

Version of November 19, 2004

An overview of the security of wireless networks

Eduardo B. Fernandez, Imad Jawhar, Maria M. Larrondo-Petrie, and Michael VanHilst
Dept. of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL

Introduction

More and more applications are being accessed through wireless systems, including commerce, medical, manufacturing, and others [Var00]. Wireless devices have become an extension of corporate databases and individuals. Their security compromises are as serious as any attack to the corporate database and may have damaging effects on the privacy of individuals and the protection of assets of an enterprise. Wireless devices include cellular phones, two-way radios, PDAs, laptop computers, and similar. These are normally portable devices with limitations of weight, size, memory, and power. The increase in functions in cellular devices creates new possibilities for attacks. Standard attacks against the Internet may now take new forms. Lists of vulnerabilities are already available, showing flaws in many existing products [Iss, Mit].

Communicating in the wireless environment has its own issues and challenges. It is characterized by relatively low bandwidth and data rates, as well as higher error rates, and the need for low power consumption (for mobile devices). The mobility of the nodes in cases such as ad hoc networks adds another significant layer of complexity and unpredictability.

There exist many different forms of wireless communications and networking [Sta02]. Some popular forms of wireless communications include:

Satellite communication: It uses microwave links, and provides global connection of many network infrastructures. There are three basic classes of satellites: GEO (Geostationary Earth Orbit), MEO (Medium Earth Orbit), and LEO (Low Earth Orbit).

Cellular networks: These are currently among the most widely used types of networks. The geographic area is divided into *cells*. Each cell is serviced by a *base station* (BS) and several base stations are served by a Mobile Telecommunications Switching Office (MTSO) or a similar structure. The latter provides connection to the wired telephone infrastructure. The new generation of cellular networks uses digital traffic channels, encryption, error detection/correction, and allows channel access to be dynamically shared by all users. *Global System for Mobile communication* (GSM) standard is widely used. The configuration of a typical cellular network is shown in Figure 1.

Cordless systems: They are used inside homes and buildings, and provide wireless communications between a cordless device such as a telephone and a base station.

Typically, TDMA (Time Division Multiple Access) and TDD (Time Division Duplex) communication protocols are used in such systems.

