Wireless Network Security And Mobile System

Lalita Devi
Lecturer, Computer Science, Govt.P.G.College, Sec- 9, Gurgaon, Maharishi Dayanand University, Haryana, India.

Abstract: The current wireless local area network face some of the major security issues, In recent years, with the popularity of a variety of wireless devices and wireless local area network with its easy access, integrity, availability and confidentiality. Wireless LANs go on improve the quality of life. The evolution of security standardization based upon the work of the IEEE has evolved from WEP to WPA which introduced new key management and integrity mechanism through to WPA2 (IEEE 802.11).

Keywords: 802.11 Wireless standard, WAP, SSL.

1. Introduction:
A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networks operate using radio frequency technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. 802.11 is a wireless LAN Standard which is increasingly being adopted by many wireless devices to establish communication at the Physical and Data link layer of OSI Model. WEP (Wireless equivalent protocol)-data is encrypted with WEP to protect the wireless link between the client and the access points. WAP (Wireless application protocol)-Wireless application protocol is a technical standard for accessing information over a mobile network. SSL (Secure sockets layer)-is a standard security technology for establishing an encrypted link between a server and a client. It secure data especially during online transaction or when transmitting the confidential data.

2. Wireless Environment:
Communication in the wireless environment has its own issue and challenges. Generally it has the following characteristics:-

i) Relatively high error rates.
ii) Relatively low bandwidth and data rates.
iii) Need for low power consumption to preserve battery life of mobile system.
iv) Mobility of nodes add more complexity because of topology changes.
v) Signal fading.
vi) Handoff issues.
vii) And other challenges. All these affect design and design for security.

There exist many forms of wireless communications and networking. Some very popular forms of wireless communications are:-

2.1 Satellite communication: Uses microwave links and provides global connections of many network infrastructures. An artificial satellite sent to space for the purpose of telecommunications. Three types of satellites:

i) GEO - Geostationary Earth Orbit Satellites.
ii) MEO - Medium Earth Orbit Satellites.
iii) LEO - Low Earth Orbit Satellites.

2.2 Cellular Network: Cellular Network widely used recently. It is Quickly increasing in popularity all over the world. In which geographic area is divided into cells and each cell is serviced by a Base station. Several stations are served by a mobile telecommunication Switching Offices (MTSO) or similar structure. Base stations connect the mobile user to the MTSO. MTSO connects base station to telephone switching office. The first generations of system was AMPS (Advanced Mobile Phone Service), which used analog communications. The second generation uses digital traffic channels, encryption, error detection, correction and allows channel access to be dynamically shared by all users. The third generation system will have the voice quality that is comparable to Public Switched Telephone networks.

i) Higher data rates.
ii) Symmetrical and Asymmetrical data transmission rates.
iii) Support for both packet and circuit switched data networking.
iv) Support for wide variety of mobile equipment.
v) More flexible to accept new services and techniques.

2.3 Cordless System: Cordless systems are used inside homes and buildings, because the range is limited usually to the same building or some short distance from base station. Cordless systems allow wireless communications between cordless devices such as telephone to a single multiple base stations using TDMA (TIME DIVISION MULTIPLE ACCESS) and TDD (TIME DIVISION DUPLEX) communications. The handsets communicate with a base station connected to a fixed telephone lines.

2.4 Wireless local loop: It is the popular way to provide wireless last mile connections between the end user and the local switching telephone centre. Wireless local loop allows reduction in installation cost and time. Selective installation is possible (only install when customer desires service, not in anticipation of the customer desiring service).

2.5 Mobile IP: A user is able to maintain connect ability to the Internet while moving from one access point to another. It uses process registration, agent solicitation, move detection, and tunnelling to achieve this objective. It is designed to allow mobile devices users to move
from one network to another while maintaining a permanent IP address. The mobile IP protocol allows for location independent routing of IP datagram’s on internet. Examples of use are in roaming between overlapping wireless systems. Mobile IP is not required in cellular systems such as 3G.

2.6 Wireless Local Area Networks (WLANs): It’s rapidly becoming very popular due to following characteristics: -
   i) Decrease in size of electronic and digital equipment.
   ii) Need for mobility
   iii) Cost effectiveness
   iv) Rapid deployment ability
   v) Speed of mobile computing devices
   v) Convenience

There are four types of wireless LANs:-

LAN Extension
Cross building interconnect
Nomadic access
Ad-hoc networking
Bluetooth

3. 802.11 Wireless Standard:-
   • This is a wireless LAN standard, which is increasingly being adopted by many wireless devices to establish communications at the physical and data link layers of the OSI model.
   • In 2000 vendors sold around a million 802.11 network interface cards, and sales are expected to go up to 3.9 million in 2004.
   • The 802.11 architecture uses the wired equivalent privacy protocol (WEP).
   • Data is encrypted with WEP to protect the wireless link between clients and access points.
   • Network administrators distribute a WEP-algorithm-based key for authorized users, which prevents access by unauthorized users.
   • The protocol has authentications, deauthentication (this service is invoked whenever an existing authentication is to be terminated), and privacy provisions.
   • Authentication (and deauthentication) services are used for establishing identity of a station. The standard does not specify any particular authentication scheme.

