IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Wireless Architectures And Network Security.

Chandrakant D Prajapati[*1], Bhargav P Padhya[2], Suhas A Patel[3]

[*1,2]Department of Computer Science, Ganpat University, Kherva, Mehsana, Gujarat, India

[3]BCA Department, AMPICS, Ganpat University, Kherva, Mehsana, Gujarat, India

cdp01,@ganpatuniversity.ac.in

Abstract

In this paper is simply to define and understand Wireless Architecture and discussing the various protocols that exist in this field today One of the most frequently asked questions put to a wireless broadband service provider by their subscribers is, "what about security?". It is indeed wise for subscribers to be concerned about security, on any type of network. Disgruntled former employees, hackers, viruses, Internet-based attacks, and industrial employees are an unfortunate fact of life in any form of networking today. This paper shows the similarities and differences between security on wire-line and wireless networks, threats to the security of any network. And those elements unique to wireless technology used by SkyRiver available to these potential threats.

Keywords: Wireless networks, Wireless security, Wireless threats, WAP, WWW model, VPN, Adaptive Polling etc.

Introduction

Wireless Communication is simply a medium. Wireless Communication is about the tools used to communicate from one device to another. As subscribers to such technology, one needs to find the best type of wireless services that suits his needs. The goal of this survey paper is not to market any particular product that utilizes wireless technology of any sort. Wireless networking provides many advantages, but it also coupled with new security threats.

Wireless Application Protocol, also known as WAP to those who inhibit the Wireless World, is a survey paper of its own. However, WAP will be addressed as well not only because there is a need to discuss WAP, but because it would be unjust to not even mention WAP when discussing Wireless Technology. WAP has been one of the most recent and the most fully developed protocols out there. In very little time, WAP served as a basis and model for other protocols such as another very recent protocol on the market today.

A wireless network has all of the properties of a wire-line network (except, of course, the wire), and thus security measures taken to ensure the integrity and security of data in the wire-line network environment are applicable to wireless networks as well. The primary difference between a wire-line network and a wireless network is at the physical layer (wire versus airspace) and all other network strengths and weaknesses remain.

With the advent of wireless broadband service, wireless service providers and equipment manufacturers have included an additional set of unique security elements that are not available in the wire-line world. Based on these elements, the argument can easily be made that wireless networks are at least as secure as wire-line networks.

Wireless security can be broken into two parts: Authentication and encryption.

Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa, while encryption mechanisms ensure that it is not possible to intercept and decode data. For many years, MAC access control lists have been used for authentication, and 802.11 WEP has been used for encryption.

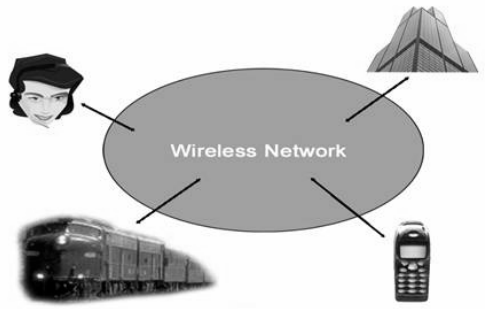

Figure 1: Wireless network and product

Components of Wireless Communication

Although each protocol has different specifications and criteria, there are general characteristics and goals that each protocol tries to achieve. Several of these protocols are discussed in this survey paper as well. Below are some general guidelines these protocols.

- ***Unlimited roaming and range*:** The location of the user with the portable device is irrelevant. No matter how far or how near a user is from the base provider, data can still be sent and received.

- ***Guarantee of Delivery*:** All messages and data is guaranteed to be delivered regardless of where a user is located or the user's status. Even if the portable device is turned off, when it is turned on again, the user will see a new message.

- ***Dependability of Delivery*:** All messages are guaranteed of accurate and full transmission.

- ***Notification*:** Notifies the user that there is data that has been sent and needs to be looked at.

- ***Connectivity Options*:** Send and receive are given a wide range of options not only in hardware for the portable device, but also are given options in receiving messages (choosing a type of connection for instance).

- ***Millions of Users*:** Ability to engage millions of users.

- ***Priority Alerts*:** Able to distinguish between messages and data that are of higher importance than others. Able to control high-priority data traffic and do so correctly and rapidly.

- ***Communication*:** The ability to communicate between one user to another through one portable device to another where each portable device holds reliable and user-friendly software applications.

- ***Host Mobility*:** One host contains its settings on a network – its IP address, Subnet Mask, Gateway Address, and so on.

Wireless Application Protocol (WAP)

The Wireless Application Protocol has become the standard for communication between server applications and its clients. That is exactly what the Wireless Application Protocol is; for example, WAP is used as a standardized method so that a cellular phone can talk to a server among the cellular network that it belongs to. Because WAP has become so global, it no longer is bounded by the means of the cellular market. WAP has become the link of the Internet to the Mobile World, bridging a gap between two of the top industries of the world.

WAP also follows a model similar to the Internet. The Internet itself has a layered protocol stack. The portable device using WAP has browser software that connects to a WAP Gateway and sends requests to receive data from web servers. Data could be a web page or an email. The content is then sent back to the portable device, and depending on the capability of the portable device to receive and view data, the data is received and viewable.

WAP founders include Ericsson, Nokia, Motorola, and Phone.Com (formerly Unwired Planet). In December 1997, these three large companies, all with strong influence on the Mobile market, formed the WAP Forum, an organization with open membership and now with over 300 members worldwide. The purpose of this forum is to make sure that the specifications of WAP do not go astray.
Basic specifications of WAP include: micro browsing, scripting, wireless telephone applications, and a layered protocol etc.

The WAP Model

The World Wide Web Model follows a three-layer protocol. Referring to the diagram, the WAP model follows the World Wide Web model in that there is an Origin Server, a Proxy, and a Gateway. The Origin Server serves as the main web server where one would find CGI scripts and other sorts of scripts. The Origin Server also holds content that Clients will want to view. The Proxy serves as an application that connects from the Origin Server to the Gateway. The Proxy sends and receives content to the Gateway.

The Gateway is another server that acts as an origin server between the client and the origin server. Most clients would not be able to tell if they are in contact with the Gateway service. The Gateway serves as a protection for the Origin Server.

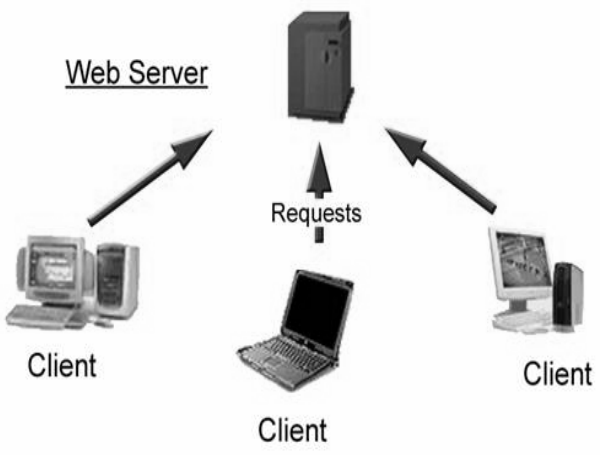

Figure 2: WWW Model. Clients make requests to the server for data.

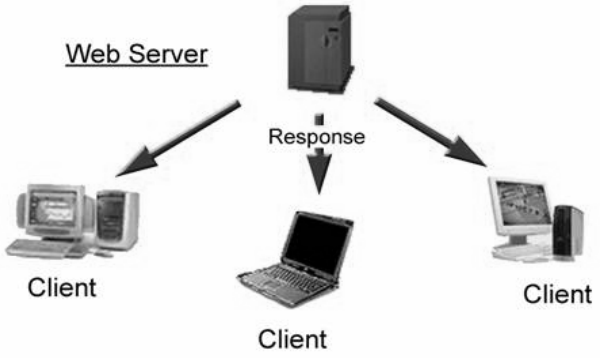

Figure 3: WWW Model. Web Server responding to Client requests and sending requested data.

The WAP Model has a similar set-up as the World Wide Web Model. There is also an Origin Server with a Gateway. Again the Origin Server contains content and scripts, while the Gateway acts as a server to the Clients. The Gateway uses the proxy. In the WAP Model, the Client, for example, could be a mobile phone. The Client makes a request in WML or in HDML depending on the device and request, and the Gateway will encode the request to the Origin Server and once the Origin Server responds with information to send, it sends the data back through the Gateway, where the Gateway will encode the information again, and send it to the Client.

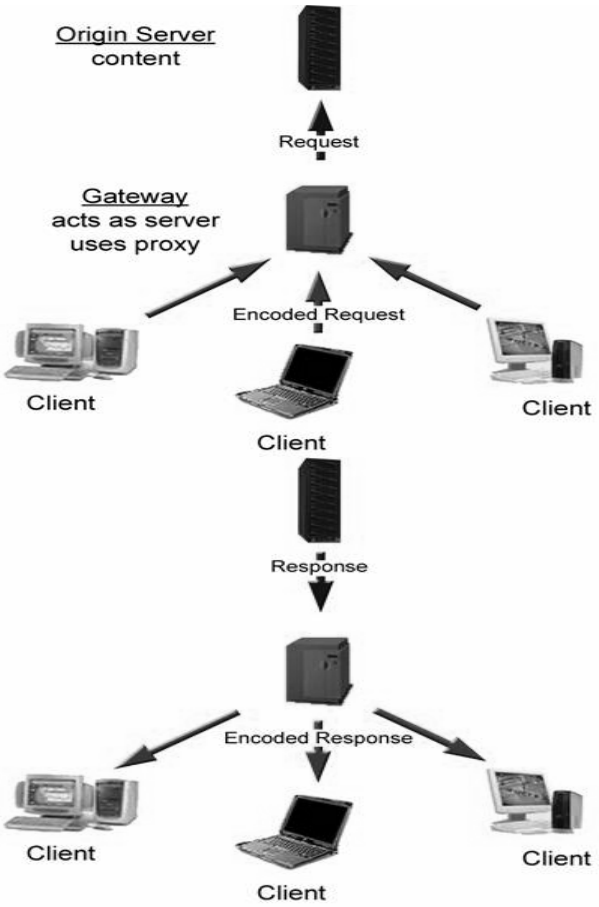

Figure 4: The WAP Model follows closely with the WWW Model.

WAP Architecture is divided into several layers. This is often called the 'WAP Stack'.

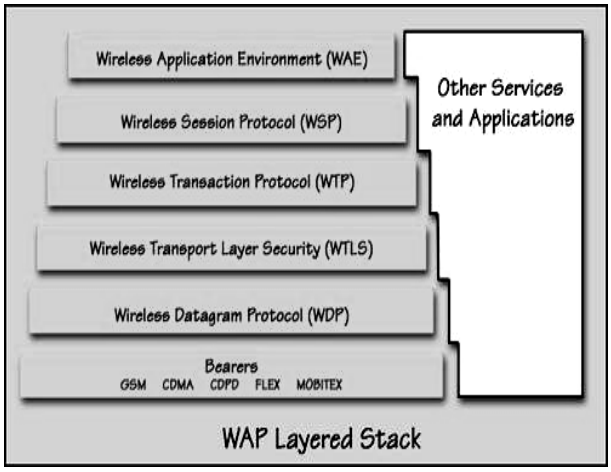

Figure 5: WAP Architecture

Wireless Application Environment (WAE)
WAE is able to be used with Phone.com's HDML, the World Wide Web's HTML, and should work with other technologies of the web, such as Uniform Resource Locator (URL) and Hyper Text Transfer Protocols (HTTP), and other modern technologies that are found within a mobile network.
In the WAP model, WAE would be the application environments that sends and receives requests from the Clients to the Gateway to the Origin Server. WAE relies heavily on URL and HTTP ideals by assuming the existence of a gateway server and support from the WAP gateway in the network.
WAE is composed of user agents such as browsers, text editors, date book or phonebook. WAE is also composed of scripting, higher-lever programming languages and image formats. WAE uses languages such as WMLScript (similar to JavaScript) and WML (similar to HTML).

Wireless Session Protocol (WSP)
The Wireless Session Protocol is the layer that deals with communication between client and proxy or server. The WSP provides dialog between client and server. WSP provides the following services:

Opens a session of communication between client and server.

Establishes a protocol and negotiation between client and server.

Exchanges encoded data between client and server

Exchanges request and replies between client and server.

Supports several asynchronous transmissions of data.

Wireless Transaction Protocol (WTP)
The Wireless Transaction Protocol, in a simple definition, deals with the transaction of data. WTP handles transactions, re-transmission of data, and with the separation and concatenation of data.

This particular protocol has a separate interface that manages and referees the WTP layer and the settings of the handheld device. This management application is known as the WTP Management Entity. For WTP to work, the following factors are important:

The handheld device is within coverage area of base agent.

The handheld device is turned on and has a power and is reliable.

Resources are adequate especially with the CPU and memory.

WTP settings are correctly inputted.

Wireless Transport Layer Security (WTLS)

The Wireless Transport Layer Security is the layer that handles security of data and validity of data between two communicating to manage, start, and finish security issues between two portable devices.
To transport data, WTLS needs: the source address and port number to identify the message creator, and from where the message is being sent, the destination address and port number to which data is being sent, and of course, the data itself. WTLS has a connection interface which provides a connection protocol between client and server.

Wireless Data Protocol (WDP)
The Wireless Data Protocol acts as the communication layer between the upper level protocols (WTLS, WTP, and WSP), and the bearer services. WDP allows the upper layers to function independently from the wireless network at hand, as long as the WTP layer is specifically set to the settings of the bearer settings.

The function of the WDP is to provide a stable environment so that any of the underlying bearers can operate using WAP. WDP can be adapted to different bearers with different services however the services offered by WDP remains constant thus providing a continuous interface to the upper layers of the WAP stack.

Threats to Network Security

Any network, wireless or wire-line, is subject to substantial security risks and issues. These include:

- Threats to the physical security of a network
- Unauthorized access
- Privacy

Physical Security
Given the physical security of wire-line networks on the wire, anyone gaining access to that wire can damage the network or compromise the integrity and security of information on it. Without the proper security measures in place, even registered users of the network may be able to access information that would otherwise be restricted. Disgruntled current and ex-employees have been known to read, distribute, and even alter valuable company data files. Network traffic can be intercepted and decoded with commonly available software tools once one has physical access to the network cabling. In a wire-line network including cable systems, countless cases have been documented of wiretapping, hacking by

authorized users and even people down the street hacking into their neighbor's computers.

Subscribers, regardless of whether or not they have wireless segments on their networks, need to have the appropriate security products for their environments, the proper security levels set for their users, and an on-going process to audit the effectiveness of security policies and procedures. Physical access to network wires needs to be protected. Unfortunately, the vast amount of wire inherent in most networks provides many points for unauthorized access.

Unauthorized Access

Another area of concern for security-conscious subscribers is the growing use of the Internet. Often, if users from inside can get out to the Internet, then users from outside can get into a network if proper precautions haven't been taken. And this applies not only to the Internet, but also to any remote network access capabilities that might be installed. Remote access products that allow traveling sales and marketing people to dial in for their email, remote offices connected via dial-up lines, intranets, and "extranets" that connect vendors and customers to a network can all leave the network vulnerable to hackers, viruses, and other intruders. Firewall products offering packet filtering, proxy servers, and user-to-session filtering add additional protection.

Many products are available to help subscribers secure their networks from the above threats. User authentication and authorization is provided by most network operating systems, and can be enhanced by adding third-party products.

Privacy

Perhaps the most difficult threat to detect is someone just looking at (and likely copying) raw data on the network. Wire-line networks are particularly vulnerable to eavesdropping. Most Ethernet adapters on the market today offer a "promiscuous mode" that, with off-the-shelf software, enables them to capture every packet on the network. Most network administrators have some kind of "packet sniffer" and/or network traffic analyzer for trouble-shooting the network. Inexpensive and readily available hardware and software let anyone with physical access to the network to read, capture, and display any type of packet data on the net.

While data encryption is the only line of defense against this kind of threat unfortunately, no wireline network service provider incorporates this technology as even an option that subscribers could use with their product.

Security on SkyRiver's Wireless Network

We can see that data security considerations impact the entire network architecture. And while these data security considerations apply equally to wireless networks, the technology used in the physical layer (airspace) of wireless networks actually increases overall network security, as follows:

Spread Spectrum Technology

SkyRiver's wireless networks use a form of spread-spectrum radio transmission technique. Spread spectrum technology was first introduced about 50 years ago by the military with the objective of improving both message integrity and security. Spread-spectrum systems are designed to be resistant to noise, interference, jamming, and unauthorized detection.

Spread spectrum communications is a means of transmitting a signal over a much wider frequency bandwidth than the minimum bandwidth normally required to transmit the information. The minimum is for the spread spectrum to have a bandwidth of at least 10 times the information bandwidth.

A typical radio signal contains both the data itself (which is the useful content) and a carrier frequency, which is modulated or blended with the data signal in order to "carry" the transmission across the operating range of the transmitter.

In SkyRiver's Direct Sequence Spread Spectrum (DSSS) transmissions, another element is introduced called a pseudo-noise (PN) code sequence. This is a binary – and hence digital – code sequence which, when modulated with the carrier frequency and original content, causes the resultant signal to spread across a much wider frequency spectrum, whereas the original radio signal would have occupied only a specific radio frequency. This has the resultant effect of dissipating the signal intensity over a broad range of frequencies, thus shrouding the transmitted signal, and making it indistinguishable from random white noise.

At the receiver end, in a process known as "correlation", a similar pseudo-noise code sequence matching exactly the one used by the transmitter is generated in order to "decode" the transmission by reconstituting the spread spectrum signal into intelligible information again. Naturally, without this code sequence, the spread spectrum signal is useless. Therein lies the security-enhancing feature of DSSS transmissions, which explains why there is military interest in the technology. Because DSSS transmissions are harder to detect, there is a lower probability of interception. Because it does not occupy specific radio frequencies, it is harder to jam.

And because it employs binary code sequences to "encrypt" the transmitted data, it makes it hard for unauthorized parties to "listen in", or to spoof or imitate network members.

Station Authentication

SkyRiver's wireless network like most wireless networks, has the ability, through an authentication management function, to specifically authorize or exclude individual wireless stations. Thus an individual wireless user can be included in a network, or, at any time, locked out. Stations also need to know a wide variety of information, including radio domains, channels (specific frequencies) as well as IP addresses and subnets in order to access the network. Thus unauthorized network access becomes very difficult even for hackers who possess the equipment to attack the SkyRiver network.

Physical & Network Security

SkyRiver's network elements are in secure locations with environmental controls (including but not limited to remotely monitored intrusion alarms). These equipment rooms require specific authorization for access. Moreover, since the access points used in wireless network function as routers, individual wireless subscribers are isolated from the majority of network traffic. Network subscribers are unable to gain IP access to any network elements again limiting the possibility of network penetration or access to raw network packets.