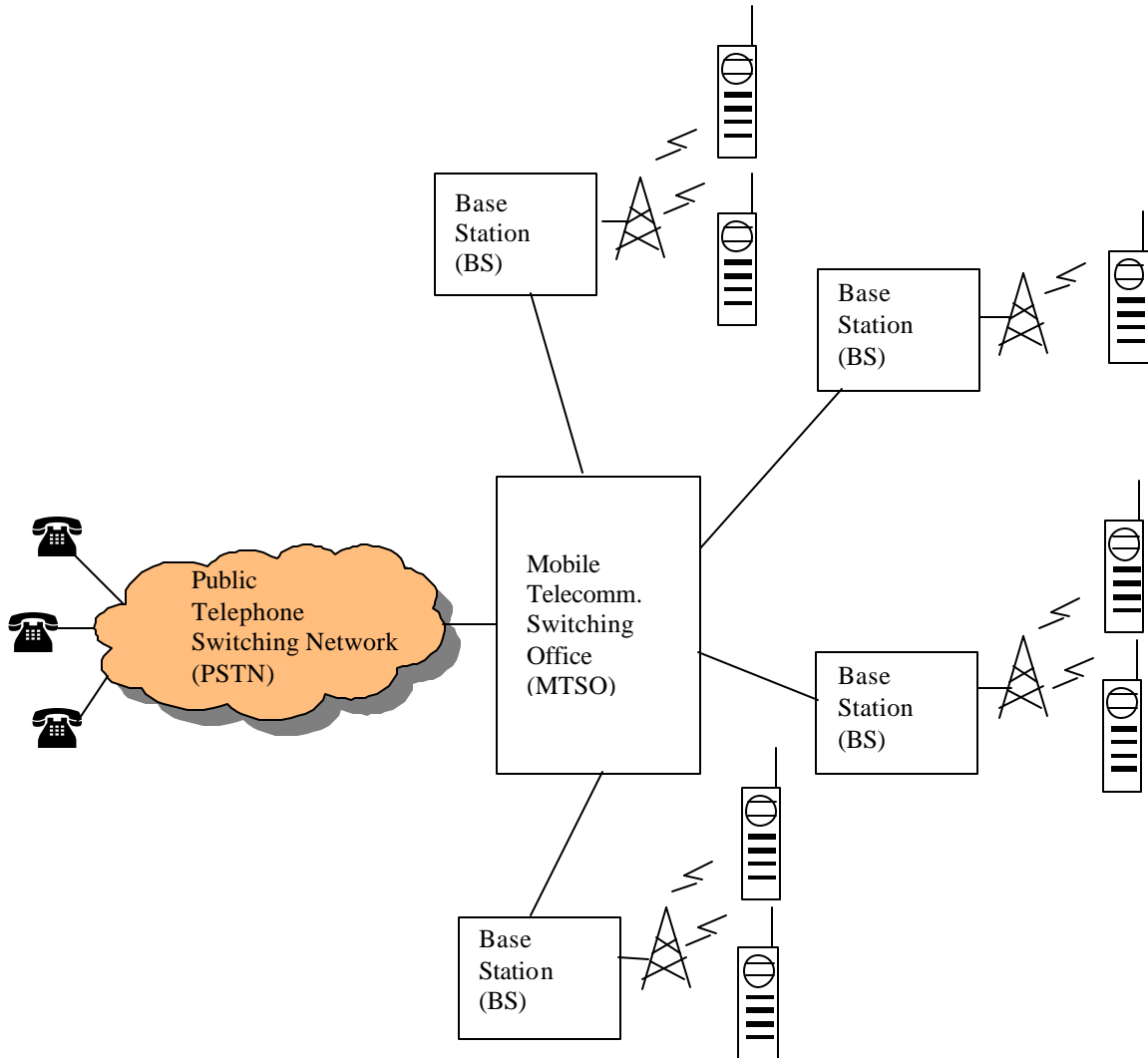


Figure 1 Configuration of a cellular network

Wireless Local Loops (WLL): They are used to provide last mile connections from the end user to the local switching telephone center. They have an advantage over their wired counterparts in low cost and relative ease of installation which can be done selectively and on demand.

Mobile Internet Protocol (Mobile IP): It provides nomadic access from different access points allowing the user to maintain connectivity as he/she moves from one access point to another. Mobile IP includes processes of registration, move detection, agent solicitation, and tunneling of data messages.

Wireless Local Area Networks (WLANs): They have increased popularity due to their characteristics of mobility, convenience, rapid deployment, and cost effectiveness, in addition to the small size, and increased power and speed of wireless devices. Two standards are typically used: IEEE 802.11 (Wi-Fi) and Bluetooth.

There are four types of WLANs:

LAN extensions: They allow connection between mobile wireless devices and a wired network. Some example applications are manufacturing stock exchange, and warehouses.

Cross-building interconnects: They allow fast wireless connections between buildings. Microwave communications with dish shaped antennas are used. This type is a link more than it is a LAN.

Nomadic access: It is used to allow communication between mobile devices such as laptops, and PDA's to existing fixed wired networks. For example, applications can use such systems to transfer data from wireless devices to the home, office, or campus network.

Mobile ad hoc networks (MANETs): As mobile wireless computers and devices become increasingly smart, small, portable, and powerful, the need to interconnect these devices increases. MANETs allow such computing devices to establish networks on the fly without any pre-existing infrastructure. Numerous applications exist using MANETs such as disaster recovery, military missions, classrooms, and conferences. Multi-hop routing is used to provide communication between nodes (e.g. laptops or computers inside moving vehicles) that are out of range of each other. Each host provides routing capabilities to the mobile network. MANETs have dynamic topologies as nodes are allowed to move from one location to another, as well as join, and leave the network at any time. Typically, these networks use Wi-Fi and Bluetooth which are discussed later in this chapter.

The security of wireless systems can be divided into four sections:

- Security of the application. This means the security of user applications and standard applications such as email.
- Security of the devices. How to protect the physical device in case it is lost or stolen.
- Security of the wireless communication. How to protect messages in transit.
- Security of the server that connects to the Internet or other wired network. After this server the information goes to a network with the usual security problems of a wired network (not discussed here).

