VARIOUS SECURITY ISSUES IN WIRELESS AND ADHOC NETWORKS

Vaibhav Shukla*

Ashish Mishra**

Som Nath Ghosh***

Abstract:

As we know that the present day environment is the mobile environment and the people use the mobile devices very frequently people aware about the both type of networks that are wireless and the adhoc networks. These are the two networks that we used very frequently. Basically the difference between the two networks is that in the wireless network we work under fixed infrastructure and in the adhoc network no any type of fixed infrastructure is required. So as we see the differences between these networks the security issues in these type of networks are different and we basically study these issues in this paper.

Key words- Adhoc network, Manet, EAP**,** Authentication, Encryption.

* Asst. Professor (MCA), Jagran Institute of Management, 620, W Block Saket Nagar, Kanpur, U.P.-208014

** Asst. Professor (MCA), Jagran Institute of Management, 620, W Block Saket Nagar, Kanpur, U.P.-208014

*** Asst. Professor (MCA), Jagran Institute of Management, 620, W Block Saket Nagar, Kanpur, U.P.-208014

Introduction:

In the present days technical environment we uses the internet very frequently so a large range of systems uses the wide range of networks and for a wide variety of applications drives need to support security solutions that meet the requirements of a wide variety of customers. Here in the present day's mobile computing environment mobile consumers and service providers focus on secure mobile services and devises. The various security soft wares are available in the market which is frequently used by the users to provide security for their net book, laptop, Personal Digital Assistant (PDA) or Smartphone. Various type of protections uses some of them are using passwords, data encryption, spam filter, antivirus and a firewall. Here in this paper we focus on the security issues in the Wi-Fi (IEEE 802.11) Wireless LAN systems.

(1)Traditional Security Methods:

Basically we divided the wireless security in the two parts one is the Authentication and second one is Encryption. For a wireless client an access point can be identified by using a Authentication mechanisms, on the other hand the encryption mechanism is used for encrypting the original data. In the encryption process we convert the original data in to the coded form so that it is not possible to intercept and decode data. For the authentication process MAC access control lists have been used and for the encryption process 802.11 WEP has been used.

(a) Authentication

For the MAC authentication of wireless client the access points are required ,this show that traffic through only authorized MAC addresses will be allowed through the access point. For checking the validity of the MAC address we use the access point .This validity is checked by checking it against either a RADIUS server external to the access point or against a database within the non-volatile storage of the access point. In this mechanism the authentication is unilateral and easily gathered so it is called the weak authentication mechanism. Basically there are two reasons for which it can be gathered. The first reason is that there exists software which is used to change the MAC address of some 802.11 cards and the second reason is that authentication is tied to the hardware that a person is using and not to the identity of the user. Hence there is a possibility to steal a legitimate user's PC and gain illegal access to a network. In the concept of unilateral authentication we show that to authenticate the user the access points are required but on the other hand the user doesn't authenticate the access point.

(b) Encryption

To provide the encryption in WAP the VPN software is used. In the case of public wireless hotspot providers that are trying to attract as many users as possible by keeping client configuration as simple as possible we frequently use this option. In the case of hotspot customers for connecting them to there company's network they uses VPN software. The VPN software is more popular because it offers the best commercially available encryption strength because of this the VPN is also preferable to many enterprise administrator. The VPN software uses advanced encryption mechanisms, such as AES, so that decryption is virtually impossible.

(c) Wi-Fi Protected Access

The intermediate solution that can be applied to existing WLAN hardware is the Wi-Fi; the Wi-Fi user uses the Wi-Fi Protected Access (WPA).The Wi-Fi Protected access is a standards-based, interoperable security enhancement. The WPA works in such a way that it strongly increases the level of data protection and access control for existing and future wireless LAN systems. The WAP is compatible with the with the upcoming IEEE 802.11i standards. The main advantage of WAP is that when we installed the WAP properly then it provides an assurance to the wireless LAN users that only authorized persons are able to access network so it prevents the unauthorized users to used there private network. The main goals for creating the Wi-Fi Protected Access was: Available immediately.

(i) A strong, interoperable security replacement for WEP.

(ii) For both the home and the large enterprise users the WAP is Applicable.

The 802.11 authentications and encryption were improved to meet these goals.

(2) Terms:

Some terminologies that are used to understand 802.1x security mechanism are as follows. The figure 1 shows the location role of each one of these terms in the authentication process.

(a) Supplicant

The supplicants are the end user systems that are used for seeking access to the network.

(b) Authenticator

For network access control the access points are required and called authenticator.

(c) Authentication Server (RADIUS Server)

Authenticates the end user, negotiates key material with the end user, and controls access to the network via the authenticator.

