confidentiality and Integrity of the information transmitted [4]. Regarding validation, there is a need to execute a component to permit STAs to confirm to allow access to the WLAN. These instruments must be proficient, adaptable and solid. Secrecy implies concealing high touchy information amid data transmission among STAs and AP. This is done to deny different clients from tuning in to the correspondence. Honesty implies safeguarding the exactness and the accuracy of data transmitted among STAs and AP [5]. Any security arrangement ought to accomplish these three objectives together. The security and the board issue become gigantic as more APs are introduced in the system. So there is a need to incorporate and oversee security issues in little WLANs just as substantial ones and a need to create procedures to counter security dangers. As WLANs applications like remote Internet and remote online business spread extremely quick, there is a need to guarantee the security of such applications. Numerous papers have been composed to address WLANs security issues (see [3], [4], [6]-[12], [18] and [21]). This paper audits WLANs security issue in both physical and intelligent angles and talks about the current accessible answers for these issues. The accompanying segments will in this manner disk significant dangers influencing WLANs security and accessible security conventions and advances used to counter these dangers.

2 WLAN SECURITY ASSAULTS

There are numerous security dangers and assaults that can harm the security of WLANs. Those assaults can be arranged into consistent assaults and physical assaults.

2.1 Logical assaults

2.1.1 Attacks on WEP: Wired Equivalent Privacy (WEP) is a security convention dependent on encryption calculation called "RC4" that intends to give security to the WLAN like the security gave in the wired LAN [2]. WEP has numerous disadvantages like the utilization of little Initialization Vector (IV) and short RC4 encryption key just as utilizing XOR activity to figure the key with the plain content to create figure content. Sending the MAC addresses and the IV free notwithstanding the regular utilization of a solitary IV and the way that mystery keys are really shared between correspondences parties are WEPs real security issues [4]. WEP scrambled messages can be effectively recovered utilizing freely accessible devices like WEPCrack [3] and AirSnort [4]. More exchange about WEP is tended to in later segments.

2.1.2 MAC Address Spoofing: MAC addresses are sent free when a correspondence among STAs and AP happens. An approach to tie down access to APs and subsequently to the system is to channel gets to dependent on MAC locations of the STAs endeavoring to get to the system [7]. Since MAC addresses are sent free, an assailant can acquire the MAC address of approved station by sniffing wireless transmissions utilizing instruments like ethereal [5] or kismet [6] to create a database of genuine remote stations and their MAC addresses. The aggressor can without much of a stretch parody the MAC address of an authentic remote station and utilize that MAC address to access the WLAN. Taking STAs with MAC tends to approved by the AP is additionally conceivable. This can cause a noteworthy security infringement. The system security director must be told of any stolen or lost STA to expel it from the rundown of STAs permitted to get to the AP subsequently the WLAN.

2.1.3 Denial of Service assault: Denial of Service assaults or DoS is a genuine risk on both wired and remote systems. This assault expects to handicap the accessibility

ISSN:-2581-6934|www.jidps.com

of the system and the administrations it gives [5]. In WLANs, DoS is led in a few different ways like meddling the recurrence range by outer RF sources subsequently denying access to the WLAN or, in best cases, giving access with lower information rates [3]. Another way is sending fizzled affiliation messages to AP and over-burdens the AP with associations till it breakdown which, accordingly, will deny different STAs from partner with the AP. Endeavors are house keeper by scientists to beat such assault by presenting new system components like Admission Controller (AC) and Global Monitor (GM) [36]. Air conditioning and GM assigns explicit data transmission to be used by STAs and on account of substantial traffic on AP, they can de-course a few parcels to neighboring AP to stop DoS assaults on APs.

Additionally assailants endeavor to misuse the validation conspire utilized by APs; this will drive the AP to reject every single authentic association started by legitimate STAs. Little is done as such far to counter DoS assaults [11], the way that DoS assaults are not kidding and devices to counter them are least pulled in aggressors to vandalize WLANs utilizing such assaults.