We now look at each aspect in turn.

Application security

Application development

There are two common approaches for user applications in wireless devices: WAP (Wireless Application Protocol), and applications based on the two standard component approaches, J2ME and .NET. The latter include standard object-oriented applications or applications using web services. Middleware software supports wireless applications at both the client and server sides [Vau04]. Devices using Bluetooth can use Java [jav] or .NET.

WAP

WAP is a thin-client (micro browser) development protocol, specifically designed for development of user applications. WAP uses WML (Wireless Markup Language) and WMLScript to develop applications that can be interpreted at the browser and accessed at the server using HTTP. WAP requires a gateway to the wired Internet, and cannot store and process data locally.

WAP uses WTLS (Wireless Transport Layer Security) [Ash01]. This protocol provides confidentiality, integrity, and authentication and uses RSA cryptography, but can also use Elliptic Curve Cryptography. It is based on the IETF SSL/TLS protocols. WTLS provides security for communications between the WAP wireless device and the WAP gateway (discussed later). Current WAP devices use Class 2 WTLS, which enforces server-side authentication using public key certificates similar to the SSL/TLS protocol. Future Class 3 devices will also allow client-side authentication using certificates. This level will use a WAP Identity Module (WIM), with mandatory support for RSA public keys and optional support for elliptic curve cryptography.

Web services

A web service is a component or set of functions accessible through the web that can be incorporated into an application. Web services expose an XML interface, can be registered and located through a registry, communicate using XML messages using standard web protocols, and support loosely-coupled connections between systems. Web services represent the latest approach to distribution and are considered an important technology for business integration and collaboration.

Wireless devices can access web services using SOAP (Simple Object Access Protocol). Web services are still not widely used in portable devices [Gra04]. The limited processing power of portable devices and the lack of network reliability are a serious obstacle for a full implementation. Using appropriate gateway middleware, it is however possible for portable devices to access web services.

There are several toolkits that simplify the process of building applications using web services. For example, Java-based client systems can use Sun ONE and kSOAP [Yua02a], while server-side systems can be built with Sun or IBM toolkits [ibm]. There are similar tools for .NET-based systems. In addition to the specific designs used, security also depends on the security of these component platforms [Fer04a].

The richness of web services brings along a new set of security problems [Fer02]. All the attacks that are possible in wired systems are also possible in wireless systems using web services, e.g., viruses, buffer overflow attacks, message interception, denial of service, etc. Web services introduce several extra layers in the system architecture and we have to consider the unique security problems of these layers. Since these are layers that run on top of the platform layers, the security of the platforms is still fundamental for the security of the complete system. Wireless systems using web services have to face, in addition, the general vulnerabilities of wireless networks and may also add new security problems to these networks although this aspect has not been explored in detail. There is also a variety of standards for web services security and a designer of wireless devices should follow at least the most important ones to be able to have a credibly secure system. On the other hand, the extra layers bring more flexibility and fineness for security; for example, encryption can be applied at the XML element level, authorization can be applied to specific operations in a web service interface. This greater security precision allows applying policies in a finer and more flexible way.

WAP applications have fewer security risks compared to web services. On the other hand, their functionality is considerably lower.

Personalized information

An important mobile application aspect is the delivery of personalized information to subscribers [Dog02]. Using specialized interfaces users are able to select services offered by some companies; for example, lists of stores who have sales, stock market alerts, etc. Some of these services may be location dependent, e.g., lists of nearby restaurants. Clearly, the companies that provide these services need to control access to their customer information, which in addition to the usual information about credit and SSNs includes now a privacy aspect (the company is able to track the client movements).

Access control to sensitive information in or through the device

The portable device may contain files that need to be restricted in access and it is the function of its operating system to perform this control. Control of types of access is important; for example, a user may play a song, but she may not copy it. This type of control can complement other types of digital rights management.