(d) EAP

EAP refers to the Extensible Authentication Protocol. For negotiating other security protocols this protocol is used and it also used as a secure protocol.

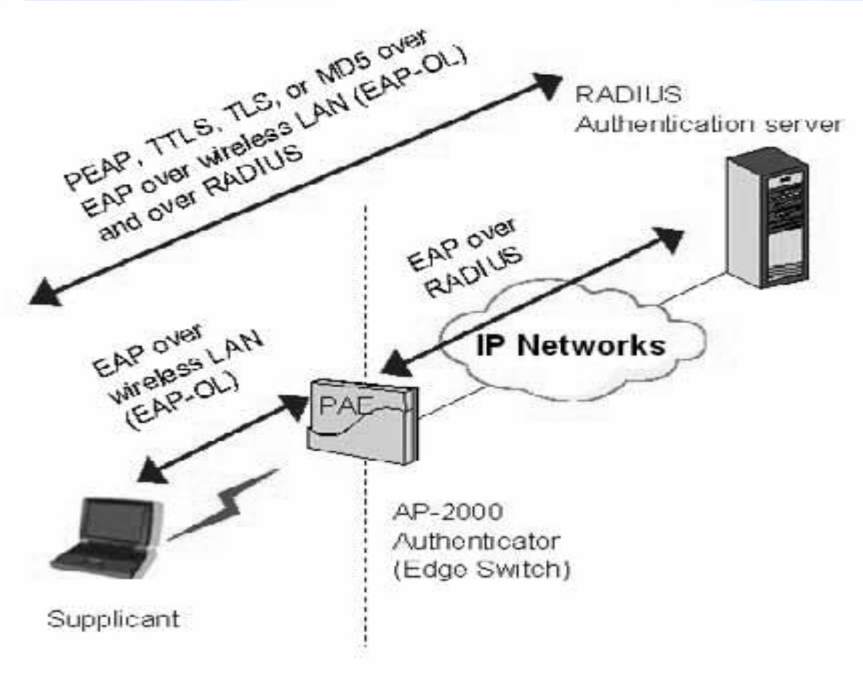

Figure 1: EAP and 802.1x

(e) EAPOL (EAP over LAN)

EAPOL refers to the EAP over LAN and is used to identify the version of EAP over wireless networks we used EAPOL.

(f) PAE -Port Access Entity

The port access entity is used as the toggle switches. No traffic allowed passing except for 802.1X traffic when switch is open. The user data is allowed to pass after authentication is successful, and the switch closes.

(3) SECURITY AND AD HOC NETWORKING TECHNOLOGIES:

A network is called an ad hoc network when it does not rely on any infrastructure such as routers in wired and access points in wireless networks. Hence we can say that the ad hoc network is the network in which the communicating nodes do not necessarily rely on a fixed infrastructure. Now when the concept of as hoc network came in existence there are some new challenges arises for the necessary security architecture they apply. The ad hoc network is designed for specific environment and may have to operate with full availability even in difficult conditions. We use various security solutions in the traditional networks but these security issues are not directly applied in the ad hoc network. In an ad hoc network any type of fixed network is not required for managing the operation it can be formed, merged together or partitioned into separate networks on the fly. In some cases the mobile may be the nodes of the ad hoc networks which apply the wireless communication to maintain the connectivity. The network used in the case of mobile wireless devices is called as mobile ad hoc networks (MANET). However the mobility is not a requirement for nodes in ad hoc networks. The static and the wired nodes are used in adhoc networks, which may make use of services offered by fixed infrastructure. In the ad hoc network basically the security issues are different as compare to other network technologies these technologies are not fully applicable in ad hoc network. Basically in adhoc network the performance of nodes are critical in adhoc network, since the amount of available power for excessive calculation and radio transmission are constrained. On the other hand the available radio frequencies and the bandwidth may be heavily restricted and may vary rapidly. As we know that the amount of available memory and CPU power is typically small, the implementation of strong protection for ad hoc networks is non-trivial.

(a)Physical Security

On comparing to the adhoc network with any fixed wired network we see that in ad hoc networks especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However the overall protection of the network is highly dependent on the ad hoc networking approach and the environment in which the nodes operate. Basically for ad hoc networks that consist of independent nodes and work in a hostile battlefield, the physical security of single nodes may be severely threatened. In such scenarios, the protection of nodes cannot rely on physical security. In the case of the classroom example scenario, the physical security of a node is an important issue to the owner of the node. This could perhaps be for privacy reasons, but the breaking of the physical security does not affect the security of the system as such.