2.1.4 Man-in-the-center assault: This is a renowned assault in both wired and remote systems. An unlawful STA blocks the correspondence between real STAs and the AP. The illicit STA tricks the AP and claims to be a genuine STA; then again, it additionally tricks the opposite end STA and professes to be trusted AP. Utilizing procedures like IEEE802.1x to accomplish common validations among APs and STAs just as receiving a smart remote Intrusion Detection System can help in forestalling such assaults. Figure 2 indicates how this assault is led [17].

2.1.5 Bad system plan: WLANs work as an expansion to the wired LAN subsequently the security of the LAN depends exceptionally on the security of the WLAN. The defenselessness of WLANs implies that the wired LAN is legitimately on hazard. An appropriate WLAN configuration ought to be actualized by attempting to isolate the WLAN from the wired LAN by setting the WLAN in the Demilitarized Zone (DMZ) with firewalls, switches and any extra access control innovation to confine the entrance to the WLAN. Additionally devoting explicit subnets for WLAN than the once utilized for wired LAN could help in restricting security breaks. Cautious wired and remote LAN organize configuration assumes imperative job to tie down access to the WLAN [9].

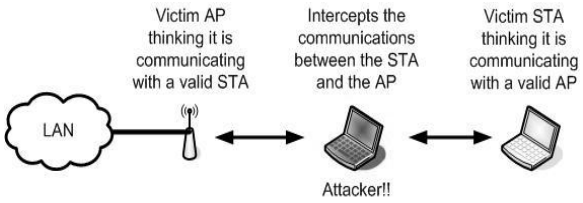

Fig. 2 Representation of the famous Man-in-the-middle attack for both wired and wireless networks

2.1.6Default AP configurations: Most APs are ship ped with minimum or no security configuration by default. This is true because shipping them with all security features enabled will make usage and ope ration difficult for normal users. The aim of AP s uppliers is to deliver high data rate, out of the b ox installation APs with out sincere commitment to security. Network security administrators should config ure these AP according to the organizations security policy [18]. Some of the default unsecured setting in APs shipped today are default passwords which happens to be weak or blank. Service Set Identifi er (SSID) is the name given to a certain WLAN and it is announced by the AP, the knowledge of SSID is important and works like the first securit y defense. Unfortunately, by default, some APs disa ble SSID request which means users can access the WLAN without proving the knowledge of SSID [12]. On the other hand, Some APs don't disable S SID request, in fact the SSID request is enabled b ut the SSID name itself is broadcasted in the air. This is another security problem because it advertis es the existence of the WLAN. SSID requests shou ld be enabled and SSID names shouldn't be broadc asted so users have to prove the knowledge of W LAN's SSID prior establishing communication. Anothe r default configuration in APs is that Dynamic Hos t Configuration Protocol (DHCP) is ON so users c

ISSN:-2581-6934|www.jidps.com

an obtain IP addresses automatically and hence acce ss the WLAN easily. Simple Network Management Protocol (SNMP) parameters are also set to unsecur ed values [10]. Network security administrators have the responsibility to change these configurations to maximize APs security.

2.2 Physical attacks

2.2.1 Rogue Access Points: In normal situations, AP authenticates STAs to grant access to the WLA N. The AP is never asked for authentication, this raises a security concern, what if the AP is install ed without IT center's awareness? These APs are c alled "Rogue APs" and they form a security hole in the network [18]. An attacker can install a Rog ue AP with security features disabled causing a ma ss security threat. There is a need for mutual auth entication between STAs and APs to ensure that b oth parties are legitimate. Technologies like IEEE802 .1x can be used to overcome this problem [7]. Ne twork security administrators can discover Rogue AP s by using wireless analyzing tools to search and audit the network.

2.2.2 Physical placement of APs: The installation location of APs is another security issue because p lacing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once f ound causing the AP to switch to its default settin gs which is totally insecure. It is very important f or network security administrators to carefully choose appropriate places to mount APs.