When portable devices need to access corporate databases some type of Role-Based Access Control (RBAC) is necessary, where users can access specific data related to applications such as banking, shopping, health, navigation, and surveillance. Management and enforcement of application and institution constraints can be performed following PMI (Privilege Management Infrastructure) [Cha01]. PMI is a standard of ITU X.509.

Viruses and other malware

With increase in functions, the typical problems of larger systems are also appearing in portable devices. One of these problems is attacks by viruses [Fol01]. The first portable virus to appear was Liberty, followed shortly by Phage. The WML script language used

by WAP can also be a source of possible attacks [Gho01]. The devices do not distinguish between script code from the phone or downloaded from potentially insecure sites, all of it executes with the same rights. An infected device can be used to launch denial of service attacks on other devices or the network. Similarly to wired systems, up-to-date antivirus programs are needed. Companies such as Symantec, McAfee, and Trend Micro have specialized products for handheld devices.

Downloaded contents

Downloaded contents may include malicious software. Another issue is the control of unauthorized copying of downloaded contents, such as music, wallpaper, and games. This is a problem of digital rights management.

Location detection

Location detection is a problem unique to mobile devices. The actual location of the device should be kept hidden in some cases for privacy or for strategical reasons.

It is possible to control access to VLANs by associating users with access points. There are products that can keep track of users and access points and use this information for network administration [Cox04].

Operating system security

Portable devices have evolved from having ad hoc supervisors to standard operating systems. Some systems use the Java run-time system as supervisor. High-end cell phones run complete operating systems such as Palm OS or Microsoft Windows CE, and provide IP networking capabilities for web browsing, email and instant messaging. Some typical security features include:

- *A unique device identifier*—this can be provided and can be accessed by an application.
- *A kernel configuration with enhanced protection* ---this allows using the protected kernel mode, instead of the full-kernel mode, while running threads to prevent accessing certain physical memory.
- *Digital authentication in the dial-up boot loader*—the dial-up boot loader is a program in ROM used to upgrade the OS image file (NK.bin) using flash memory or a remote server. The OS image file should be signed using digital encryption to verify its integrity before it is downloaded.

Smartphone [mic04] is a Windows CE-based cellular phone that comes bundled with a set of applications, such as address book, email, and calendar. The provider that sells the Smartphone can limit the devices' ability to load and run programs. A locked cell phone either restricts unsigned applications or does not run them at all. Depending on the provider, an encryption key may be needed to run the application [Alf00].

It is clear that, similarly to larger systems, the operating system is fundamental for security. Since many of the security flaws of Microsoft's operating systems come from their general approach to systems design [Fer04], one should watch out for similar

problems in their small OSs. The utilities of the OS are the main culprit in the attacks that have happened in wired systems and it is important to have utilities with strong security. For example, some products attempt to improve the security of email systems [Kno04].

Device security

If a portable device is lost or stolen user authentication can prevent somebody from gaining access to confidential information. Possibilities include PINs, pass-phrases, and biometrics. Some portable devices already have fingerprint readers [Rie00]. In networks that only authenticate the device instead of the user, losing a device is more serious than in networks that authenticate users or roles.

Communications security

An obvious problem of wireless communications is that they are very easy to intercept. This implies that some form of encryption is a must for the confidentiality of messages. The available approaches depend on the standard used. Cellular networks use GSM, while WLANs use two standard protocols:

- IEEE 802.11a (Wi-Fi) can reach up to 1800 feet (550 meters). Devices connect to Access Points (APs), that have unique identifiers (BSS ID). APs are basically transceivers that take the radio signals to the WLAN switch, which performs all the required network management. WLAN switches support 802.11 at layer 2 and IP traffic at layer 3. The wireless network has a SSID (Service Set Identifier). It is also possible to set up Peer-to-Peer (P2P) networks.
- Bluetooth. A protocol for short-range (up to 100 meters) wireless networks. Bluetooth devices are typically structured into ad-hoc networks.

We describe these protocols in more detail and discuss their security below.