VPN

It is a commonly accepted fact that Internet technologies have changed the way that companies disseminate information to their customers, partners, employees, and suppliers. Initially, companies were conservative with the information they published on the Internet – product information, product availability and other less business critical items. More recently, using the Internet as a means of providing more cost effective access to business critical information such as order status, inventory levels, or even financial information has gained wider acceptance through Virtual Private Networks or VPNs. A Virtual Private Network is a business solution that provides secure, private connections to network applications using a public or "unsecured" medium such as the Internet. With a VPN deployed across the Internet, virtual private connections can be established from almost anywhere in the world.

Adaptive Polling

SkyRiver overcomes many of the problems inherent in wireless networks by centralizing control of the wireless network at the SkyRiver Base Station. The SkyRiver Base Station uses a highly optimized polling technique to tell remote wireless stations when they can transmit.

First of all, SkyRiver polling is adaptive. Each station's polling interval is determined by a number of independent factors, including the remote station's recent usage history. The total number of currently connected systems (among other variables) is used to determine maximum and minimum polling intervals.

Second, SkyRiver polling is dynamic. As remote stations transmit less frequently (i.e. they do not have a packet to transmit when polled), they are polled less often. For example: a station, which has been dormant for several minutes, may not be polled for an extended period of time. Stations that have data ready to transmit when polled are polled more often. This enables SkyRiver to make optimum use of the wireless bandwidth, while still maintaining a high level of "fairness" between wireless clients.

To avoid problems associated with pure polling schemes, SkyRiver also employs a "free for all" period to enable stations that have data available but are low in the polling queue to transmit without much delay. The "free for all" period allows a station that may not have transmitted for a long period of time to begin transmitting once again and move to a higher priority in the polling scheme.

The determination of polling intervals based on a complex combination of factors is finely tuned and the result of years of research into wireless performance in production environments. SkyRiver polling and the associated "free for all" period, combined with super-packet aggregation, allow wireless networks running SkyRiver to perform at the highest rate possible.

Conclusions

It's important to point out here that absolute security is an abstract, theoretical concept - it does not exist anywhere. Any network, wireless or wireline, is vulnerable if precautions are not taken or if someone is motivated enough and has enough money. No one wants to risk having the network data exposed to the casual observer or open to malicious mischief. Regardless of whether the network is wire-line or wireless, steps can and should always be taken to preserve network security and integrity.

It should be clear from the discussion above that wireless networks can take advantage of all of the security measures available on wire-line networks, and then add additional security features not available in the wire-line world. As a result, wireless networks can be as secure, and in fact more secure, than their wire-line counterparts.

Wireless technology brings together the two biggest industries together: the Internet with the Mobile. Wireless devices used to be used only through big companies and large institutes or organizations with certain needs. Perhaps the United Parcel Service (UPS) needs some sort of wireless device or PDA to communicate with the delivery base to confirm a delivery.

References

[1] Brewer, Borisov, et al, "802.11 Security", http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[2] Arbaugh, W., Mishra, A., .An Initial Security Analysis of the 802.1X Standard.

[3] Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, Department of Computer Engg. Kyung Hee University, Korea Security in Wireless Sensor Networks: Issues and Challenges

[4] Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications",

[5] White paper - Scott Akrie

[6] Joseph B. Evans,* Weichao Wang and Benjamin J. Ewy Department of Electrical Engineering and Computer Science, University of Kansas, Lawrence, KS 66045-7621, USA

[7] Akyildiz, I.F., Wang, X. and Wang, W. (2005) 'Wireless mesh networks: a survey', Computer Networks Journal (Elsevier),

[8] Anton, B., Bullock, B. and Short, J. (2003) 'Best current practices for Wireless Internet Service Provider (WISP) roaming, version 1.0.', Wi-Fi Alliance.

[9] Bharghavan, V. (1997) 'Challenges and solutions to adaptive computing and seamless mobility over heterogeneous wireless networks', International Journal on Wireless Personal Communications:

[10] http://www.wapforum.org

[11] http://www.ieee.com

[12] http://www.wap-resources.net