(b)Security of Network Operations

In the case of ad hoc network basically the security can be based on the protection in the link or network layer. The logical link layer offers strong security services for protecting confidentiality and authenticity in some ad-hoc solutions. All of the security requirements need not be addressed in the network or upper layers in this case. In the case of some wireless LANs, link layer encryption is applied. The security services are implemented in higher layers in many of the cases, for instance in network layer, since many ad hoc networks apply IP-based routing and recommend or suggest the use of IPSec. For handling the rapid changes in the networking environment we use the MANET routing protocols. As we know that routing protocol are responsible for specifying and maintaining the necessary routing fabric for the nodes, the protocol must be protected from any attack against authenticity, confidentiality, non-repudiation, integrity, and availability. If confidentiality of the routing information is threatened, the adversary could be able to identify or locate nodes by eavesdropping the routing traffic they send and forward. The users of the ad hoc network are very vulnerable to all kinds of attacks without the protection of location, identity and communication; the users may not be able to carry out there missions at all if availability of the network is broken, and as the network is broken so the communication links are broken or compromised. If we use the public key cryptosystem authenticity and integrity of routing information are often handled in parallel. Here the digital signatures are applied for both confirming the origin of the data and its integrity. The attacker is able to destroy messages, manipulate packet headers or even generate false traffic without any integrity protection, so that the actions cannot be distinguished from hardware or network failures. Nodes can confirm the source of new or changed routing information by using the Authenticity of the routing data. On the other hand if authenticity is not guaranteed, the adversary could perform impersonation attacks, divert traffic to arbitrary destinations or even scramble the routing fabric so that connectivity is severely broken in the ad hoc network. In worst case, the attacker can perform his actions and leave the network without being regarded as a malicious party.

(c)Security of Key Management

Basically in any of the distributed system, in the ad hoc networks, we uses a proper key management system because the whole security is based on the use of a proper key management system .An environment –specific and efficient key management system is needed because the ad hoc networks significantly vary from each other in many aspects .For providing the protection to the nodes against eavesdropping (for example) by using encryption, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. The exchange of encryption keys may have to be addressed on-demand for very rapidly changing ad hoc networks. In the case of less dynamic environment such as class room, the keys may be configured manually. The whole protection mechanism relies on the security of the private key in the case when we use the public key cryptography. Consequently, as the physical security of nodes may be poor, private keys have to be stored in the nodes confidentially, for instance encrypted with a system key. In the case of dynamic ad hoc networks, this is not a wanted feature and thus, the security of the private key must be guaranteed with proper hardware protection (smart cards) or by distributing the key in parts to several nodes. For preventing such types of attacks the hardware protection alone is not an adequate solution. Hardware protection is, however, never alone an adequate solution for preventing attacks as such. In the case of the adhoc network as we know no any centralized recourse exist so a centralized approach in key management is may not be an available option in this case. However centralized approaches are vulnerable as single point of failures. There is an inadequate protection approach in which we perform the mechanical replication of the private keys. For example, the private keys of the nodes simply have then a multiple possibility to be compromised. Hence a distributed approach in key management is needed for any cryptosystems.

(d)Access Control

In the ad hoc networking the access control is an applicable concept as there usually exist a need for controlling the access to the network and to the services it provides. Several access control mechanism working in parallel because the networking approach may allow or require the forming of groups in for instance network layer. The routing protocol must guarantee that no authorized nodes are allowed to join the network or a packet forwarding group such as the clusters in the hierarchical routing approach in the network layer. The access control mechanism must guarantee that unauthorized parties cannot have accesses to services, for instance, the vital key management service in the application lavel.

(4)SECURITY THREATS IN AD HOC NETWORKS:

In the case of adhoc network environment the security threats are divided in to the two groups. The first one is passive attacks which typically involve only eavesdropping of data. And the other one is active attack which involves actions performed by adversaries, for instance, the replication, modification and deletion of exchanged data. There are some types of external attacks which are typically active attacks that are targeted, e.g., to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. There are some external attacks that attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. In the ad hoc network the internal attacks are more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus, protected with the security mechanisms the network and its services offer. Thus, such malicious insiders who may even operate in a group may use the standard security means to actually protect their attacks .As such types of malicious parties' compromises the security of whole ad hoc network so it is called the compromised nodes.

(5)Denial of Service:

The unauthorized access unintentionally failure or malicious action forms the severe security risk in any distributed system and is called the denial of service threat. The area of application of the ad hoc network is responsible for such type of attacks. There are many form of denial of service attacks the classical way is to flood any centralized resource so that it no longer operates correctly or crashes, but due to the distribution of responsibilities this may not be an applicable approach in the adhoc network. However there are more secret threats available in the ad hoc networks: as we discussed in the ex the routing protocols may be reconfigured by using the compromised nodes so that they send the routing information very frequently, thus causing congestion or very rarely, thus preventing nodes to gain new information about the changed topology of the network. In this case if the compromised nodes and the changes to the routing protocols are not detected, the consequences are severe, as from the viewpoint of the nodes the network may seem to operate normally .The new type of failure which we called the byzantine failure derived by this kind of invalid operation of the network initiated by malicious nodes.