IEEE 802.11 Wireless LAN Standard

It is the most widely used communications protocol for wireless LANs. The protocol resides in the physical and data link layers of the OSI model. It defines functions and specifications for the physical and MAC (Medium Access) layers. The MAC layer covers three functional areas: Reliable data delivery, access control, and security. The protocol defines different building blocks such as BSS (Basic Service Set) and ESS (Extended Service Set). Each ESS consists of one or more BSS. Stations in a BSS compete for access to the shared wireless medium. Most ad hoc network routing protocols are designed and tested on top of the IEEE 802.11 protocol. Figure 2 shows the scope of the IEEE 802.11 standard in reference to the layers of the OSI model. It shows how the data link layer is actually divided into the MAC and LLC (Logical Link Layer). The latter is responsible for providing the upper layers with three types of services, which are:

1. Unacknowledged connectionless service:
 - a. No flow and error control support.
 - b. No guarantee of data delivery.
2. Connection-mode service:
 - a. Logical connection is set up between two users.
 - b. Flow and error control are provided.

3. Acknowledged connectionless service:
 - a. This service is a cross between previous two.
 - b. Datagrams are acknowledged.
 - c. No prior logical set up required.

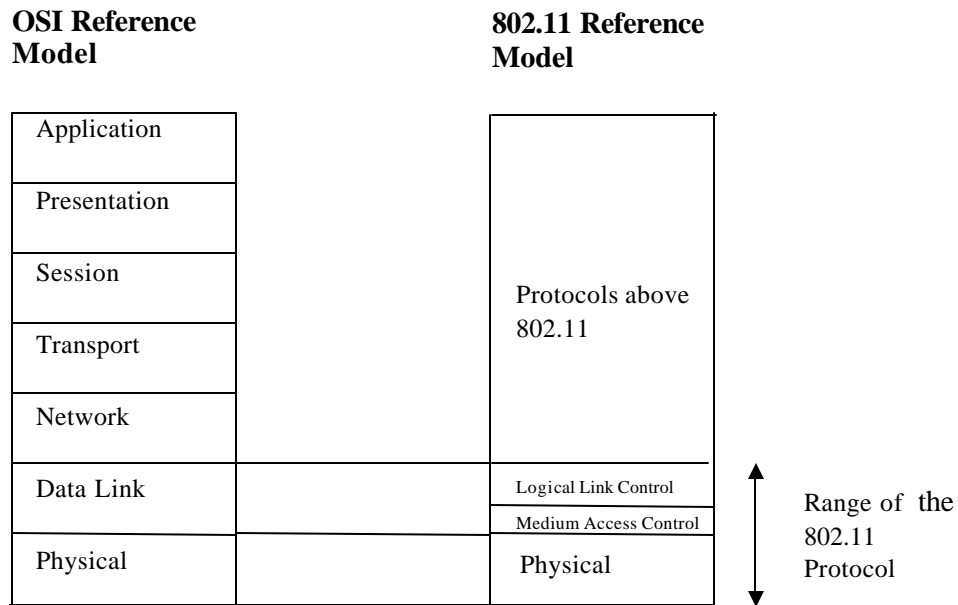


Figure 2 Correspondence of the IEEE 802.11 layers to the layers of the OSI reference model.

802.11 uses Wired Equivalent Privacy (WEP). WEP provides device or access point authentication as well as message secrecy through a variant of the RC4 cryptographic algorithm. The implementation of this algorithm has been shown to be flawed [isa]. Access to the wireless network is controlled using a static key.

WEP is being replaced by Wi-Fi Protected Access (WPA). WPA supports the AES encryption algorithm, provides effective key distribution, and can interact with RADIUS or LDAP servers. Authentication is based on the 802.1X and the Extensible Authentication protocol (EAP) and requires the use of an authentication server. An alternative (or complement) is using SSL VPNs [Ave04]. Other specialized products detect unauthorized access points and users.

WLAN switches apply security controls, including authentication (a comparison of some of them is in [Che04]). Authentication can be provided locally or by connecting to a RADIUS or LDAP server.

Because the RSA algorithm is rather inefficient in its use of key length, *elliptic curve cryptography* (ECC) algorithms have been proposed [cer]. For example, an elliptic curve algorithm with a key length of 150 bits takes 3.8×10 to the 10^{th} MIPS-years to be broken by brute force, while the RSA with a key length of 512 takes only 3×10 to the 4^{th} years. However, this approach requires that all ECC users agree on a common set of parameters, otherwise the extra information needed effectively extends the key [Fer99].