2.2.3 AP's coverage: The main difference between WLANs and wired/fixed LANs is that WLANs reli es on Radio Frequency (RF) signals as a communi cation medium. The signals broadcasted by the AP can propagate outside the perimeter of a room or a building, where an AP is placed, allowing users who are not physically in the building to gain ac cess to the network. Attackers use special equipment s and sniffing tools to find available WLANs and eavesdrop live communications while driving a car or roaming around CBD areas. Because RF signals obey no boundaries, attackers outside a building ca n receive such signals and launch attacks on the WLAN. This kind of attack is called "war driving" [19]. Publicly available tools are used for war dri ving like NetStumbler [20]. Hobbyists also chalk bu ildings to indicate that signals are broadcasted from the building and the WLAN in it can be easily accessed. This marking is called "war chalking". In War chalking, information about the speed of the connection and whether the authentication scheme us ed is open or shared keys are mentioned in the f orm of special codes agreed upon between warchalk ers. There are a lot of doubts and debates in the wireless network community regarding the legality of war chalking and war driving activities. Network security administrators can test the propagation of APs by using special tools to verify to what exten t the signals can reach. Accordingly they can contr ol the propagation of APs by lowering the signal strength or by using smart type of antennas to co ntrol the direction of the signal or move the AP to a place where it is guaranteed that the signal will not travel beyond the building premises [7]. S ome work has been done in the area of smart an tennas in APs to direct the propagation of traffic [38]. Directing the propagation of traffic as well as managing the power of signals originating from th e APs can be helpful in restricting the coverage o f APs to specified regions. Sometimes public and o pen access to the WLAN is preferable, such public WLANs are called "hot spots" [9]. Implementing hot spots is subject to many of the mentioned sec urity problems. It is important to understand that br eaking the security of a hot spot will result in br eaking the security of wired network connected to that hot spot. The control and monitoring of APs is minimal because it is installed in a public area like hotel lobbies, coffee shops, and airport lounge s so preventing physical access to AP is more diff icult as the site has to be monitored all the time.

ISSN:-2581-6934|www.jidps.com

In this case, there is a tradeoff between giving users the mobility and the flexibility to log in to the network in public areas versus the security of the network infrastructure. The network backbone can be highly secured but a breach in the security of the network access node (i.e. AP) can always lead to a breach in the security of the backbone behind the node.

3 LITERATURE SURVEY

Yi Ma et al [1] In order to solve the problem of vulnerable password guessing attacks caused by dictionary attacks, replay attacks in the authentication process, and man-in-the middle attacks in the existing wireless local area network in terms of security authentication, we make some improvements to the 802.1X / EAP authentication protocol based on the study of the current IEEE802.11i security protocol with high security. After introducing the idea of Kerberos protocol authentication and applying the idea in the authentication process of 802.1X / EAP, a new protocol of Kerberos extensible authentication protocol (KEAP) is proposed. Firstly, the protocol introduces an asymmetric key encryption method, uses public key encryption during data transmission, and the receiver uses the corresponding private key for decryption. With unidirectional characteristics and high security, the encryption can avoid password guessing attacks caused by dictionary attacks as much as possible. Secondly, aiming at the problem that the request message sent from the client to the authentication server is vulnerable to replay attacks, the protocol uses a combination of the message sequence number and the random number, and the message serial number is added to the request message sent from the client to the authentication server. And establish a list database for storing message serial number and random number in the authentication server. After receiving a transfer message, the serial number and the random number are extracted and compared with the values in the list database to distinguish whether it is a retransmission message.

Abhijit Bodhe et al [2] Wireless local area Networks (WLANs) are unit cost effective and fascinating gateways to mobile computing which allows computers or laptops to be mobile and cable less including communicate with speeds near the speeds of wired LANs. These options came with high-ticket worth to pay in areas of security of the network. This paper identifies and summarizes these security considerations and their solutions, the paper overviews each physical and logical WLANs security issues followed by a review of the most technologies would not to overcome those. The paper also addresses logical security attacks like man in- the-middle attack(MIM) and Denial of Service(DoS) attacks furthermore as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the primary logical answer to secure WLANs. However, WEP suffered several issues that were partly resolved by IEEE802.1x protocols. Towards perfection in securing our personal WLANs, IEEE802.11i emerged as a replacement waterproof layer normal that for good fixes most of the safety issues found in WEP and alternative temporary WLANs security solutions. This paper discusses the safety threats and risks related to wireless networks. With some best practices in company readying for WLAN

EMIL SELVAN GSR **et al [3]** Wireless networking technology is becoming increasingly popular but, at the same time, has introduced many security issues. Wired equivalent privacy (WEP) standards are followed in wireless local area networks for providing security. However, WEP is fatally crippled by the fact that WEP keys are the same for all users, all sessions, never change, and its poor implementation of the RC4 encryption scheme. The authentication mechanism is based on a simple challenge-response protocol. The main problem with the previ

ISSN:-2581-6934|www.jidps.com

ously used method was same key was used for both encryption and authentication. But, the proposed authentication is by means of certificates using extensible authentication protocol and a session key is transferred after successful authentication between mobile node and server. This session key is then used for encrypting messages using advanced encryption standard between mobile node and server.

4 CONCLUSION

IEEE802.11 was initially designed to interconnect wireless devices to wired networks; the aim was to achieve networking with minimum or no security. Security was not an important issue at that stage, however, with the successful of WLANs and the fast adoption of this technology, security became important and achieving security became a primary concern. Wired Equivalent Privacy (WEP) security protocols was the first to be adopted in an attempt to satisfy the need for securing wireless networks, soon WEP became vulnerable and there was a demand for a better security protocol. Industries already invested in wireless devices so any new protocol should consider the hardware capabilities of such devices. TKIP came into picture with promise of a better security using the same hardware. An upgrade in software is what made TKIP more secured than WE. However, the core encryption algorithm is still the same, weak RC4 stream cipher, with this encryption algorithm and the design flaws it experiences.

REFERENCES

[1] Yi Ma, Hongyun Ning, The Improvement of Wireless LAN Security Authentication Mechanism Based on Kerberos, 2018 International Conference on Electronics Technology, 978-1-5386-5752-2/18/ IEEE

[2] Abhijit Bodhe Mayur Masuti Dr. A.S.Umesh,,wireless lan security attacks and ccm protocol with some best practices in deployment of services , International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 0056 Volume: 03 Issue: 01 | Jan-2016

[3] emil selvan gsr**1**, gayathri n**1**, rakesh kumar s**2**, ankush rai**3**, jagadeesh kannan r**,** advanced encryption and extended authentication for wireless local area networks, Advances in Smart Computing and Bioinformatics, AJPCR, Special Issue (April), DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19987

[4] Matthew S. Gast, 802.11 Wireless Networks, O' REILLY, 2002.

[5] William Stallings, Cryptography and Network Security, Principles and Practices, 3rd Edition, Prentice Hall 2003.

[6] Matija Sorman, Tomislav Kovac and Damir Maurovic, "Implementing Improved WLAN security", 46th International Symposium Electronics in Marine. ELMAR-2004, Zadar. Croatia, 16-18 June 2004.

[7] Joon S.Park and Derrick Dicoi, "WLAN Security: Current and Future". IEEE Computer Society, October 2003.

[8] Nancy R. Mead and Gary McGraw. "Wireless Security's Future". IEEE Computer Society, IEEE Security and Privacy, August 2003.

[9] Joseph Williams, "Providing for Wireless LAN Security, Part 2". IEEE IT Pro, November | December 2002.

[10] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications", ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[11] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless network security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.

[12] Wang Shunman, TaoRan, WmgYue and ZhangJi , "Wireless LAN and it's security problem". Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.