(6)SECURITY – THE UNSOLVED PROBLEM FOR MOBILE AGENTS:

The definition of the mobile agent says that it is a computer program that migrates from one computer to another computer autonomously and continues its execution on the destination computer. There are basically two issues involved one is of protecting the host machine and the other is protecting the mobile agents. Different types of threats are caused by mobile agents. These threats that are caused by the mobile agents are harmful for the users in such a way that thread distract the files in the internal/external data storage, these threats are responsible for destruction of current execution environment ,destruction of hardware. The Mobile agent and host are vulnerable to a number of threats some of them are:

(A)Agent to Platform: In this category we represent the set of threats in which the agents' exploit security weakness of an agent platform or launch attacks against an agent's platform. In this category the threats include masquerading, denial of services and unauthorized access.

(a) Masquerading

The masquerading may be define as when ever an unauthorized agent poses the identity of another agent, then it is said to be masquerading. The masquerading agents may act as unauthorized agents to gain access services and recourses.

(b) Denial of Services

By consuming or corrupting the agents platform's computing resources the mobile agents can launch denials of services attacks. Basically for exploiting system vulnerabilities the denials of service attacks can be launched. For reducing the risk of introducing malicious code in to an organization computer system we use program testing, configuration management and design review.

(c) Unauthorized Access

For preventing unauthorized users or processes from accessing services and recourses for which they have not given permission and privileges various access control mechanism are used. The access control mechanism requires the platform or the agent to first authenticate a mobile agents identity before it is instantiated on the platform.

(B)Security Services

(a) Confidentiality

In the confidentiality we says that only authorized users can only access, read and decode the data hence by this process the sensitive data must be secure.

(b) Authentication

In the authentication process agent server must authenticate itself to the agent and an agent must authenticate it to the host.

(c) Integrity

The process of integrity provides the assurance that during the process of transmission the traffic is not altered.

(d) Authorization

In the authorization process the host enforces strict access control to its recourses.

(e) Auditing

Auditing keeps track of the system and if an agent misbehaves, it will be logged.

(f) Access control

The process of access control defines only authorized users are able to access the recourses.

(7)DISTINGUISH BETWEEN PRIVACY AND SECURITY:

There are basically two terms Privacy and Security the concept of these terms are little bit confusing. Some people say that these two terms are same but basically these are two different aspects that are closely related to each other. So for relating these two terms we can say that security is necessary tool to build the privacy. Privacy is recognized as the necessity human right by the European Union (Privacy Directive) and the OECD (Principles of Fair Information Practice). In the M-commerce environment, privacy is an important issue to gain widespread adoption by consumers around the world. Now suppose we consider an example of GSM technology then in this case the privacy issues means voice privacy – can someone listen to my call? Now if we follow the privacy goals then this allow us to say no, and if we talk on the security issues then we uses the security technology ,encryption that allows me to force it. Here in this example both the security and privacy goals are same. Here in this example the security goal implies authenticating handsets. In some cases this may be done by RF fingerprinting, which is not a privacy issue. In the security issues we securely authenticate that the handset is the one that is linked to an account, thus, ensuring that the right person is billed. Both the security and privacy aspects are orthogonal to each other. There is a term called Secure Socket layer which offers the privacy against the eavesdroppers, but this is better called the confidentiality.

Conclusion:

By the above discussion we can say that there are various security issues in the wireless and in adhoc networks. There are different technologies we use to achieve these security goals. Various security mechanisms we use in these types of networks. We use the concept of authentication, authorization, auditing, etc. for providing the security.

References:

- D. Arnold, A. Bond, and M. Chilvers. Hector: Distributed objects in Python. Dr Dobb's Source Book (Distributed Objects), 22(13), Jan. 1997.
- J. Bates, D. Halls, and J. Bacon. A framework to support mobile users of multimedia applications. ACM J. Mobile Networks and Nomadic Applic. (NOMAD), 1996.
- Berry and K. Raymond. The A1p architecture model. In Proc. 3rd IFIP Int
- Conf. on ODP, pages 55{66, 1994.
- W. Brookes. A type description language supporting interoperability in open distributed systems. In Proc. 1st IFIP Workshop on Formal
- Deering,S(1996)Internet protocol version 6 specification
- Hendrick C (1988) Routing Information Protocol RFC 1058 updated by RFC 2453 (RIPv2)