4. WAP (Wireless Application Protocol):
   WAP is a technical “standard “created by wireless and Internet companies to enable internet access from a cellular phone. WAP is an open standard which empowers mobile users of wireless terminals such as wireless phones, pagers and PDA’s to access and interact with internet information and service instantly. It is designed to work with all wireless network technologies such as GSM, CDMA, TDMA, FLEX, ReFLAX, IDEN, TETRA, DECT, Data TAC and MOBITEX based on existing standards such as IP, XML, HTML and HTTP. WAP is independent of OS means it can be implemented on any OS including Palm OS, EPOC 32, WINDOWS CE, OS/9, JAVA OS, etc.

In the latest class of secure wireless protocols from the WAP Forum, client-side certificates are specified and used as part of client-side authentication and non-repudiation services.

Wireless Device is the entity that receives content from internet via a WAP Gateway. This is usually a WAP Browser. WAP Browser is software running on the WAP content arriving from the internet and decides how to display it on WAP Device.

4.1 WAP Programming Model:-

4.2 WML (Wireless Markup Language):
Wireless markup Language formerly called HDML (Handled Device markup Language). It is a tag Language that allows the text potion of web pages to be presented on cellular phones and personal digital Assistants (PDA’s) via wireless access. WML is used for delivering data to WAP Devices and is HTML like in its appearance.

4.3 Components of WAP Architecture:
(a) WAE (Wireless Application Environment): Wireless application Environment is general purpose application environment based on the architecture of World Wide Web and the mobile telephony technologies. It contain WML and WTA. The primary objective of WAE is to provide interoperable Environment.

(b) WSP (Wireless Session Protocol): WSP based on HTTP provides a lightweight session layer to allow efficient exchange of data between two applications and it establish the connection at the beginning. The primary objective is too optimized for low-bandwidth bearer network with long latency.

Application layer consistent with two layer services:-
(i) Connection oriented service that operates above the transaction layer protocol (WTP).
(ii) Connectionless service that operates above a secure and Non- secure datagram service (WDP).

(c) WTP (Wireless Transaction Protocol): It is a standard used in Mobile telephony to provide the internet content and advanced telephony services to the digital Mobile phones. The WAP Transaction Protocol (WTP) layer provides transaction support, adding reliability to Datagram service provided by the WDP.

(d) WTLS (Wireless Transport Layer Security): WTLS is a security level for Wireless Application Protocol (WAP) Applications and it uses cryptographic algorithms for encryption of data. WTLS is based on the TLS/SSL (Transport Layer Security) Protocol. It is optimized to problematic issues surrounding the mobile network. It is a lightweight protocol with all types of wireless Networks as well as for all handheld devices.

(e) WDP (Wireless datagram Protocol): The WAP Datagram Protocol (WDP) provides a common interface to the upper layer of the protocol stack so that they can function independently.

It is the Transport Layer that sends and Receive messages via any available bearer network, including SMS, USSD, and GPRS. WDP perform three basic tasks :
(i) Port addressing
(ii) Segmentation of datagrams and subsequent reassembly of the packets at the receiving end.
(iii) Error reporting.

5. SSL (Secure Sockets Layer):
SSL (Secure Socket Layer) is a standard security technology for establishing an encrypted link between a server and a client. SSL is most widely used security Protocol essentially every commercial web browser and Server support security Web Transaction. In our everyday life we buying Online using secure web pages. SSL is most widely used for web traffic transactions. SSL currently being used in different stages of transaction communication between wireless devices and the wired infrastructure.

6. Advantages of WAP (Wireless Application Protocol) and SSL (Secure Socket Layer):
It is an open standard. It is independent of Operating System means it can work with all types of Operating System. WAP can works with all types of wireless Networks as well as for all handheld devices. WAP enable fast and easy delivery of relevant information and service to mobile uses. It provides a support for secure application and communication. SSL (Secure Socket Layer) is the secured way to transact the Private Information. Through SSL sensitive information keep encrypted and no other one can read during the transmission over the internet.

7. Conclusion:
Transmission with security has become an important issue over time for data. The main goal of this paper is to find out the way of accessing the data on small or handheld devices with security. To achieve this goal we are using the WAP specification which provides the Web like experience on small portable devices like – Mobile phones and PDA’s. WAP is independent of operating system it can works with all types of operating system. WAP enable fast and easy delivery of relevant information and service to mobile users. SSL (Secure Socket Layer) is used in Mobile Phone network Security with various aspects such as access control, confidentiality, authentication, non- repudiation and integrity of data communications.

8. References: