9 Wireless Security: Wi-Fi, Cellular and Satellite Security[1]

[1] This chapter is based on . Umar, A., "Mobility and Wireless Communications: Applications, Networks, Platforms, and Security," NGE Solutions, April 2004 (target). See www.amjadumar.com for additional information.

9.1 Introduction

The growth of wireless networks and mobile services over the last few years has been tremendous. Naturally, the security concerns are becoming more serious concomitant with the growth of wireless. As more people (estimated to be more than 500 million in 2003) access critical information wirelessly, and as consumers begin to do their business and banking on devices that are connected over wireless networks, wireless security has moved to the forefront.

In essence, wireless networks face the same type of security issues (e.g., privacy, integrity, authentication) as the wired networks do. Wireless security, in essence, is not much different from wired security. The same security concerns exist, whether you are wired or not: authenticate whom you are talking to, secure the data as it travels from the handheld device to the destination host, and ensure that the traffic has not been altered en route. Companies such as Amazon.com and E-Trade do this in the wired world. However, wireless has some unique difficulties such as limited bandwidth, high latency and unstable connections. The main differentiating issue of wireless network security is that the information is transmitted over a common medium (the air). Thus it is easier to tap into and tamper with wireless traffic.

There are a number of stories about eavesdropping of wireless traffic. For example, competitors have been able to capture the emails between HP personnel by simply sitting in the office parking lot with an antenna. Something similar also happened to Sun Microsystems. In addition, information sent by a federal agency wirelessly was intercepted and then used against the agency in a future negotiation. My own students, from a wireless network class that I taught, spent a day in Manhattan and captured a disk full of plain text (un-encrypted data) by simply driving around the Manhattan business district in a car with a simple antenna. They were just doing research to demonstrate how vulnerable wireless communications are (well, that is what they told me!).

The issues of wireless security are not evenly divided. Some areas are more vulnerable than others. For example, Free Space Optics (FSO) systems transmit information by using laser beams – a very difficult technology to intercept – while wireless Ethernet LANs are more susceptible to intervention. In addition, there are issues at different levels (networks, middleware, and applications). The objective of this chapter is to provide

enough details so that a sound solution based on a comprehensive checklist can be developed. The checklist must include the enterprise applications and corporate databases, computing platforms (computers, operating systems), middleware (web servers), and networks (network hardware, routing software, wireless network security). The sections of this chapter start from network layers and proceed to higher-layer approaches and attempt to answer the following questions:

- What are issues specific to wireless LANs, cellular networks, satellites, wireless local loops, and wireless personal area networks?
- How can TCP/IP security through VPNs and IPSec be used to secure wireless communications?
- How does higher level security (such as for WAP) interplay with wireless network security?

We will discuss the issues of mobile applications in a later chapter.

Chapter Highlights

- Wireless security can be discussed at several levels (wireless physical network, TCP/IP, middleware, application).
- Numerous technologies exist to deal with the issues at various levels. Some techniques are better than others.
- Wireless networks impose special problems because the information is carried through the air and thus is easier to tap (you just need an antenna).
- There are many areas of vulnerability in wireless networks:
  - Location services (HLR/VLR) are privacy concerns.
  - The current wireless access points present a large security problem.
  - Mobile ad hoc networks are concerns.
  - Several products use the un-authenticated Diffie-Hellman (DH) algorithm which suffers from a well-known *man-in-the-middle* attack.
  - The Wired Equivalent Privacy (WEP) algorithm, part of the IEEE802.11standard for wireless LANs, is designed to protect wireless communication from eavesdropping.
  - Several weaknesses of WEP have been demonstrated.
- Approaches to deal with wireless network security include:
  - Turn on security at wireless links to avoid eavesdropping even if it is deficient.
  - For example, use WEP because it does provide some security – make up for WEP security by providing higher layers of security (e.g., SSL).
  - Make sure that all access points are themselves monitored and controlled so that no one sets up rogue access points.
  - Treat wireless networks as un-trusted networks. Thus put the internal WLANs outside the firewall so that they are treated as outsiders.
  - Minimize placing critical applications and databases on wireless networks – move them to wired networks behind firewalls.
  - Make sure that the passwords on wireless networks are different than those on the wired networks. Hackers usually capture passwords from wireless networks and then use them to gain access over wired networks.
- Some emerging wireless networks (FSO, UWB) offer very strong security features.
- Mobile ad hoc networks (MANET) raise many security issues that are not resolved.
- Mobile IP allows you to maintain the same Internet connection address ("care of"

address) as you move around. There are many security issues and evolving solutions in Mobile IP.
- WAP specification ensures that a secure protocol is available for transactions on a wireless handset. WAP uses the Wireless Transport Layer Security (WTLS) protocol.

9.2 Overview of Wireless Networks and Wireless Security

9.2.1 Wireless Networks at a Glance

Wireless networks, as the name implies, interconnect devices without using wires – instead they use the air as the main transmission medium. Wireless networks are enjoying widespread public approval with a rapidly increasing demand. The increase in the number of cellular phones, palm pilots, PDAs, laptops, notebooks, and other handheld devices is phenomenal. To meet this demand, mobile communications technologies are emerging with digital speech transmission and the ability to integrate cordless systems into other networks. In the meantime, researchers are developing the next generation of technologies for several years to come.

The unique features of wireless networks are:
- The bandwidths, and consequently data rates, of communication channels are restricted by government regulations. The government policies allow only a few frequency ranges for wireless communications.
- The communication channel between senders/receivers is often impaired by noise, interference and weather fluctuations.
- The senders and receivers of information are not physically connected to a network. Thus the location of a sender/receiver is unknown prior to the start of communication and can change during the conversation.

A very large body of work on wireless networks exists, with emphasis on different aspects such as radio transmission technologies, standards, protocols, systems engineering, and carriers. See, for example, the *Mobile Communications* series by Artech Publishing. For our purpose, wireless networks can be broadly classified in terms of wireless local area networks, wide area networks and metropolitan area networks (see Figure 9-1). As we will see in this chapter, each wireless network type introduces its own unique vulnerability.

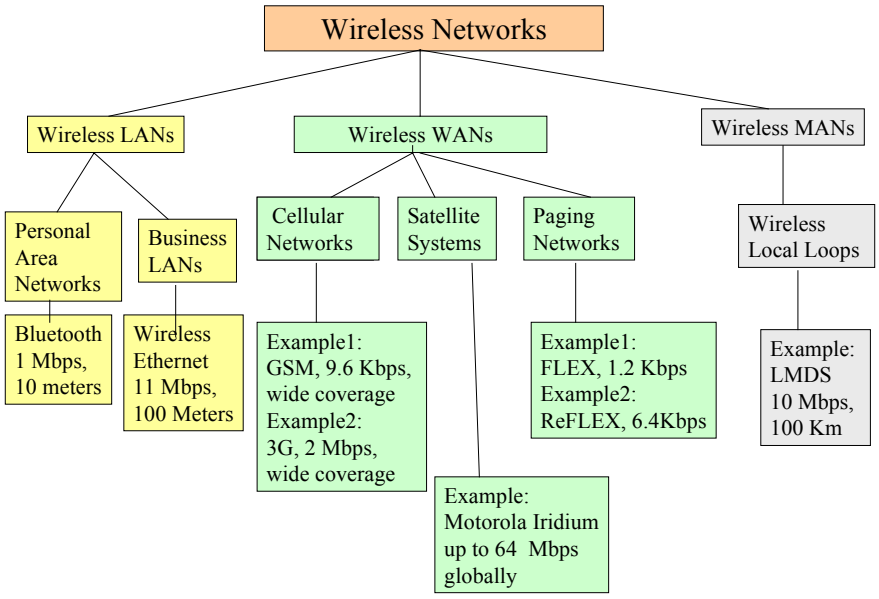


Figure 9-1: A View of Wireless Network Landscape – A Taxonomy

Wireless LANs (WLANs) allow workstations in a small area (typically less than 100 meters) to communicate with each other without using physical cables. Although several attempts to standardize Wireless LANs are underway, the IEEE 802.11 (for 11 Mbps data rate) wireless LANs (also known as Wi-Fi or wireless Ethernet) by far are the most popular. Bluetooth LANs (for data rates in the 700 kbps to 1 Mbps range) and cordless LANs are examples of wireless personal area networks (WPANs). We will discuss 802.11 and WPAN security in Sections 9.3 and 9.4.

Wireless WANs (WWANs) provide wireless support over long distances. Traditional examples of wireless WANs are satellite systems (see Section 9.6). However, a great deal of wireless WAN activity at present revolves around the cellular networks that provide support for cellular phones and handheld devices such as PDAs and laptops. We discuss cellular networks and the future third-generation (3G) wireless WANs in Section 9.5.

Wireless metropolitan area networks (WMANs) have been used in traditional packet radio systems, often in law-enforcement or utility applications. An interesting area of growth for wireless MANs is the wireless local loop (WLL) that is gaining popularity with long distance telephone companies. WLLs are ***fixed wireless networks*** where the devices being connected are stationary (see Section 9.7).

New types of wireless networks are being introduced in the marketplace on an ongoing basis due to the government, academic, and industry activities in this vibrant area. Examples include Free Space Optics (FSO), Ultra Wideband (UWB) wireless, and mobile ad hoc networks (see Section 9.8). These networks offer much higher data rates than the existing wireless systems and also support very flexible wireless configurations.

The wireless networks in the aforementioned categories are offering higher data rates than before. However, the wired networks are also offering higher data services. Table 9-1 summarizes the typical data rates in the wireless versus wired world. As you can see, the wireless technology is much slower than the wired type, but it offers greater

flexibility to the users. On the other hand, it introduces several security risks, as we will see.

Table 9-1: Wireless Versus Wired Networks

	Local Area Networks (LANs)	Metropolitan Area Networks (MANs)	Wide Area Networks (WANs)
Wired	Wired LANs Ethernet (10-100 Mbps, 150 to 500 meters) Token Ring (4 -16 Mbps, 200 to 500 meters)	Wired MANs FDDI (100 Mbps, 50 Kilometers)	Wired WANs Dial up (56 Kbps) DSL/cable modems (200 Kbps - 1 Mbps) ATM (44 Mbps to 140 Mbps) Frame Relay (44 Mbps)
Wireless	Wireless LANs Bluetooth (1 Mbps, 10 meters) IEEE 802.11 LANs (2-11 Mbps, 100 meters)	Wireless MANs wireless local loops (10 Mbps, 100 Kilometers)	Wireless WANs Current GSM systems at 9.6Kbps, future 3G systems at 2 Mbps

9.2.2 A Quick Overview of Wireless Security

Each wireless network type reviewed in the previous section introduces its own unique vulnerability. In addition, higher-level security issues of wireless middleware and wireless applications need to be considered. It is best to think of wireless security at various layers (physical wireless network, TCP/IP, middleware, application) and analyze the security technologies available at these layers (see Figure 9-2). The solution approach at each layer employs various security technologies to support the privacy, integrity, authorization, authentication, accounting, and availability (PIA4) requirements. For example, IPSec, SSL, and SET employ the same type of cryptographic technologies (private-public key encryption, digital certificates, hashes, etc) to support PIA4, albeit at different layers of the system.

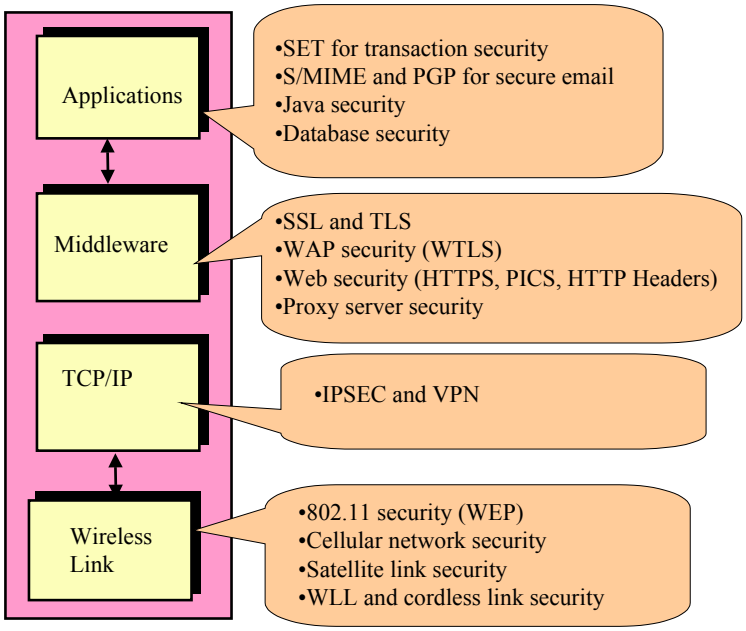


Figure 9-2: Security Technologies at Different Layers – A Starter Checklist

Security is needed at these different levels, since security at each level fulfills different requirements. Let us briefly review the strengths and weaknesses of security at various levels and suggest some guidelines before going into details (see Table 9-2):

1. Wireless link security protects communications at the physical wireless link (layer 1 and 2) levels. This type of security is at the heart of wireless networks (WLANs, WLLs, cellular networks, satellites). This type of security is especially important in wireless because of eavesdropping and other threats we have discussed previously. Although this security does not give complete end-to-end security for a network (all links of a network need to be secure), it attempts to protect at least some segments of wireless links. Some guidelines are:

- Turn on security at wireless links to avoid eavesdropping even if it is deficient. For example, use Wired Equivalent Privacy (WEP) for wireless LANs because it does provide some security; and make up for WEP security deficiencies by providing higher layers of security (e.g., SSL).
- Make sure that all access points are themselves monitored and controlled so that no one sets up rogue access points.
- Treat wireless networks as un-trusted networks. Thus, put the internal WLANs outside the firewall so that they are treated as outsiders. In addition, minimize placing critical applications and databases on wireless networks – move them to wired networks behind firewalls.
- Make sure that the passwords on wireless networks are different than those used on the wired networks. Hackers usually capture passwords from wireless networks and then use them to gain access over wired networks.

2. TCP/IP network security encrypts TCP/IP packets. This can be provided by using VPNs employing IPSec. VPNs for wireless networks provide many benefits because all traffic spanning many links can be secured. Many firewalls and gateways are also erected to regulate the IP traffic and operate at this level. VPNs are commonly used to overcome wireless link security weaknesses. However, there are some drawbacks of VPNs:

- Roaming between VPNs is not completely transparent.
- VPNs have to overcome firewall barriers.
- VPNs do not support multicasting.
- VPNs do introduce excessive overhead. Everything is encrypted, even if you are surfing the web.

3. **Middleware-level security** can secure point-to-point communication between specific clients and servers. For example, SSL (Secure Socket Layer) secures most web clients and servers. Similarly, WTLS secures communications between WAP clients and WAP servers (WAP gateway). This is important especially if lower-level security was not employed or was week due to wireless. Specific issues with middleware-level security are:

- Middleware security only applies to the applications that operate on top of the said middleware. For example, CORBA security can only protect CORBA applications and WAP security can only secure WAP applications.
- Gaps may exist between different types of middleware security. For example, WTLS protects between the WAP device and WAP gateway. A gap exists when the WAP gateway has to translate to the final website using SSL.

4. Application-level security is provided by database managers, Java security, SET (Secure Electronic Transactions), PGP, S-MIME, and several other application-specific security packages. A variety of security approaches exists at the application level, where authorization controls are used within applications to regulate access to specific data, and cryptographic infrastructures are built to strongly authenticate users and provide confidentiality. In particular, applications themselves provide access control and strong user authentication. Specific considerations for this level of security (we will visit these in a later chapter) are:

- Different applications use different security features. You need to turn security for each application to make it secure. For example, SET makes transactions secure while S/MIME and PGP make the email secure.
- Very strong application-level security should be used for applications and databases that are accessed over wireless networks.
- Application-level firewalls that filter application traffic provide a much finer level of security as compared to IP-level firewalls.

Security must be considered at all levels. However, a very high level of security at every level (e.g., encryption at all levels) can add significant overhead. Tradeoffs are essential. But you have to decide what level to emphasize. Securing a higher layer while keeping lower layers unsecured makes the system vulnerable to intrusions from the lower layers. In general, lack of security at a certain layer might compromise the overall system even if other layers are secured. Consider, for instance, a system where the application data is secure, but is transmitted over an insecure network. In this case, the overall security of the application could be suspect. Specifically, application security protects application data (e.g., database security mechanisms allow the data to be stored on the hosts in a

protected manner) and system resources (e.g., Java Security), while SSL, IPSec, and wireless link security protects data while being transferred on the network.

Table 9-2: Security Levels

Security Level	Example of Security	Why Needed?	Why Not Enough?
Application-level security	SET, PGP, S-MIME	Provide security specific to an application	Only protection of application-specific data
Client/Server Security	SSL and WTLS Security	Assures secure communication over an unsecure link	Only middleware-level security
IP Level	IPSec, VPN	Protects the IP path	Does not protect databases.
Network Link Level	Wireless LAN Security, 3G and Satellite Security	Deters breaking in at physical link level	Protects only one link. Does not cover other links in a large network

9.3 Wireless LAN Security

9.3.1 Overview

The wireless LAN industry has grown at a notable rate of between 40% and 60% per year since the mid 1990s and is around $2 billion at the time of this writing. The result is a very widespread use of wireless LANs (WLANs), especially the ones based on the IEEE 802.11 standard. These WLANs, commonly known as Wi-Fi (abbreviation of wireless fidelity) are especially pervasive. Visit any major office building, department store, or hospital, and you will discover 802.11 cards in most PCs and access points hanging from the ceilings. The popularity of Wi-Fi LANs is driven by several factors. First, product prices have decreased dramatically over the past year. Second, new wireless LAN applications are continually being adopted, with more corporate and individual reliance on mobile computing platforms. Finally, a strong grassroots movement is building open and free Wi-Fi hotspots around the globe. These no-fee hotspots are springing up in coffee shops, university campuses, and residential areas and are competing with expensive wireless connections from telecom providers [Schmidt 2003]. For example, in mid-2003, the New York City wireless open network (95 active nodes) was competing with the two main payment-based WLANs operated by T-Mobile USA (120 nodes) and Wayport (3 nodes). See [Schmidt 2003] and the websites www.nodedb.com and www.t-mobile.com for additional information on free WLANs.

The main appeal of wireless LANs is that they allow workstations in a building to communicate with each other without using physical cables. Figure 9-3 shows a simple wireless LAN configuration. Each station in the wireless LAN has a wireless LAN

adapter (in fact a radio transmitter/receiver) that operates in certain frequency ranges. Connectivity to wired networks is provided through an ***"access point,"*** also known as a local bridge. Wireless communication is limited by how far signals carry for given power output. Wireless LANs use cells, called microcells (similar to the cellular telephone system) to extend the range of wireless connectivity. At any point in time, a mobile PC equipped with a wireless LAN adapter is associated with a single access point and its microcell, or area of coverage. Individual microcells overlap to allow continuous communication within wired network. They handle low-power signals and "hand off" users as they roam through a given geographic area. Figure 9-3 illustrates microcells in a wireless LAN environment.

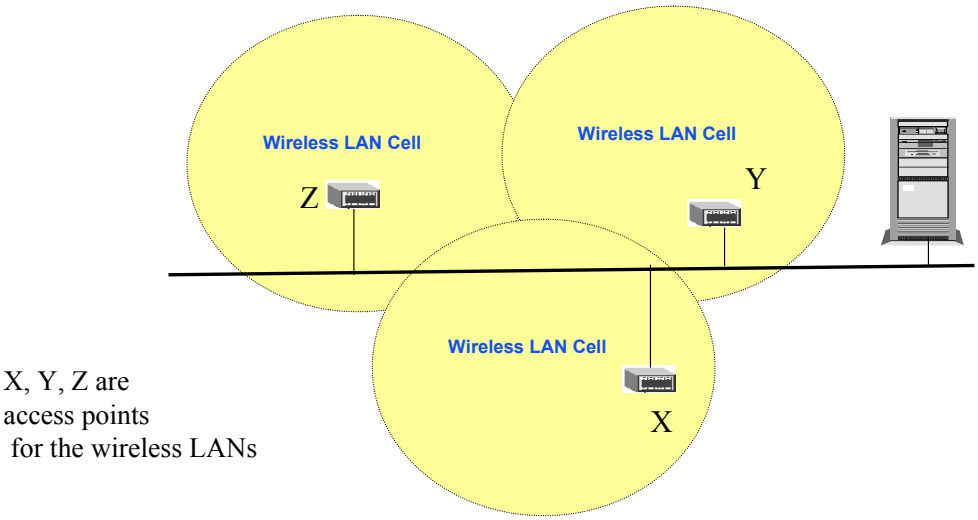


Figure 9-3: A Simple Wireless LAN Environment

9.3.2 The Wireless Ethernet (802.11) LANs

The IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks Standards Working Group in 1990. The standard has been upgraded (802.11b) to support up to 11 Mbps data rates and greater vendor interoperability. Higher data rates are possible with newer standards such as 802.11g. At the time of this writing, base-station transceivers for this LAN are priced around $1000 and transceiver cards for laptops and desktop PCs range between $100 to $200.

The IEEE802.11b LAN operates in a manner very similar to the wired Ethernet LANs. Of course, there are no cables – the data packets are sent over radio waves. The 802.11b LAN uses the 2.2 to 2.4835 GHz band, the so-called unlicensed bandwidth reserved for short-range, low-power devices. (The IEEE 802.11a standard operates in the 5 GHz band and is expected to go up to 54 Mbps). As stated previously, a government license is not required to use the devices or the radio transmitter and to operate other equipment in this frequency range. IEEE802.11b LANs are standardized around the direct sequence spread spectrum (DSSS) radio signals. This scheme divides the frequency spectrum into 14 slightly overlapping channels, each 22 MHz wide. So, if each wireless LAN is configured to use one channel, then an office building or a high school can operate 14

wireless LANs in the same physical space. The transmitters in each channel "spread" their signals on the entire 22 MHz bandwidth to improve reception.

Figure 9-4 shows a sample high school environment that houses several wireless LANs so that the students can access the school server as well as the public Internet.

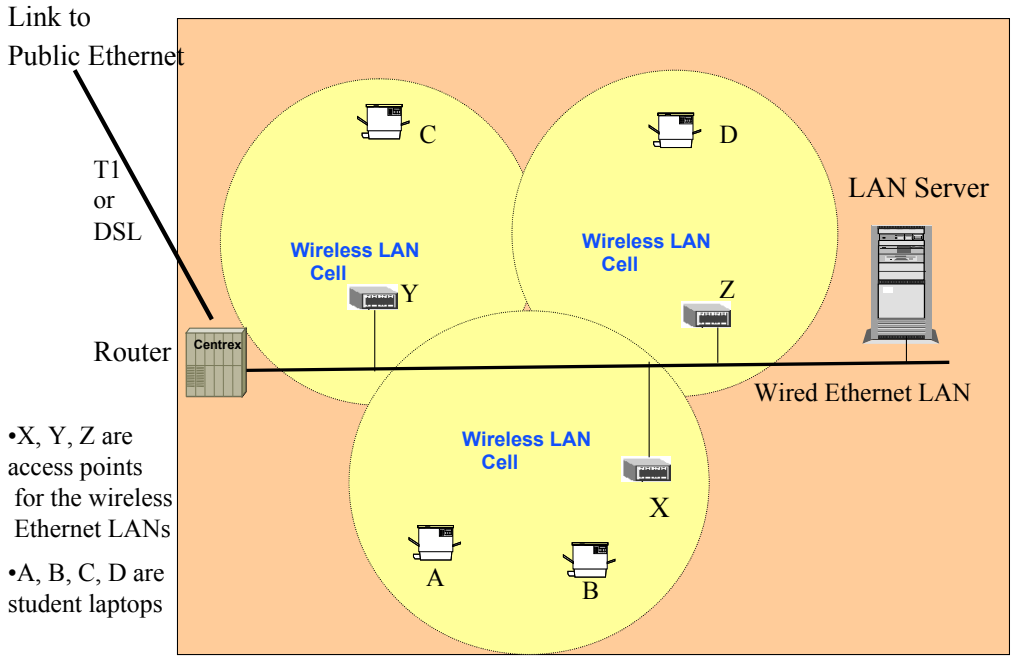


Figure 9-4: A Sample High School with Wireless LANs

9.3.3 Wireless Ethernet (802.11) Security Issues

There are several areas of concern in wireless LAN security. In particular, the current wireless *access points* present a large security problem. Although some organizations believe that the security provided by their deployed wireless access points is sufficient to prevent unauthorized access and use, many researchers have shown otherwise [Cam-Winger 2003, Housley 2003, Arbaugh 2001, LAN97, Walker 1997]. A number of vendors are releasing high-end access points claiming that they address the wireless security problems. Unfortunately, very few products provide enough information to determine the level of protection that the product will provide. In addition, several products use the un-authenticated Diffie-Hellman (DH) algorithm which suffers from a well-known *man-in-the-middle* attack. The problem is that an attacker can insert himself in the middle of the key exchange between the client and the access point – obtaining the session key, K (see the previous chapter for a discussion of the man-in-the-middle problem). Thus the use of un-authenticated Diffie-Hellman introduces a greater vulnerability to the organization's network. Due to these and other wireless security problems, organizations with deployed wireless networks are vulnerable to unauthorized

use of, and access to, their internal infrastructure. The specific areas of vulnerability for 802.11-based wireless LANs are:

- **Random Connectivity.** A user can potentially walk into a building and be connected to the access point by just being in the vicinity. This is unlike wired networks where the computer has to be physically connected to a corporate network.
- **Identity Issues.** Identity is an important part of a security system – without it a malicious outsider can potentially masquerade as a valid user. In WLANs, the MAC address of the WLAN card is used as the only form of identity for both devices and users. Most current open source device drivers allow the users to change the MAC address [Housley 2003]. This creates a security problem.
- **Access Control Issues.** Access control is usually based on ACLs (access control lists) that are based on identity (i.e., the MAC address). Since a MAC address can be changed, a malicious user can access someone else's ACL. Another approach is the "closed network" where a user presents a secret to the access point before gaining access. Unfortunately, the "secret" in WLANs is the access point address, which can be easily sniffed.
- **Authentication Issues.** WLANs use a shared key with a challenge and a response for authentication. Several products use the un-authenticated Diffie-Hellman (DH) algorithm for such an approach, But DH suffers from a well-known *man-in-the-middle* attack as stated previously.

Different approaches to wireless LAN security are reviewed in this section. As we will see, many vulnerabilities in wireless LAN security exist that are being addressed at present, but many problems still exist. Practical approaches to achieve WLAN security are also discussed.

9.3.4 Wired Equivalent Privacy (WEP)

The algorithm, part of the IEEE802.11 standard for wireless LANs, is designed to protect wireless communication from eavesdropping. WEP is also intended to prevent unauthorized access to a wireless network. Although this is not an explicit goal of the 802.11 standard, it is frequently considered to be a feature of WEP.

WEP is a cipher and relies on a secret key that is shared between a mobile station (e.g., a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to protect the wireless LAN from attacks; however, commercial systems do not support such techniques widely.

A number of flaws have been found in the WEP algorithm that could seriously undermine the security claims of the system. In particular, a group of researchers at Berkeley (www.drizzle.com/~aboba/IEEE/wep-draft.zip) found that the following types of attacks against WEP are practical to mount using only inexpensive off-the-shelf equipment:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plain text.

- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

Note that these attacks apply to both 40-bit and the 128-bit versions of WEP equally well. They also apply to networks that use the 802.11b standard (802.11b is an extension of 802.11 to support higher data rates; it leaves the WEP algorithm unchanged). Based on these experiments, it is recommended that anyone using an 802.11 wireless network not rely on WEP for security, and employ higher-level (e.g., application) security measures to protect their wireless network data. See Cam-Wingert [2003], Arbough [2001], and Walker [2000, 2001] for additional discussion of WEP security.

The following two approaches are currently being pursued to overcome WEP problems (see Cam-Wingert [2003] for details):

- **TKIP: Short-Term Solution**. Most existing 802.11 systems implement WEP in hardware. To address the WEP vulnerabilities on the already-deployed 802.11 networks, TKIP (Temporal Key Integrity Protocol) has been developed. TKIP is an interim solution because it does not replace WEP – it adapts WEP protocols to address well-known WEP problems. Users of TKIP go through a firmware/driver upgrade to include the TKIP algorithms.
- **CCMP: Long-Term Solution**. A long-range solution that replaces WEP instead of adapting it is CCMP (Counter-Mode-CBC-MAC Protocol). CCMP uses the Advanced Encryption System (AES) that provides a much stronger encryption and integrity for users. AES uses 128-, 192-, and 256-bit keys and thus is hard to break. The bad news is that AES requires much more processing power – in some cases a separate processor is needed for AES processing.

9.3.5 IEEE 802.1X "Network Port Authentication"

IEEE 802.1X "Network Port Authentication" is an IEEE standard (approved in June 2001) that enables authentication and key management for IEEE 802 Local Area Networks, including Ethernet, Token Ring, FDDI, and 802.11. It basically brings the authentication/key management technologies of dial-up networks to the wired and wireless LANs. The link www.drizzle.com/~aboba/IEEE/802-1x-d11.pdf gives the IEEE 802.1X specification (IEEE Standard, as of June 2001); the Wireless World 2001 and BAWUG Presentations on IEEE 802.1X can be found at www.drizzle.com/~aboba/IEEE/BAWUG.ppt.

IEEE 802.1X is not a cipher, so it is not an alternative to WEP. However, it can be used to derive authentication and encryption keys for use with any cipher, and can also be used to periodically refresh keys. IEEE 802.1X is not a single authentication method; rather it utilizes Extensible Authentication Protocol (EAP) as its authentication framework. EAP is an IETF standard for extensible authentication in network access. It is supported within PPP, IEEE 802.1X, and VPNs (L2TP/IPsec and PIC). The EAP (Proposed Standard, RFC 2284) is discussed in www.ietf.org/internet-drafts/draft-ietf-pppext-rfc2284bis-01.txt Due to EAP support, 802.1X-enabled switches and access points can support a wide variety of authentication methods, including certificate-based authentication, smart cards, token cards, one-time passwords, etc. Switches and access points act as a "pass through" for EAP so new authentication methods can be added

without the need to upgrade the switch or access point, by adding software on the host and back-end authentication server.

IEEE 802.1X was designed to be scaleable – it adds no per-packet overhead because it does not involve encapsulation (unlike PPPOE or VPN). This means that it can be implemented on existing switches and access points with no performance impact. IEEE 802.1X can scale from speeds of 11 Mbps (802.11) to 10+ Gbps, and can be enabled on existing switches with a firmware upgrade, without the need to buy new hardware. IEEE 802.1X also integrates well with AAA (authentication, authorization and accounting) standards such as RADIUS and LDAP. Thus VPNs and RADIUS servers (including Windows 2000 IAS) that support EAP can be used to manage IEEE 802.1X-based network access. Through RADIUS, IEEE 802.1X permits management of authorization on a per-user basis. Information about using RADIUS with IEEE 802.1X can be found at www.ietf.org/internet-drafts/draft-congdon-radius-8021x-17.txt.

9.3.6 802.11 Wireless Roaming

Roaming, an important aspect of wireless networks, is the ability to connect to multiple ISPs while maintaining an account with only one. To keep the same IP address while roaming, there are approaches at layer 2 as well as layer 3. Mobile IP is the layer 3 approach and dynamic VLANs and tunneling are layer 2 approaches (both are enabled by RADIUS tunneling attributes). "Shared use" access points (APs) need to be enabled to support roaming within 802.11. Shared-use APs are important for wireless because they save cost (it costs more to deploy multiple APs in the same location) and also reduce interference (the limited radio channels in 802.11 make radio interference a potential problem). Standards are in progress that describe, for example, how to do seamless, authenticated fast handoff between 802.11 access points. The link (www.ietf.org/rfc/rfc2194.txt) surveys roaming implementations and (www.ietf.org/rfc/rfc2477.txt) discusses roaming architecture and requirements.

9.3.7 Approaches to Secure WLANs

As discussed above, the Wired Equivalent Privacy (WEP) algorithm, part of the IEEE802.11standard for wireless LANs, is designed to protect wireless communication from eavesdropping. However, several weaknesses of WEP have been demonstrated. Several other problems also exist as discussed previously.

Given all these problems with equipment built to 802.11 standards, how to safely use it? Here are some thoughts and suggestions:

- Make sure that WLANs do not bypass the corporate firewalls. It is best to place the WLANs outside instead of inside the corporate firewalls. This way, any WLAN internal or external will have to go through the firewall to access any corporate resources.
- It is best to encrypt the wireless LAN traffic by using solutions such as wireless VPN. In this case, a WLAN traffic is authenticated and encrypted in a fashion similar to the dial-up traffic.
- Heavily protect the resources accessed through wireless LANs. For example, higher-level security offered by SSL, PGP, and SET (discussed later in this chapter) can be used to protect Web resources, email, and financial transactions.

- It should be also recognized that some users do not want a great deal of security because it limits their ability to communicate freely with others. For example, the free and open WLAN communities continue to exchange unencrypted information and send IDs and passwords as clear text despite warnings [Schmidt 2003]. In such cases, the current WLAN security is quite adequate.

9.4 Wireless Personal Area Network Security

9.4.1 Overview

Wireless personal area networks (WPANs) are small networks designed primarily for SOHO (Small Office Home Office) environments. Although 802.11 networks can be used as WPANs, they may be an overkill. Besides 802.11, the main contenders for the WPAN are cordless phones, HomeRF and Bluetooth. In addition, the emerging UWB (Ultra Wide Broadband) networks are a good contender mainly because of their strong security.

WPANs have security issues that are somewhat similar to the wireless LAN issues discussed previously. In terms of PIA4, these are:

- Privacy issues due to possible eavesdropping by randomly connected users
- Integrity issues due to the intervention of randomly connected users and "man in the middle" problems
- Authentication issues due to identity problems
- Authorization issues because unauthorized and unauthenticated users may access the network and possibly modify network resources (e.g., APs)
- Accountability issues because a mobile user may say that he/she never established connection with an AP
- Availability issues due to possible jamming and denial-of-service attacks

9.4.2 Cordless Phone and Home RF Security

Cordless phones are a special class of cellular networks in which the cell sizes are very small (less than 100 meters, typically) and there is no need for location and roaming support. Many households have cordless phones for convenience. DECT (Digital Enhanced Cordless Telecommunications), developed in Europe, is the most commonly used standard and provides for cordless security. DECT architecture, shown in Figure 9-5, consists of several layers based on the ISO-OSI model. The security is handled at a higher level. In particular, mobility management is responsible for security of DECT communications. It is organized into the following groups of services:

- Identity procedures that are used for the mobile unit to identify itself to the base station
- Authentication procedure that establishes that the mobile unit is a valid network user
- Location procedure that is used in systems with multiple base stations to track location of mobile unit
- Access rights procedure that establishes that the mobile unit has the right to gain access to a specific type of local or global network

- Key allocation procedure that distributes encryption keys for protecting network control information and user information
- Parameter retrieval procedure that is used to exchange information about the parameters of the mobile unit and network operation
- Ciphering-related procedure for encryption and decryption operations

In general, the DECT security is based on the GSM cellular phone security. It added features such as an enhanced key management support and the possibility of the mobile terminal to authenticate the network. A related standard, from a DECT security point of view, is the Terrestrial Trunked Radio (TETRA) standard that has been built on DECT security. TETRA added features which are relevant for Professional Mobile Radio users, such as end-to-end encryption, encryption for closed user groups and secure enabling and disabling of mobile terminals. A full description of the DECT security model can be found in the formal ETSI standards via http://www.etsi.org.

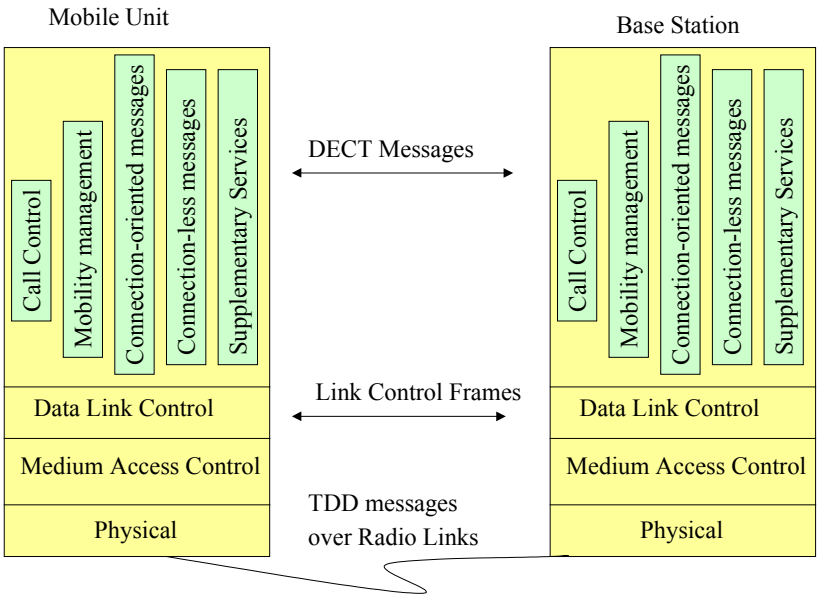


Figure 9-5: DECT Architecture

HomeRF goes beyond cordless phones and defines a set of networking options for SOHO wireless networks. HomeRF includes DECT and has the following security features that protect against the following possible attacks:

- For privacy, it includes support for 128-bit encryption so all the data traveling across the radio waves is encrypted. When exporting HomeRF to countries of concern to the NSA (National Security Administration), the encryption algorithm is flexible enough to revert back to lower sizes (56 or 40 bits). In addition, HomeRF uses frequency hopping that keeps the "data channel" shifting from one frequency to another many times a second. This makes it very difficult for someone to eavesdrop on your home network.
- For integrity, HomeRF uses hashing and error detection/correction to assure that the messages did not change in transit.

- For authentication, it uses a "network password" without which the peripherals cannot communicate with a home network. HomeRF uses a 24-bit network IP that is specific to each personal area network. This network IP prevents devices outside of a user's personal area network intercepting and using information sent from a remote personal area network. Taking an apartment block as an example, HomeRF devices from one system could potentially interfere with another apartment's HomeRF system.
- For authorization, HomeRF uses the DECT access rights procedure to assure that the mobile unit has the right to gain access to a specific type of local or global network.
- For accountability, HomeRF does not directly provide any support.
- For availability, HomeRF applications can be replicated.

9.4.3 Bluetooth Security

Bluetooth is a medium-speed wireless LAN (1 Mbps, 10 meter) specification introduced by Ericsson, IBM, Intel, Nokia, and Toshiba in May 1998. The main idea is to develop a way for users to connect a wide range of mobile devices quickly and easily, without cables. To ensure that this technology is seamlessly implemented in a diverse range of devices, a special interest group, formally announced on May 20, 1998, was formed to design a royalty-free, open specification technology, code named "Bluetooth." The SIG has quickly gained membership from companies such as 3COM/Palm, Axis Communication, Compaq, Dell, Lucent Technologies UK Limited, Motorola, Qualcomm, and Xircom, and is encouraging the involvement of all other companies. Currently, almost 2000 companies are part of the Bluetooth SIG. According to a Dataquest forecast, 79% of digital handsets and more than 200 million PCs will use Bluetooth in the early 2000s.

Bluetooth technology is basically a wireless personal area networking (WPAN) technology that has gained significant industry support (some of it is suffering because of the popularity of Wi-Fi). Bluetooth coexists with most wireless LAN solutions. The Bluetooth specification of 1 Mbps is intended as a small form-factor (i.e., few participants), low-cost radio solution that can provide links between highly mobile devices such as mobile phones, mobile computers and other portable handheld devices. This technology, embedded in a wide range of devices to enable simple, *spontaneous* wireless connectivity is a complement to wireless LANs which are designed to provide *continuous* connectivity via standard wired LAN features and functionality.

Figure 9-6 shows a simple Bluetooth configuration. Bluetooth was designed to allow low-bandwidth wireless connections to become so simple to use that they seamlessly mesh into your daily life. The idea originated from connecting different devices (e.g., mouse, printer, headset, cellular phone) to a laptop in a small personal area network, called Piconet (see Figure 9-6). The Piconet could, however, be connected to a wired LAN (through an access point), or to a cellular network through a cellular phone (see Figure 9-6). A simple example of a Bluetooth application is updating your cellular phone directory. The main idea is that this could happen automatically as soon as the phone is within the range (10 meters) of your desktop computer where your directory resides.

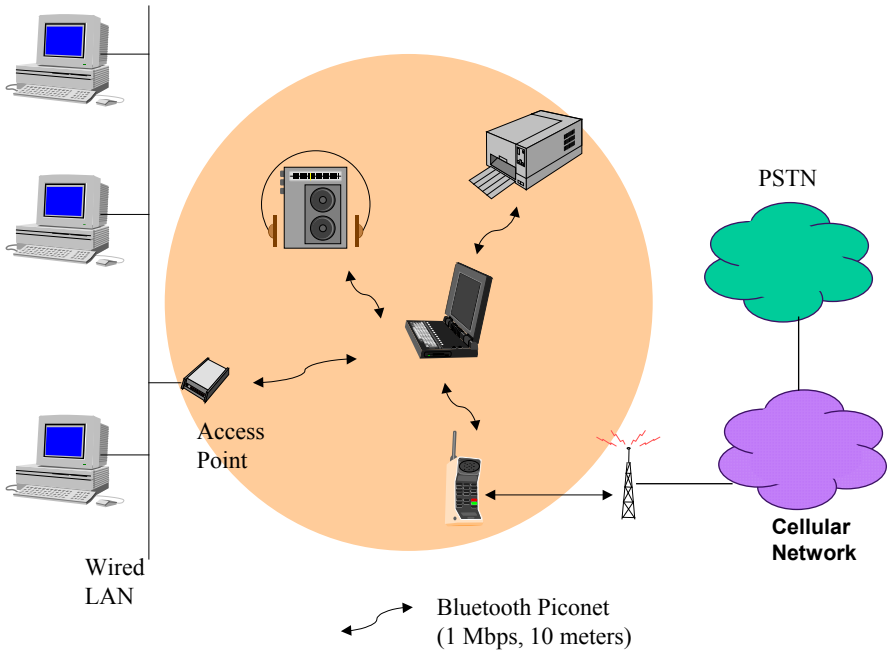


Figure 9-6: A Simple Bluetooth Configuraation

Bluetooth, like other wireless networks, raises some security concerns and addresses few of the related concerns. Some security checks, such as encryption and authorization, can be done at the application level. But since wireless technology lends itself to eavesdropping, it is crucial to understand the application-level security needs. In addition, an authentication protocol is necessary to ensure that the communicating devices are on a Bluetooth network. Spoofing and similar problems that exist on IP networks today are much worse with Bluetooth because it doesn't require any physical connection to the network. Security is an important feature of Bluetooth. The radio transceiver is designed to communicate properly even in noisy frequency locations while at the same time maintaining data integrity through error-correction methods, encryption, and authentication to protect any data transmission in any type of climate.

9.5 Cellular Wireless Network Security

9.5.1 Overview

Cellular networks are wireless WANs that establish a connection between cellular users. Figure 9-7 shows a high-level view of a cellular communication network used in wide areas. The cellular network is comprised of many ***"cells"*** that typically cover 1 to 25 miles in area. The users communicate within a cell through wireless communications. A ***Base Transceiver Station (BTS***) is used by the mobile units in each cell by using wireless communications. One BTS is assigned to each cell. Regular cable communication channels can be used to connect the BTSs to ***the Mobile Telephone Switching Center (MTSC)***. The MTSC is the heart of cellular networks – it determines the destination of the call received from a BTS and routes it to a proper destination either

by sending it to another BTS or to a regular telephone network. Keep in mind that the communication is wireless within a cell only. The bulk of cell-to-cell communication is carried through regular telephone lines The MTSC uses two databases, called ***Home Location Register (HLR)*** and ***Visitor location Register (VLR),*** to locate the mobile users.

The following security concerns are unique to the cellular networks:

- The call setup information that includes the user ID and other information should be protected.
- The speech and data transmitted during a cellular conversation should be kept private and confidential.
- Privacy of user location. The location (cell ID) from where the user is calling should be private; also the VLR/HLR records that trace where the user has been visiting should be kept private.
- The calling patterns (e.g., calling home everyday at 5 P.M. to inform your family about when you will be home) should be private.
- The user-ID in the cellular networks should be kept private.

.

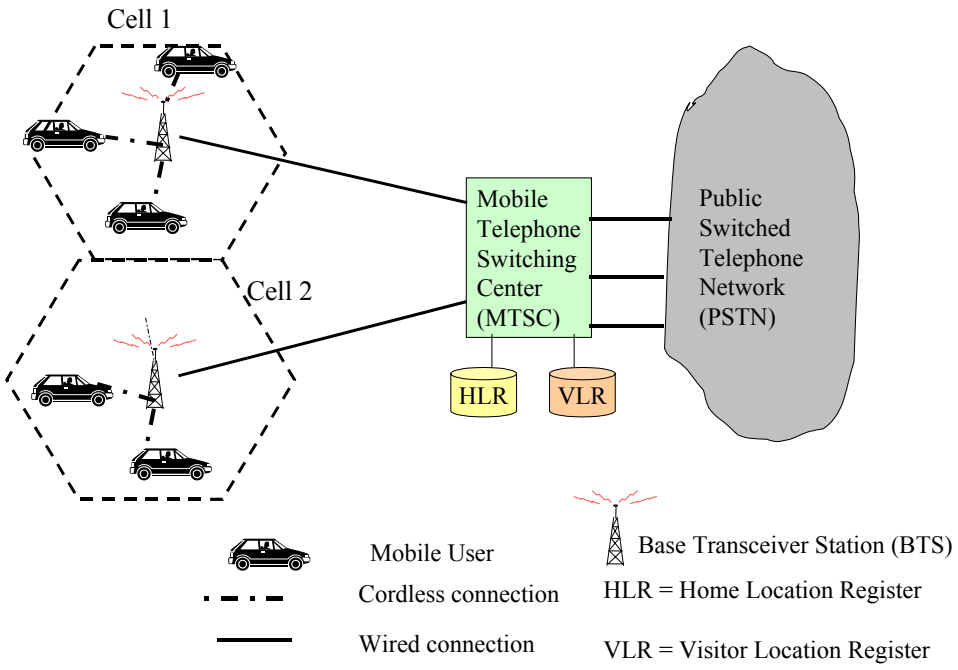


Figure 9-7: A Cellular Communication Network

9.5.2 Cellular Network Security Solution Approaches

The security approaches of cellular networks can be discussed in terms of the various generations of cellular networks:

1G: First-generation wireless cellular: These systems, introduced in the early 1980s, use analog transmission, and are primarily intended for speech. These networks are very slow (less than 1 kilobits per second). The security for these networks was virtually non-

existent. Several hackers were able to capture large amounts of cellular data by just driving around in the neighborhood with a car antenna.

2G: Second-generation wireless cellular: Introduced in late 1980s, these systems use digital transmission and are also intended primarily for speech. However, they do support low bit-rate data transmissions. The high-tier 2G systems use GSM and the low-tier type is intended for low-cost, low-power, low-mobility PCS. These systems, most prevalent at present, operate at 9.6 kbps. GSM systems have improved the security by introducing three elements: a SIM (subscriber information module) that contains a unique user ID that can be used for authentication, the GSM handset that includes an encryption algorithm, and the GSM network itself that supports encryption. GSM security is described extensively in the GSM recommendations.

2.5G Systems are essentially 2G systems that have evolved to medium-rate (around 100kbps) data. As part of 2.5G initiative, GSM is being extended by the ***General Packet Radio System (GPRS)*** to support data rates of 112 kilobits per second. Generally, 2.5G technologies have been developed for third-generation (3G) networks, but they are applied incrementally to existing networks. This approach allows carriers to offer new high-speed data and increased voice capacity at much lower cost than deploying all new 3G networks. Plus, they can do so using their existing spectrum. GPRS uses encryption in its core network to avoid eavesdropping. In addition, since GPRS uses packet switching services, the IPSec services described previously can be used in GPRS. IPSec, as you recall, encrypts the packets before transmission.

3G Systems represent the future broadband multimedia applications and can operate at 2 million bits per second. 3G systems are evolved from 2G – building on the success of GSM – and dual-mode terminals to ease migration from 2G to 3G are commercially available. 3G system specifications include extensive security features in user equipment and the underlying network.

In essence, the security of cellular networks is improving as the next generation of cellular networks is being introduced.

9.6 Satellite Security

9.6.1 Overview

There are several issues that keep satellites from becoming the ultimate wireless WAN. The most important is the turnaround propagation delay (can be about a second) that affects performance of many applications. Also, security questions abound. Satellite security is a major issue in commercial as well as government settings. In particular, security is an important issue in IP over satellite, since an attacker can easily intercept such communication and can even corrupt the transmitted data [Noubir 1998]. Consequently, commercial satellite services have largely been excluded from national initiatives to tighten up the US communications infrastructure (see Wrexler [2002]).

The problem is particularly severe for government agencies. For example, the US General Accounting Office (GAO) released a report warning that the nation's

commercial satellites have been largely ignored in discussions of critical infrastructure protection and are vulnerable to attack from hackers [Roberts 2002]. The report, posted on the GAO's website, found critical vulnerabilities in the nation's commercial satellite network. It further suggests that federal agencies using commercial satellites may be exposing sensitive data to unauthorized snooping. Although the government uses encryption to protect satellite communications and employs physical security to protect ground stations, many federal agencies rely on commercial satellite service providers to provide security for tracking, satellites and satellite control stations.

The commercial satellite providers fall short of the security standards the government uses to protect its own satellite networks. In addition, government agencies cannot impose specific security requirements on commercial satellite service providers, because existing federal laws governing satellite system security apply only to satellites used for national security. According to current policy, federal agencies only have power to secure those satellites that they own. At the same time, the dependence of the federal government on commercial satellites is increasing. Traffic from federal agencies makes up 10% of all traffic handled by commercial satellites. In addition, up to 45% of all federal government traffic between the Persian Gulf region and the US is carried over commercial satellite networks. The GAO report recommends expanding the current federal policy governing satellite security to cover commercial satellites used by government agencies.

Besides the government issues, the privacy of sensitive commercial information that traverses satellites is a concern. For example, point-of-sale transactions and credit card authorizations, Internet traffic, telemedicine information, backhaul mobile traffic, and location-tracking information is carried over satellites. Satellites also transmit global positioning information to aircraft and air traffic controllers. The Federal Aviation Administration (FAA) also plans to use satellite systems to broadcast live cockpit communications from domestic airliners for national security purposes (see the sidebar, “Use of Aircraft Satellite Security Systems”). Security of satellites communications is naturally important.

FAA Use of Aircraft Satellite Security Systems

The Federal Aviation Administration (FAA) plans to use satellite systems to broadcast live cockpit communications from domestic airliners for security purposes. Qualcomm demonstrated a system that uses a global satellite constellation to beam real-time cockpit conversations and potentially live video streams from commercial aircraft to controllers on the ground. This is intended to provide controllers real-time information to help avert a potential hijacking. The task is, however, complex because the satellite equipment would have to be “type certified" for each kind of aircraft, ranging from small commuter planes to jumbo jets. The FAA will also have to rigorously test the new systems to ensure that they do not interfere with the operations of key systems, such as airborne navigation systems. In addition, management of live voice and video data streams from large numbers of aircraft would be equally difficult because there are between 35,000 to 40,000 flights a day in the US.

Besides cockpit information, other efforts for using satellites for commercial flights are underway. Boeing, for example, is planning broadband Internet service for passengers.

The offering, Connexion by Boeing, could be adapted to broadcast real-time images from aircraft cabins and the cockpit to enhance security.

Source: Brewin [2001].

9.6.2 Approaches to Secure Satellite Communications

Satellite communications are typically secured through scrambling of satellite signals by using cryptography or spread spectrum techniques. Spread spectrum, as discussed in a previous chapter, is most widely used in wireless LANs but was developed for military and intelligence operations. The message is "spread" over a range of frequencies to make it jam-resistant – it basically transmits different data bits on different signals, based on a secret scheme, for secure communications. The receiver must know the parameters of the spread-spectrum signal being broadcast to understand the signal. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise.

For additional security, the messages can be encrypted before transmission and decrypted on reception – a technique used in VPNs (Virtual Private Networks). VPNs, as stated previously, set up a private network over a public network by using encryption. VPNs use IETF IPSec (RFC 2401) and related standards to transport encrypted messages over shared networks. IPSec provides security at the packet level, instead of security at the application layer. It encrypts and signs Headers and/or Data parts of an IP Header. In addition to spread spectrum and encryption, the security can be also improved by using attack-resistant satellite components and employing better physical security on ground stations.

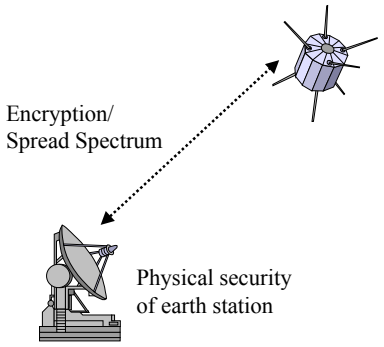


Figure 9-8: Satellite Security Approaches

The main challenge in achieving satellite security is to strike a balance between performance and security [Wexler 2003]. For example, satellite VPNs (Virtual Private Networks) that encrypt messages by using IPSec are good solution candidates. This would allow secure IP VPN services for satellite users and support highly distributed sites. However, TCP was developed for low-delay lines and is very slow when the IP packets are transmitted over satellite because of the high round-trip time of satellite links. To overcome this limitation, several modifications to TCP and other IP protocols have been suggested. For example, some very small aperture terminal (VSAT) and satellite

modem vendors have enhanced their implementations of TCP and HTTP to accelerate throughput. But many IP VPN security solutions do not interoperate with these protocol modifications. Thus, the users have to choose between performance and security.

Some companies, such as Encore Networks, have built satellite VPN appliances that interface to the various enhanced versions of TCP and HTTP. Development of IPSec that does not interfere with TCP is an interesting area of research. For example, a set of rules for optimizing TCP without interfering with IPsec have been proposed [Naubir 1999]. Secure IP over satellite VPNs can be of benefit to many users. For example, a broadband satellite VPN with accompanying service-level agreements (SLA) would be very beneficial for businesses with widely distributed offices.

9.7 Wireless Local Loop (WLL) Security

WLLs are examples of wireless metropolitan area networks and offer broadband wireless data rates between 10 to 50 Mbps. WLLs are ***fixed wireless networks*** where the devices being connected are stationary. Thus there is no need for location services and security does not involve mobility support. Figure 9-9 shows a possible configuration for WLL. A base station antenna, mounted on top of a tall building, serves each WLL cell that consists of residential and business subscribers. A WLL provider can serve one or many WLL cells from its switching center.

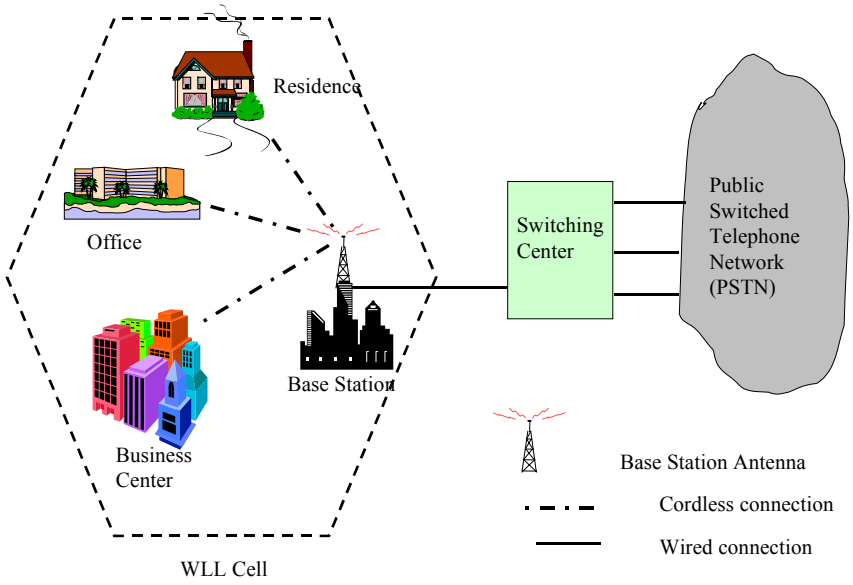
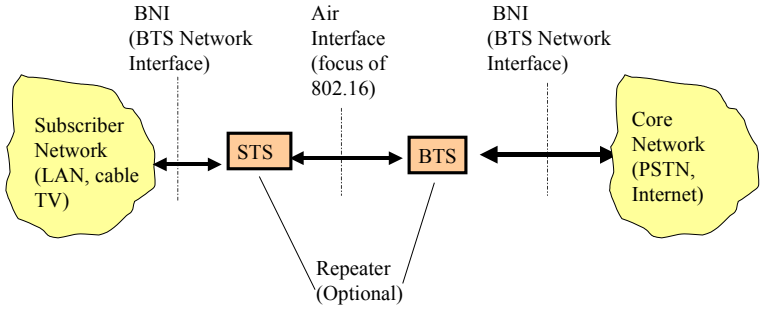


Figure 9-9: WLL Configuration

Several wireless local loops are in operation at present. The best known examples are MMDS and LMDS. Multichannel multipoint distribution service (MMDS) is an older service that operates in the 2.15 GHZ to 2.68 GHZ frequency ranges and can offer 27 Mbps over 50 km. Local multipoint distribution service (LMDS) is a newer service for

30 GHZ (US) and 40 GHZ (Europe) frequency ranges and can deliver up to 37 Mbps within 2 to 4 km distances. The security of WLL is at lower layers (layer 1 to 3) and is addressed by the IEEE 802.16 standard. Figure 9-10 shows the abstract reference model that is at the foundation of IEEE 802.16 specification.



Subscriber Network = (LAN, PBX, IP-based network)
Core Network = PSTN. Internet
BTS = Base transceiver station
STS = Subscriber transceiver station

Figure 9-10: IEEE 806.16 Reference Architecture

The 802.16 security is specified through a security manager (SM) that protects against unauthorized access to data transport services by enforcing encryption of the associated service flows across the network. SM employs an authenticated client/server key management protocol in which the SM, the server, controls distribution of keying material to client devices. Security is based on two component protocols:

- An encapsulation protocol for encrypting packet data across the fixed broadband wireless access network. This protocol defines a) a set of supported cryptographic suites, i.e., pairings of data encryption and authentication algorithms, and b) the rules for applying those algorithms to a MAC PDU payload. Encryption services are defined as a set of capabilities within the MAC security sublayer. Encryption is always applied to the MAC PDU payload; the Generic MAC Header is not encrypted.
- A key management protocol (Privacy Key Management, or "PKM") providing the secure distribution of keying data from SM to devices. Through this key management protocol, devices and SM synchronize keying data. In addition, the SM uses the protocol to enforce conditional access to network services. A DEV uses the Privacy Key Management protocol to obtain authorization and traffic keying material from the SM, and to support key refresh.

It should be borne in mind that this security is only intended for lower layers (layer 1 to 3) because 802.16 concentrates on lower layers. Intricate details of 802.16 security can be found in the specification on the IEEE 802 website (http://standards.ieee.org/getieee802/).

9.8 Emerging Wireless Network Security

9.8.1 Overview

We have discussed different wireless networks in the past few sections. A great deal of research is currently being conducted on different aspects of broadband mobile networking. Work is being done to optimize physical-layer technologies of existing wireless networks, as well as to develop and enhance higher-level protocols and applications that facilitate user mobility between different wireless technologies. Research is also proceeding to develop new alternatives in wireless personal area networks, wireless LANs, wireless local loops and wireless WANs. It is beyond the scope of this book to discuss these developments[2]; we only discuss the following few because of their possible impact on wireless security:

- Ultra Wideband (UWB) – a promising new technology in the areas of wireless local area networks and wireless personal area networks.
- Free-Space Optics (FSO) – a line-of-sight technology that uses lasers for wireless optical communication in a wireless local loop environment.
- Mobile ad hoc network (MANET) - a set of wireless mobile nodes forming a dynamic autonomous network without an access point.

Another interesting development is the powerline communication (PLC) networks – the LANs that use existing powerlines to carry data. Although not strictly wireless, PLCs can be discussed under wireless networks because you do not need *additional* wires for communications.

Due to these and other developments, it is likely that the next generation of broadband mobile applications will need to support multiple physical wireless network technologies. One of the most complicated aspects of this process is to incorporate the security approaches used in different types of emerging and existing wireless networks.

9.8.2 Free Space Optics (FSO) Security

Free-Space Optics (FSO) uses high-intensity optical waves (lasers) to transmit information. FSO has emerged as a solution option in the deployment of next-generation wireless networks because of its high availability, bandwidth scalability, and deployment simplicity. As a result of its worldwide license-free operation, combined with a multitude of applications, FSO is providing an attractive and cost-effective option for high speed connectivity between LANs in metropolitan settings.

The main advantage of FSO transmission is that it is among the most secure connectivity solutions. It is virtually impossible to intercept FSO networks at the physical layer. Eavesdropping and physical intercept are extraordinarily difficult and the chance of an attempted intercept being discovered is very high. For these reasons, organizations with serious security requirements (e.g., government and military) adopt free space laser

[2] See Umar, A., "Mobile Computing and Wireless Communications: Applications, Networks, Platforms, and Security," NGE Solutions, June 2004 (target). See www.amjadumar.com for additional information.

communication systems for voice, video and broadband data communications. Specifically, there are a number of factors that make intercepting FSO links virtually impossible:

- **Detection Considerations**. FSO laser beams cannot be detected with spectrum analyzers or RF meters. Thus the typical wireless detection and interception systems do not work.
- **Physical Considerations.** FSO laser transmissions travel along a line-of-sight path that cannot be intercepted easily. An adversary needs to intercept a portion of the transmitted beam to intercept an FSO link, without exposing himself and his equipment. This is not easy because the optical intercept equipment must be carefully placed in the very narrow beam and pointed at the originating transceiver. Because the FSO transceivers are typically installed high above street level, such efforts are quite difficult and the chance of discovery are very high.
- **Signal Considerations.** It is difficult to intercept the laser beam without altering the signal reception. Although it is possible to intercept the beam without bringing down the link, any attempt could be detected as an anomalous power loss at the receiver, which could be used to send an alarm to appropriate network management software.
- **Overshoot Considerations**. An interception could theoretically occur by placing an adversary receiver directly behind the FSO receiver to intercept the energy that overshoots. This intrusion is easily foiled by placing the FSO equipment indoors, behind a window, or by placing a wall behind the FSO receiver.
- **Encryption Considerations.** Even if a determined intruder overcomes the aforementioned challenges, you can still encrypt the FSO messages.

While there is no wireless communication system that can guarantee transmission security, FSO offers an excellent wireless transmission solution for the highest possible level of physical-layer security.

9.8.3 UWB Security

Ultra Wideband (UWB) is a promising new technology for wireless local area networks and wireless personal area networks. As shown in Table 9-3, UWB provides high data rates (around 50 Mbps) in very short distances (10 meters). Simply stated, UWB is a radio or wireless system that uses narrow pulses (on the order of 1 to 10 nanoseconds) for communication and sensing (short-range radar). Although UWB faces stiff competition from existing technologies, it has an established and proven track record in military applications (it was originally developed in the 1960s for the military and classified for many years). In addition, UWB has several attractive characteristics such as very low power consumption, very high throughput, and no need for a spectrum licensing requirement. After years of classified work, the Federal Communications Commission (FCC) recognized the significance of UWB in 1998 by creating a committee to conduct regulatory reviews of the technology. According to the FCC, UWB communications devices are restricted to intentional operation only between 3.1 and 10.6 GHz (other applications such as law enforcement, fire and rescue are restricted to operate between 1.99 and 10.6 GHz). Initial communications applications are further restricted to operations indoors, or to lower out-of-band emissions with outdoor hand-held use. These restrictions limit the spectrum and power use by UWB Devices.

Table 9-3: Main characteristics of UWB

Factor	UWB (projected)
Coverage	10 m
Frequency Band	3.1 – 10.6 GHz
Usable Frequency	7.5 GHz
Data Rate	50 Mbps

Long used by the US military, in February 2002 the FCC approved the commercial implementation of UWB, within limits. UWB's high data rate and increased security provide a number of niche opportunities for operators and vendors. UWB can be sold to organizations that demand military-grade security. UWB is also being targeted for Wireless HDTV.

UWB is inherently a secure technology with multiple layers of security. The first layer of UWB lies on the noise level, hence an attempting eavesdropper will not be able to decipher between noise and data unless they have access to proprietary coding schemes, algorithms, and modulation techniques. The next is the handshaking protocol invoked at the MAC level that only allows authorized parties to shake hands. Finally there are several encryption techniques that can be used for added security. The military has used UWB technology for communications for the past 20 years because of its security features.

9.8.4 Mobile Ad Hoc Network Security

Mobile ad hoc networks (MANETs) provide a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed wireless infrastructure such as access points – ad hoc networking is basically communication between stations without an access point. Instead, hosts rely on each other to keep the network connected. Thus your mobile host can communicate with other mobile hosts just by being in their vicinity. This ad hoc formation of networks without a pre-existing wireless infrastructure is highly desirable in military situations (e.g., a battlefield) or emergency situations (e.g., a building that has been just demolished). However, the principle challenge in design of these networks is their vulnerability to security attacks. The main problem is that two mobile devices in a MANET can start communicating by just being in the vicinity of each other. In particular, MANETS present the following security challenges [Zhou 1999, Ramanathan 2002]:

- **Availability Concerns.** A denial-of-service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.
- **Privacy Concerns.** Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be

valuable for enemies to identify and to locate their targets (other participating nodes) in a battlefield.

- **Integrity Concerns.** A message could be corrupted because of failures, such as radio propagation impairment, or because of malicious attacks on the network.
- **Authentication Concerns**. Due to lack of central control, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.
- **Non-repudiation (NR) Concerns.** It is difficult to define and enforce NR in MANET because the partnering hosts can change positions and roles in a dynamic manner.

Due to these challenges, MANETs are subject to attacks that can lead to impersonations, unauthorized access to secret information, deletion/modification of messages, and injection of erroneous messages. In addition, nodes roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection can be easily compromised and made to launch internal attacks. It is not advisable to have a central security authority in a MANET because if this centralized entity is compromised, then the entire network is compromised. Trust relationships among nodes are also difficult to maintain because the topology and membership of MANETs change frequently. For example, nodes frequently join and leave the network, so it is difficult to keep track of nodes that have been compromised.

MANET security is an active area of research [Castro 1999, Desmedt 1997, Sun 2001, Haas 1999, Ramanathan 2002]. Approaches to secure MANETs rely on traditional security mechanisms such as authentication protocols, digital signatures, and encryption to achieve privacy, integrity, authentication, and non-repudiation of communication. Additional measures are, however, needed. Examples of these measures [Zhou 1999, Haas 1999, Ramanathan 2002, Sun 2001] include:

- Redundancies in the network topology (i.e., multiple routes between nodes) can be exploited to achieve availability.
- Trust needs to be distributed so that no single node is trustworthy – the trust can be distributed to an aggregation of nodes. We can require consensus of at least n + 1, assuming that any n +1 nodes will unlikely be all compromised.
- Nodes can protect routing information through the use of cryptographic schemes such as digital signatures. Routing information needs to be protected because adversaries can inject erroneous routing information or distorting routing information to starve some nodes from getting any information.
- To defend against compromised nodes, redundant routing information is transmitted in the network. Thus, as long as some routing information is correct, it is used to find alternate routes and make the compromised nodes ineffective. This assumes that there are many correct nodes; thus the routing protocol could find routes that go around the compromised nodes.
- Certificate authorities (CAs) are protected rigorously because MANETs rely heavily on encryption for protecting data plus routing information. CAs are important because they are the trusted parties that keep the public/private key pairs for public key encryption – a commonly used encryption approach for MANETs. To avoid compromise of a central CA, the CA functionality is distributed to multiple nodes.

Special measures are needed to handle other special security and availability threats. For example, “black hole attack” can be launched inside a MANET by a malicious node that

advertises itself as always having the shortest path but then swallows the messages so that they are not sent anywhere. To overcome this threat, other nodes can hold "grudges" by spying on suspicious nodes and keeping track of whether they route packets that they receive [Buuchegger 2002].

The main complicating problem in MANET security is that very sophisticated security procedures cannot be employed because the mobile devices have low processing power and low battery lives. Thus only very few of the available approaches are or can be actually implemented.

Ad Hoc Networking with 802.11

Ad hoc networking is supported by 802.11. Recent IETF work in progress enables hosts to automatically assign IPv4 addresses without a DHCP server, and resolve names without a DNS server (IPv4 or IPv6). The stations can be linked into a coherent network by either acting as bridges (layer 2 approach) or routers (layer 3 approach). A problem with bridging is that convergence times are large. For example, a 802.11D spanning tree does not converge very quickly to be viable in an ad hoc network where hosts are constantly moving, associating and disassociating with each other. IEEE work on "rapid spanning tree convergence" is intended to address this problem. This could enable ad hoc networks with dozens or even hundreds of users that could stretch over a substantial geographic distance. The link (www.drizzle.com/~aboba/IEEE/802-1w-d10.pdf) describes rapid spanning tree convergence for adhoc networks.

9.9 Mobile IP Security

So far, we have discussed physical wireless networks that mainly operate at lower layers (1-3) of the systems. Let us now discuss higher-level issues that are concerned with running IP (Internet Protocol) over the physical wireless networks. Although standard IP is used over most wireless networks, mobile IP is a more interesting case.

Mobile IP was developed so that mobile devices (PDAs, portable computers) could maintain Internet connectivity while moving from one Internet attachment point to another. Consider, for example, that you are in your office with your laptop that is connected to the Internet. Assume that you issued a database query but then detached your laptop, went to a meeting room, and reconnected your laptop in the meeting room. In this case, Mobile IP will allow the system to recognize that you have moved and send the results from your query to your new location (the meeting room). The main idea of Mobile IP is that the same Internet connection address is maintained as you move your mobile device from one location to another. As we will see, the traffic is forwarded by using a "care of" address.

Let us see how the IP addressing will work in a mobile IP environment by using Figure 9-11. Let us assume that a mobile computer C1 is assigned to a particular network, called the ***home network*** for C1. The IP address for the home network is static and is called the

home address. Now, let us assume that the mobile computer has moved to another network, known as a ***foreign network***.. To be operational, C1 first registers with a network node on the foreign network. This node is called a ***foreign agent.*** The foreign agent takes responsibility for C1 and gives its address as a ***"care-of address"*** to an agent on the home network, called the ***home agent.*** As illustrated in Figure 9-11, the home agent gets all the incoming traffic for C1 (step 1), the traffic is routed it to the "care-of" address – the foreign agent (step 2), the foreign agent routes the traffic to C1 in the foreign network (step 3), and the return traffic is routed back to the IP server without having to go through the home agent (steps 4 and 5).

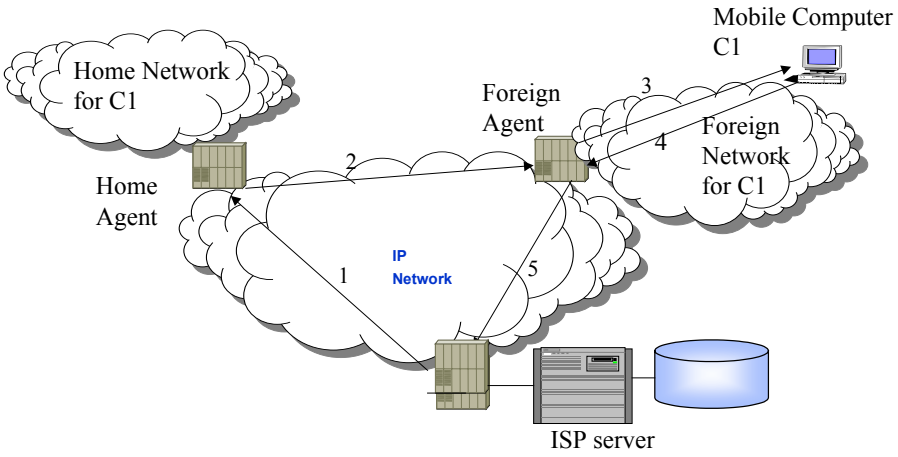


Figure 9-11: A Mobile IP Scenario

Mobile IP includes three basic capabilities to support the operations shown in Figure 9-11.

- Discovery: A mobile node uses a discovery procedure to identify prospective home and foreign agents.
- Registration: A mobile node uses an authenticated registration procedure to inform the home agent of its care-of address.
- Tunneling: Tunneling is used to forward IP datagrams from a home address to a care-of address.

Mobile IP raises several security issues in terms of PIA4:

- A malicious node may pretend to be a foreign agent and may send a registration request to a home agent. This will divert the traffic intended for the mobile node to itself, violating privacy and integrity requirements.
- A malicious node may capture and later replay an earlier registration process and thus cut off the mobile node from any traffic. This raises availability concerns.
- A foreign agent may be overtaken by a malicious user and all messages may be reviewed and/or modified before being forwarded to the mobile node. This, understandably, raises many issues. The home agent may also be compromised with similar results.

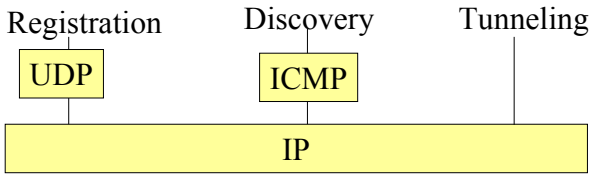


Figure 9-12: Mobile IP Processes

The solutions for Mobile IP consist of:

- Direct solutions provided by Mobile IP. For example, Mobile IP provides an authenticated registration process to assure that malicious nodes do not pretend to behave as foreign agents.
- Compensation solutions can enhance the Mobile IP by introducing additional encryption, authentication, and authorization.
- Special solutions may include monitoring the Mobile IP routing.

Mobile IP solutions are still evolving at the time of this writing.

9.10 Wireless Middleware Security

9.10.1 Overview

Wireless middleware, as discussed in previous chapters, is the set of software routines that reside above the network and below the applications to provide connectivity of mobile users to web content, databases, and applications. Security is the main concern of wireless middleware. However, different wireless middleware packages such as WAP and I-mode provide different security approaches in terms of authentication, data integrity, and data privacy. We discuss these approaches in this section. A review of SSL is presented first because SSL is used directly by some wireless middleware services such as I-mode, has been extended by WAP, and also fills in the gaps where necessary (e.g., between WAP gateways and Web servers).

9.10.2 Secure Socket Layer (SSL) for Wireless Web Security

Secure Socket Layer (SSL), also known as Transport Layer Security (TLS), is by far the most heavily used security technology for the World Wide Web. It is also used in wireless systems such as I-mode. At present, SSL is being packaged with almost all web browsers (Netscape Navigator, Microsoft Internet Explorer) and servers (Apache, IIS). SSL runs on top of TCP/IP and manages secure messaging on the network (see Figure 9-13). The SSL protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. SSL consists of software installed in browsers and on servers. All major browsers and servers today are "SSL capable". If needed, SSL software can be obtained by subscribing to a Secured Service Provider such as www.ssl.com or by obtaining a Server Certificate from www.ssl.com and installing it on an existing secured server. The SSL protocol provides, as we will see, a wide range of encryption and authentication choices to ensure that

communications between a client and a server remain private based on user requirements. The cryptographic choices are known as "cipher suites." A user can select a cipher suite when establishing an SSL session.

From an end-user point of view, the screen appearance of your browser with SSL is very similar to the one without SSL. To use SSL, you just need to type "https" instead of "http." For example, the link "https://www.fedex.com" connects you to the Federal Express website over SSL. If an SSL connection is successful, a lock appears in the bottom left part of your browser – the rest of your screen looks just about the same. Once an SSL session is established, all Web server-to-client traffic (both ways) is encrypted. This includes:

- URL of the requested document
- Contents of the requested document
- Contents of any filled-out forms
- Cookies sent from client to server
- Cookies sent from server to client
- Contents of the HTTP header

Thus SSL provides a great deal of confidentiality. However, you cannot hide that a particular browser is talking to a particular server. If this type of privacy is needed, then you should use a proxy server for unanimity.

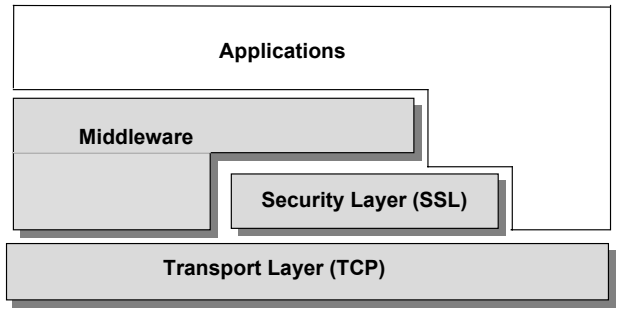


Figure 9-13: SSL

9.10.3 WAP Security and WTLS

9.10.3.1 WAP (Wireless Application Protocol) Security

WAP is a set of protocols to enable the presentation and delivery of wireless information and telephony services on mobile phones and other wireless devices. Three main constraints cause this market to be different from the wireline market. First, the wireless links are typically constrained by low bandwidth, high latency, and high error rates. Second, the wireless devices are constrained due to limited CPU power, memory and battery life as well as the need for a simple user interface. Third, wireless networks introduce challenging security issues, as discussed in previous sections.

WAP specifications address these issues by using the existing standards where possible, with or without modifications, and also by developing new standards that are optimized for the wireless environment where needed. The WAP specification has been designed such that it is independent of the air interface used or any particular device. A WAP gateway serves as the "middleman" for WAP by translating the WAP to non-WAP

(Internet-HTTP) protocols through adapters; it also enforces WAP security (see Figure 9-14). A detailed discussion of WAP was given in a previous chapter.

WAP should be analyzed for potential intrusion threats due to the weaknesses of the wireless security model. The WAP specification ensures that a secure protocol is available for transactions on a wireless handset. The Wireless Transport Layer Security (WTLS) protocol is based on the industry-standard Transport Layer Security (TLS) protocol, more popularly known as Secure Sockets Layer (SSL). WTLS is intended for use with the WAP transport protocols and has been optimized for use over narrow-band communication channels.

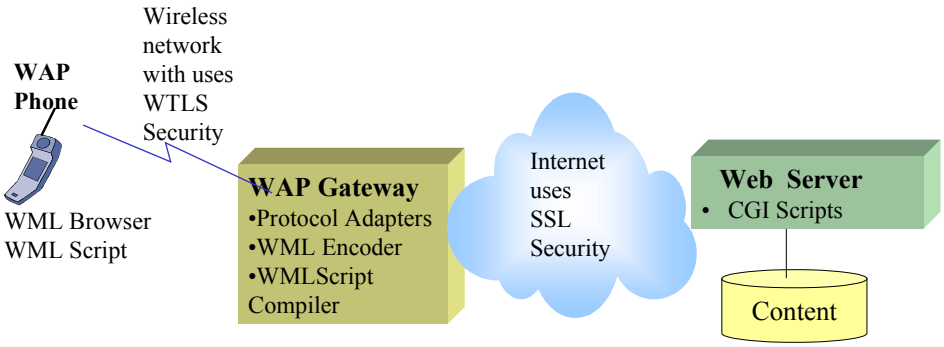


Figure 9-14: Conceptual View of WAP Security (WAP handset to Gateway uses WTLS, Gateway to Web Server uses SSL)

WTLS is not SSL, so it cannot directly communicate with SSL-enabled Web servers. As shown in Figure 9-14, WTLS works between the WAP client and the WAP gateway. The traffic from the WAP gateway to the Web server is typically protected by using SSL. Some implementations of WAP have a client-proxy-server model architecture where the proxy can be used to present a simplified view of familiar websites. An important security function performed by a proxy is that it unwraps the WAP WTLS secure data from the client and then rewraps it into SSL/TLS before passing it to a Web server. For Web applications that employ standard Internet security techniques with TLS, the WAP gateway automatically and transparently manages wireless security with minimal overhead.

WTLS can provide end-to-end security between WAP protocol endpoints. End-to-end security is achieved through two approaches: a) browser and origin server directly communicate using the WAP protocol, or b) a WAP proxy is trusted – by being, for example, located at the same physical secure place as the secure origin server.

WAP components can be attacked at several levels. Examples of the components that can be attacked are WAP clients and servers, the WAP gateway, and WAP messages. For example, intrusion of the WAP Gateway can have a very high impact on WAP users. It is important to secure the WAP Gateway through high levels of security. It should also be replicated. In addition, intrusion of WAP clients, servers and messages could have high impact. It is important to use authorization, authentication, and encryption by using WTLS. The implementation of WTLS by vendors needs to be watched.

9.10.3.2 A Closer Look at WTLS

WTLS ensures data integrity, privacy, authentication and denial-of-service protection – it does not support non-repudiation. The WTLS specification is designed to work even if packets are dropped or delivered out of sequence – a more common phenomenon in some wireless networks. Another issue is that some WTLS messages can be sent without authentication of origin. WTLS provides for client or server authentication and allows for encryption based on negotiated parameters between the handheld device and the WAP gateway. Users can implement any of the following three classes of authentication types:

- Class 1 (anonymous authentication). The client forms an encrypted connection with an unknown server. This has limited use (mainly for testing purposes) because end users have no way of determining the identity of those to whom they are talking.
- Class 2 (server authentication). Once clients are assured they are talking securely to the correct server, they can authenticate using alternative means, such as a user name/password. This is a very common model for WTLS usage. Keep in mind that WTLS certificates are not the same as X.509 certificates, and they cannot be used interchangeably.
- Class 3 (server- and client-authentication). The server and the client authenticate each other's WTLS certificate. This is the strongest class of authentication. Client certificates required for Class 3 authentication pose special management problems because the key pairs must be generated and managed on the handheld device (see the sidebar "Maintaining WTLS Certificates on Mobile Devices").

The WTLS specification does specify cryptographic algorithms that may be supported by WAP devices, but does not require this feature. For example, the WTLS specification provides support for the RSA and Diffie-Hellman key exchanges; most vendors are supporting RSA because of its widespread use. Similarly, several bulk encryption ciphers are specified; however, DES and 3DES are used most widely. In addition, WTLS supports various key lengths used with the bulk encryption algorithms, so that the security parameters can be negotiated based on user needs. The main consideration in WTLS security is to make low CPU-powered wireless devices secure by making the cryptography efficient. Because PDA and cell phone CPUs are typically slow, using SSL from end to end can take more than a minute, depending on the key size used to negotiate an SSL connection. Specialized cryptographic algorithms such as Elliptic Curve (EC) cryptography are more promising than RSA for CPU-starved PDAs and cell phones because they require far fewer resources.

Unlike SSL, WTLS does not provide for end-to-end security between WAP clients and Web servers. End-to-end security means the client and server have a secure session, without any intervening servers. When your Web browser sets up an SSL session with a Web server, the browser and Web server are communicating directly. As discussed previously, when you send your credit-card number over SSL, in effect, only the receiving Web server can receive it. WTLS works between the WAP client and the WAP gateway, as shown in Figure 9-14. The WAP gateway terminates the WTLS sessions and initiates SSL sessions to the destination Web server. The potential problem exists at the WAP gateway. Between the time the data is decrypted and "decapsulated" from WTLS and WAP and re-encapsulated and re-encrypted in SSL, the protected data is exposed – albeit for only a very short time (fraction of a millisecond). For most applications and users, this should not be a problem because to access this data, someone has to break into the WAP gateway.

Maintaining WTLS Certificates on Mobile Devices

Client certificates required for WTLS Class 3 authentication pose special management problems because the key pair associated with the client certificate resides only on the client.. First, the key pairs must be generated on the mobile device (or generated and loaded onto the mobile devices). Second, the client certificate has to be safeguarded and managed until the certificate expires. This creates several additional problems. The client certificates can be retained on the handheld device, raising concerns about theft. Alternatively, the client may refer the WAP gateway to a directory to retrieve the client certificate from a directory. This saves the communication bandwidth needed to send the client certificate over the air; however, the WAP gateway must trust the directory the client refers to in order to assure authentication. The certificate directory also must be available at all times to allow users to retrieve the certificate when requested.

9.10.4 I-Mode Security

I-Mode, from NTT DoCoMo (http://www.nttdocomo.co.jp/), is a competitor to WAP. I-mode security is important because it has millions of users. In particular, mobile commerce (mcommerce) is conducted on i-mode including mobile banking and security trading. From a security point of view, i-mode consists of the following features (see Figure 9-15):

- Security of the radio link between the i-mode handset and the cellular base station is provided through proprietary protocols and encoding controlled by NTT DoCoMo. Digital radio packets sent between handsets and radio towers are encoded via this proprietary NTT DoCoMo scheme.
- Encryption and authentication of the data between i-mode handsets and Docomo websites is supported by SSL. To support 128-bit encryption in SSL, Docomo has embedded digital certificates into its cellular phones. Digital certificates supplied by companies such as VeriSign and Baltimore Technologies are built into the i-mode phones such as the 503 cellphones and others. The SSL-based authentication and encryption make i-mode sessions secure when users are accessing websites that offer digital certificates.
- Security of private network links between the i-mode center and special service providers such as banks is sent via 128-bit SSL-encrypted dedicated lines typically over wired networks. This transmission is between the i-mode server and the bank server that does not use radio packets through the air.

I-mode network and i-mode handsets are equipped for SSL (secure socket layer) encrypted transmission, and i-mode handsets have unique identifiers allowing similar security to be implemented as on the wired Internet. Mobile banking on i-mode and corporate networks usually uses SSL encrypted communication.

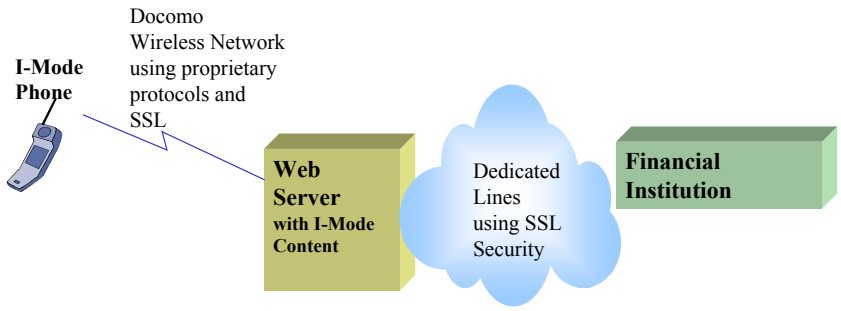


Figure 9-15: I-Mode Security – Conceptual View

9.10.5 Wireless VPN Versus WAP Security

Wireless VPNs work well in situations where you do not have a WAP gateway or if you have to support mobile users who do not have a WAP/WTLS microbrowser. On the other hand, wireless VPN is mostly restricted to handheld devices such as palm pilots because cell phones do not have the processing power or memory to run VPN software. The success of PDA-based VPN clients largely depends on the ease of use and VPN efficiencies that can be achieved on low-powered PDAs. VPN client software for the Palm and Palm Pilot is commercially available from companies such as Geritome and Top Gun.

9.11 Short Examples and Case Studies

9.11.1 Wireless in Government Services

Government agencies see great potential in wireless technology, for police services, satellite offices, temporarily relocated employees, and training through virtual classrooms. While many of the government-issued handheld devices are still used primarily to send and receive email, an increasing number are being loaded with job-specific software – as is the case with OnPatrol in Canada for police patrols. The US military is using BlackBerry handhelds for wireless management of inventory, and to help track medical records of armed-forces personnel. Sky marshalls employed at airports since 9/11 are now using the technology to communicate both with one another and with other law-enforcement officers. And, there is a widespread use of handheld devices among members of the US and Canadian federal legislatures.

Schools in remote communities have been interfacing satellite communications with wireless local-area networks (WLANs) to provide local high-speed Internet service. This opens the door to a world of educational opportunity. WLANs can enable Internet-based communication in places where wires either do not exist or cannot be installed.

Several police force offices across Canada are using a wireless solution, called OnPatrol, that involves software developed specifically for police agencies. The software is loaded onto Research in Motion (RIM) Wireless Handheld™ devices. This solution enables foot-patrol officers to securely query police databases, as well as to send and receive messages. Officers do not have to stop and write out details of a complaint because all

the information is contained in their handheld. OnPatrol is being built by xwave, a services provider that has worked with public sector organizations .

Several wireless applications are also being developed for Environment Canada (EC). The department has developed a wireless network to allow visiting EC executives from across Canada to connect easily with their regional offices. EC will also use the wireless network for presentations and training.

Security is of critical importance to government organizations using wireless technology. For example, the Canadian police officers are keen to try the handhelds but recognize the obvious security concerns associated with such small, portable devices. The EC wireless network has been developed with security as a high priority. Different measures are being used to secure these wireless networks. The idea is end-to-end encryption: from the moment the message leaves one device to the moment it is received by another. The messages are encrypted on transit and remain so while stored on the devices.

For example, a VPN is being used for securing the EC wireless access to add an extra layer of encryption, which makes the network much more difficult to break into. In addition, the OnPatrol has been developed with close attention to security. Along with incorporating 128-bit encryption, OnPatrol makes use of a log-in screen, through which users sign on with a password. As well, the device includes both application-lock-out and remote-device-erasure capabilities: application lock-out essentially shuts the device down if the wrong person repeatedly and incorrectly tries to log onto it; remote-device-erasure allows a user to disable a lost or stolen device by erasing the information contained on it.

For wireless LANs, a mixture of techniques are used. Specifically, the Wired Equivalent Privacy (WEP) encryption is turned on, the Media Access Control (MAC) address transmission is turned off, and the Service Set ID (SSID) is changed. This selective enablement/disablement makes the network harder to break into. In addition, the power-transmission levels are lowered to suit a smaller space and avoid undue eavesdropping. It is also a good idea to make sure that the vendors are FIPS-compliant (FIPS- 140-1 certification is granted to vendors that meet the security standards established by the US National Institute of Standards and Technology [NIST]).

Source - http://www.xwave.com/ebrochures/wireless_security_cs_frames.htm

9.11.2 Wireless Security in the Health Sector

Wireless communication is at the forefront of technologies being considered by the healthcare sector. There are a number of reasons why wireless communication holds such an appeal for medical practitioners and institutions, but security concerns are the major deterrents.

A major benefit of wireless communications is in the area of doctor/patient relationships. Medical practitioners must keep a large amount of collected data on all their patients. This is generally done by using a database or a paper-based filing system. A paper-based system has several obvious flaws (patient medical records can be easily lost or damaged). Even when stored on electronic databases, the doctors often have the patient's records printed to hard copy before seeing the patient. In addition, manual updates are normally performed by an office assistant based on written notes provided by the doctor – an error-

prone process. By providing a medical practitioner with a Personal Data Assistant (PDA) connected to a wireless network, these problems can be readily overcome. All patient records can be updated in real-time by the doctor without the risk of them being lost or damaged.

Wireless communications can also be of great value to doctor/institution relationships. It is not easy for doctors to keep track of medication prescriptions and billing information. For example, hospital residents commonly carry around scraps of paper containing such information for entire shifts. This can often lead to the loss or damage of such information – an outcome that is unsatisfactory and potentially financially damaging to the institution. Wireless billing improves the accurate maintenance of financial records of this type and is also considerably faster and more efficient.

But wireless networks are vulnerable to attacks as discussed in this chapter. For example, a hacker parked in the street outside an institution with no more than a laptop and a $200 wireless network card could read all of the information being passed between the doctor's PDA and the medical record server, without even leaving the vehicle. Letting a hacker access this information is a violation of doctor/patient privilege, and failing to adequately secure the information is a violation of the US Health Insurance Portability and Accountability Act (HIPAA 1996). A malicious hacker could also potentially cause financial damage to the institution by misusing the information. All are obviously big problems with serious consequences.

A wireless network can be secured in a variety of ways discussed in this chapter. For example, SSL can be used to encrypt commercial transactions over the Internet. SSL is the ideal solution to server-side security problems since most web/application servers like IBM's WebSphere support the use of SSL for communications. The process of setting up server-side SSL is normally no more difficult than generating a new key-pair and directing the web/application server to use it for encrypting the communications. Unfortunately, SSL support is not common on wireless client devices.

Without SSL support on the client-side, SSL cannot be supported across the communication channel. Even those clients that do have SSL support often have widely varying implementations that must all be supported in different ways.This can become a major issue in networks with many different types of client devices, as it leads to longer rollouts and higher maintenance costs. The only real solution to this problem is to use a Java-based SSL implementation which provides SSL in a completely platform independent way. The problem is that these Java implementations typically are too resource-hungry for the limited resources of the average wireless client.

What is really needed is a Java-based SSL solution especially designed for the limited hardware requirements of the average PDA. Companies such as Wedgetail Communications provide a number of small-footprint security implementations designed especially for wireless network devices. Of particular importance to this problem is the JCSI® Micro Edition (Java Cryptography and Security Implementation®, Micro Edition) Wedgetail Communications. JCSI Micro Edition provides an SSL/TLS library that supports RSA encryption and is also compatible with all Java™ 2 Micro Edition (J2ME™) implementations. This means that client applications only need to be written once and can run over a wide variety of wireless clients in the network.

Source: http://www.wedgetail.com/datasheets/ehealth_case_study_us.pdf

9.11.3 Wireless LANs at Texas A&M University

It is well known that many universities are going wireless. There are several reasons for this. Wireless access is a natural fit for the highly mobile university population. In addition, wireless access is a strong recruitment tool at universities to attract top-notch students, faculty and prestigious conferences. However, the rate of wireless adoption on campuses raises several security issues, because universities are populated with bright and highly energetic students who like to probe and investigate. In addition, university networks tend to be more open than corporate environments. Intrusions into proprietary or exclusive research data, as well as into course grades and student information, need to be detected and avoided.

Texas A&M has implemented a large wireless network that is protected by a wireless VPN. The university felt comfortable with this choice because it already had experience with a wired VPN. Wireless users are authenticated through a RADIUS server – all users of a laptop or handheld device in an area with a wireless access point (AP) get routed to a VPN server and RADIUS authentication. The school has adopted, like many other campuses, the 802.11b standard for its wireless transmission. The campus network includes a wired network with Ethernet ports and wireless access points in dorm rooms, campus libraries, and conference rooms in the Bush Presidential Center. The network administrators create short-term users in the school's RADIUS authentication server database, giving guests access only while they are visiting.

Texas A&M took advantage of its student population, especially the telecommunications engineering undergraduate students, to design and test the system. After examining several vendors, Texas A&M decided to use Cisco and Enterasys access points because of their flexibility with multiple cards. The university has no plans to entirely go wireless – the wired network still will be used to interconnect buildings.

Source: Saita, A., " The Wild Wireless West – Texas A&M brings law and order with WLAN," *Information Security Magazine*, January 2002.

9.12 Summary and Conclusions

Security concerns are growing more serious due to the widespread use of wireless networks. Although wireless networks face the same type of security issues (e.g., privacy, integrity, authentication) as the wired networks, the main difference is that wireless network traffic is transmitted over the air and so is easier to tap into than traffic in wired networks. This chapter has provided enough details about various wireless security issues so that a sound solution can be developed. The design procedure includes all levels of security: enterprise applications and corporate databases, middleware security (web and WAP security), and network-level security (VPNs and wireless link security).

9.13 Suggested Review Questions

1) What are the issues that are unique to wireless communications?

2) Create a table that shows different types of wireless security issues at various levels and the key technologies that are used to address these issues

3) What are the main problems in Wi-Fi security? Why is it a major concern and what specifically can be done to address these problems?

4) Why should anybody care about wireless PAN security? Are there some unique issues and approaches to solutions in this area?

5) What are the unique issues in cellular networks? What exactly do 3G networks offer in this area?

6) What are the main concerns in satellite security and what are the key practical approaches?

7) Is wireless local loop security a major concern for the everyday consumer? Who needs to worry about these issues?

8) How can FSO and UWB provide better security? What type of wireless networks can benefit from these emerging networks?

9) What are the most serious problems in MANET security? What appears to be the most promising approach?

10) Where does Mobile IP fit in the wireless security landscape? Be specific.

11) What are the wireless middleware issues in WAP and i-Mode? Why do they need to be discussed separately?

9.14 References for Wireless Security

Aron, M. "Better Security Needed for B2B." *Australasian Business Intelligence,* Nov. 4, 2002.

Arbaugh, W., et al. "Your 802.11 Wireless Network has No Clothes." Department of Computer Science, University of Maryland, College Park, Maryland 20742, March 30, 2001.

Borisov, N., Goldberg, I., and Wagner, D. "Intercepting Mobile Communications – The Insecurity of 802.11." Available at http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Brewin, R. "FAA Views Aircraft Satellite Security Systems as 'Complex Undertaking.'" *Computerworld*, Oct. 20, 2001.

Bucheggar, S. and Le Boudic, J. "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks." *Proceedings of 10th European Workshop on Parallel, Distributed and Network-based Processing*, 2002.

Byers, S. and Kormann, D. "802.11b Access Point Mapping." *Communications of ACM*, May 2003.

Castro, M. and Liskov, B. "Practical Byzantine Fault Tolerance." In *Proceedings of the 3rd Symposium on Operating System Design and Implementation*, New Orleans, February 1999.

Cam-Winget, N. et al. "Security Flaws in 802.11 Data Link Protocols." Communications of ACM, May 2003.

Desmedt, Y. and Jajodia, J. "Redistributing Secret Shares to New Access Structures and its Applications." *Technical Report ISSE TR-97-01*, George Mason University, July 1997.

Fratto, M. "Tutorial: Wireless Security." *Network Computing Magazine*, January 22, 2001.

Haas, Z. and Liang, B. "Ad hoc mobility management using quorum systems." *IEEE/ACM Transactions on Networking*, 1999.

Herzberg, A. "Payments and Banking With Personal Devices." Communications of ACM, May 2003.

Housley, R. and Arbough, W. "Security Problems in 802.11-based Networks." Communications of ACM, May 2003.

LAN97. "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer(PHY) specification. IEEE Standard 802.11, 1997 Edition," 1997.

Oppliger, R. "Security Technologies for the World Wide Web." Artech, 2000.

Noubir, G. "Optimizing Multicast Security over Satellite Links." European Space Agency Project, *Work package 20 report*, version 0.1, April 1998.

Noubir, G. and Allmen, L. "Security Issues in Internet Protocols over Satellite Links." *Proceedings of the IEEE VTC '99*.

Ramanathan, R., and Redi, J. "A Brief Overview of Ad Hoc Networks: Challenges and Directions." *IEEE Communications Magazine*, May 2002.

Roberts, P. "Government Report Finds Satellite Security Lax." IDG News Service, Oct. 4, 2002.

Schmidt, T. and Kormann, D. "Why Wi-Fi Wants To Be Free." *Communications of ACM*, May 2003.

Sheldon, T. "General Firewall White Paper." Available at http://secinf.net/info/nt/fw/firewall.html, Nov. 1996.

Stallings, W. *Network Security Essentials*. Prentice Hall, 2000.

Stein, L. *Web security: A step-by-step Reference Guide*. Addison Wesley, 1998.

Sun, J. "Mobile and Ad Hoc Networking: An Essential Technology for Pervasive Computing." Info-tech and Info-net International Conference, Beijing, 2001.

Walker, J. "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000. Available at http://grouper.ieee.org/groups/802/11/Documents/ DocumentHolder/0-362.zip

Walker, J. "Overview of 802.11 security." Available at http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3

Wexler, J. "Satellite VPNs to Address Performance and Security Issues." *Network World Wireless in the Enterprise Newsletter*, March 17, 2003.

Wexler, J. " Satellite: What's at Risk?" *Network World Wireless in the Enterprise Newsletter*, Oct. 16, 2002.

Zhou, L., and Haas, Z. "Securing Ad Hoc Networks." IEEE Network, 1999. Available at http://citeseer.nj.nec.com/zhou99securing.html

9.15 PART III - NRW Case Study Revisited: Securing Wireless and Wired Networks

9.15.1 Overview

Let us revisit the NRW case study with special attention to wireless and wired networks. A conceptual model of a NRW system is shown in Figure 9-16 for convenience. The NRW corporate web site, as indicated before, consists of a user interface that connects to an Accounts Balance Program (ABP) that allows customers to view, update, and modify account information; a customer database that contains information about customers; an investment database that contains investment data; and other typical corporate applications and databases for payroll, accounts payable/receivable, etc. The following sections expand the NRW case study analysis in Chapter 3. The focus here is on the risks introduced by wireless networks, and on the circumvention approaches available.

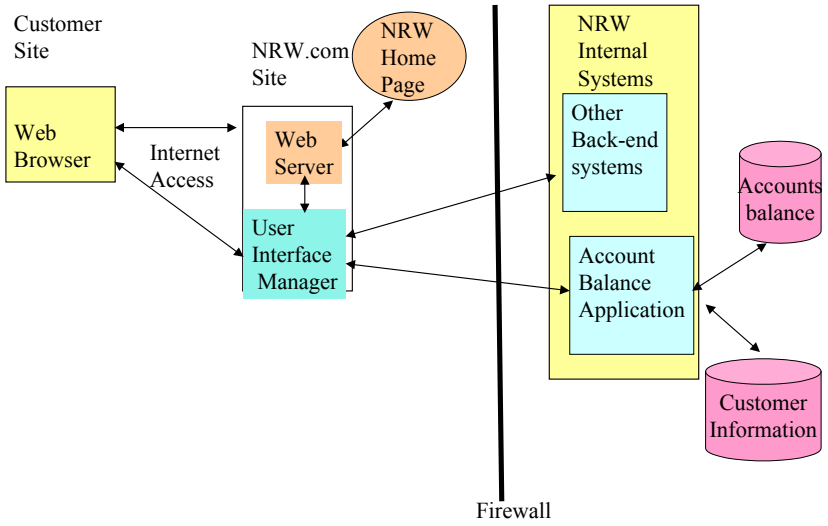


Figure 9-16: NRW System Conceptual View

9.15.2 Detailed Physical Model for Wireless and Wired Network Security Analysis

Figure 9-17 shows a detailed physical model of the NRW system with wired and wireless networks. In this system, the NRW itself is a three-tiered system in which the ABP resides on an NT server, the data is on a Unix server and the back-end systems are

at the mainframe. Many other technology components such as middleware are shown here for completeness, but they are of no concern at present (we will bring them back to life in our next visit to NRW at the end of Chapter 12). We are more concerned about protecting the path – the networks that interconnect the various players.

Our specific focus is on securing the corporate intranet that operates in the building and is connected to the public Internet. There are two firewalls – one firewall protects the internal corporate resources from the public Internet traffic, and the other is an internal firewall that provides additional protection to the back-end systems. Both of these firewalls need to be examined more closely. In addition, NRW is introducing an 802.11 wireless LAN in the corporation, and internal users should be able to access the NRW system from this WLAN, as shown below. External access from cellular phone through WAP has been suggested, but the company is not ready. This will still need to be discussed.

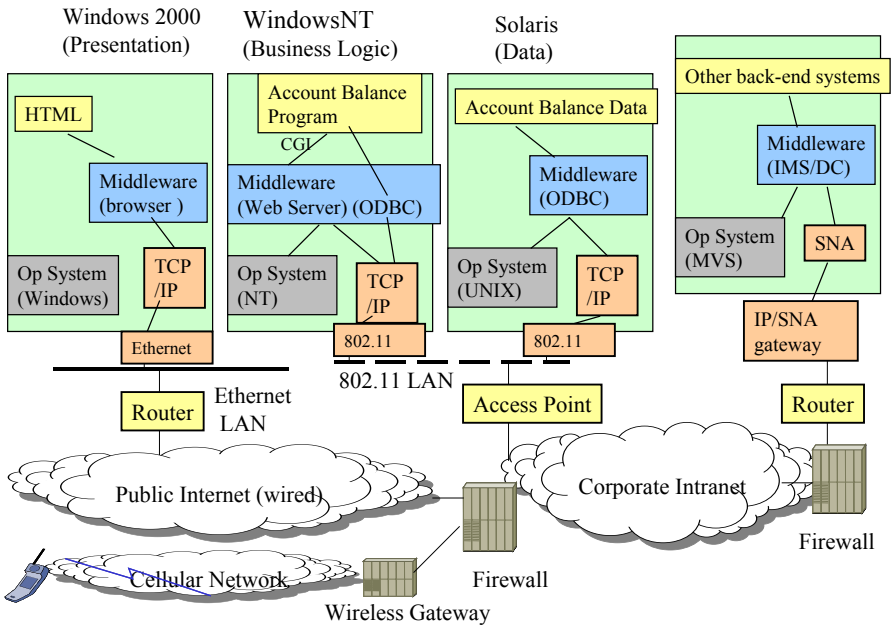


Figure 9-17: NRW System – Detailed View with Wireless and Wired Networks

9.15.3 Analyze Security Risks

The main risk of a wired network is that anyone with browser access over the public Internet can potentially invoke the ABP. This opens up many denial-of-service and other types of attacks. In addition, the internal corporate intranet, an ATM network, needs to be protected from potential intruders.

The internal/external wireless access for account management will potentially expose NRW to several security risks such as the following:

- Denial-of-service attacks can be launched by any number of means. For example, wireless network outages, network flooding, viruses, hackers, or physical equipment problems could all deny users the ability to conduct business with NRW.

- Wireless access from internal and external users will expose the company to several additional assaults on privacy, integrity, authentication, etc.
- Unauthorized wireless users may access information on customers, accounts and research information.
- Man-in-the-middle assaults, or attacks by wireless users using falsified authentication, are especially bothersome.

Should any of these events occur, NRW will risk damage to its internal systems and also to its reputation, resulting in significant loss of business. These risks can be represented in terms of the risk matrix R(i,j). For the NRW example, we can develop Table 9-4 to reflect the security risks R for a few major components – the rows – that are important for wired/wireless networks: the Public Internet, the Corporate Intranet, the internal 802.11 LAN, the external cellular network, the WAP gateway, and the two firewalls. For these components, the risks are specified in terms of PIA4 – the columns. Risks for additional components and sub-components can be similarly specified. This table only reflects the risks for compromise of each network component and not the resources that are accessed through these components. This is thus a *local* risk analysis. This table only reflects an illustrative sample – you can change values if you wish.

Table 9-4: Example of a Security Risk Matrix R

	Privacy Risks	Integrity Risks	Authentication Risks	Authorization Risks	Accountability (NR) Risks	Availability Risks
Public Internet	H	H	H	H	M	VH due to denial-of - service attacks
Corporate intranet	H	H	H	H	M	H (internal users can flood the internal network)
802.11 LAN	L	L	L	L	L	M-L (internal network)
3G Cellular Network	H	H	H	H	L (Audit trails for cellular users done at higher level – WAP)	H (need to provide external support)
Wireless middleware (WAP gateway)	H	VH (WAP gateway compromise could be disastrous)	H	H	M (Audit trails of WAP users kept)	H (WAP gateway must be available to support cellular users)
Firewall for the public Internet	M (firewall itself not easy to compromi se)	M	M	M	M	VH due to denial-of - service attacks
Firewall for the corporate intranet	L (internal firewall itself not easy to	L	L	L	L	VH due to denial-of - service attacks

	compromise)					

9.15.4 Develop Countermeasures

Now we need to develop the solutions to mitigate the risks. Let us summarize the results for NRW:

- VPN will be used to protect the public Internet access. VPNs provide encryption and authentication features over public networks for secure communications. Before a NRW VPN device communicates with another, it first must establish a password. Authentication systems like NRW's are based on digital certificates that are more secure than a password-based authentication. NRW would want to ensure that its network is semi-private, meaning that only business partners have access to the network. NRW would want a network effectively capable of detecting intrusions.
- The NRW's corporate intranet has to be highly controlled. This means that only NRW's data center personnel have physical access to NRW's application server and network equipment. If a business partner owns a piece of equipment it is to be shared between both organizations.
- The wireless LAN inside the corporation should use the latest 802.11 security available. Use of TKIP in the internal wireless network is recommended.
- The wireless LAN should be placed outside the public Internet firewall so that the traffic on it is treated as external traffic.
- Firewalls will be important to localize the different areas of the firm's security architecture. The external as well as internal firewalls have to be protected very heavily to assure that the attackers do not access and manipulate these firewalls.
- For quality of Service, NRW should ensure availability, latency, bandwidth & response time of its intranet. Quality of service should not be compromised in any security system. Servers should be physically secured and backup power sources should be available.
- NRW should take Non-repudiation (NR) into consideration. Non-repudiation is the ability to provide proof of the origin or delivery of data. NR protects both senders and recipients in a data interchange. A receiver (NRW) cannot say that he/she never received the data and the sender (customer) cannot say that he/she never sent any data.
- WTLS certificates should be used with handheld devices for cellular access.
- Migration to 3G cellular should be expedited to take advantage of the 3G security.