Bluetooth

Bluetooth is a wireless communications protocol, originated by Ericsson, that quickly was adopted by many companies. It is intended to work in a close proximity environment, such as homes, offices, classrooms, hospitals, airports, etc. Connections are established using designated master and slave nodes.

Bluetooth uses application profiles for different devices, synchronous connection-oriented (SCO) for data, and asynchronous connectionless (ACL) links for voice, which are multiplexed on the same RF link. Frequency-hopping spread spectrum with a high 1600 hops/sec rate is used to reduce interference, and provide low power, low cost radio communications. It operates in the ISM band at 2.45 GHz with a transmission power of 1 to 100 mW, a range of 10 to 100 meters, a maximum bit rate of 1 Mbps, and an effective data transfer rate of 721 Kbps.

Bluetooth provides authentication and message 128-bit encryption using hierarchical keys. Devices can be discoverable or invisible. In discovery mode a device is visible to any other device within range, which can make it vulnerable to attacks from those devices.

GSM

GSM implements authentication based on a cryptographic challenge response protocol. For encryption it uses the A5 algorithm. It also includes Anonymity using temporary identifiers. Details of GSM security can be found in [hac02].

Gateway server security

Gateways are devices that control the flow of traffic into or out of a network. Although definitions differ, for this context a gateway can be thought of as a device that passes packets between subnets (real or virtual), and performs operations above OSI layer 3 (session, flow control, protocol conversion, and application specific). Gateways can also be the source of vulnerabilities [Juu01a]. Gateways are important to wireless networks and mobile wireless devices for several reasons:

- Wireless networks do not afford the same physical levels of security as wired networks. Due to resource constraints, mobile wireless devices are themselves often less secure than wired devices. *Wireless security gateways* can protect a wired network from untrusted wireless hosts. Unlike firewalls, for which hosts are either “inside the firewall” or “outside the firewall,” the distinction between inside and outside is somewhat blurred for mobile wireless devices. A company’s

trusted workers may need “inside” kinds of connectivity while using wireless devices. Conversely, visitors may need “outside” kinds of connectivity while connecting to the company’s wired network through an access point inside the corporate firewall. Wireless security gateways address these issues by performing two-way authentication and limiting access privileges on a per-device basis.

- Mobile wireless devices often have limited resources that cannot support the same protocols as wired devices. They may therefore use resource-sharing protocols which must be translated in a protocol gateway to enable interaction with standard Internet protocol services. For example, a *WAP gateway* translates protocols in the WAP suite, including WML (HTML), WML Script (CGI), WBMP (BMP), WBXML (XML), WSP (HTTP), WTP (TCP/IP), WTLS (SSL), and WDP (UDP). These kinds of translation pose security issues both because the wireless protocols are often less secure than the corresponding wired protocols, and because, in translation, encrypted data takes an unencrypted form inside the gateway.
- Wireless devices often exist on subnets that do not support the full Internet addressing scheme. For example devices may use IP addresses reserved for local access only, or otherwise not support all of the capabilities needed for WAN access. Gateways can provide a bridge between these local subnets and a broader WAN, (i.e., Internet). Common SOHO wireless switches provide NAT to allow local devices to all access the Internet using a single IP address. Similarly, a Personal Mobile Gateway with WAN connectivity like GSM/GPRS can allow Bluetooth, 802.11, or 802.15 devices on a PAN to have full Internet connectivity. The fact that devices behind a NAT gateway do not have unique IP addresses has implications for some security strategies (i.e., IPSEC-AH [Sta99]).
- Mobile wireless devices may be involved in various sorts of commerce, such as M-commerce and downloading multimedia streams with digital rights. Depending on how you look at it, where conflicting privacy and ownership interests come into play, “trusted gateways” can bridge the no man’s land, or encapsulate the overlap as a trusted third party. This space is an area of active research and is, as yet, not as well defined as the other gateway functions. Issues here are closely tied to digital rights management. See for example the Shibboleth project [shi].

The Internet was built on “transparency” and the “end-to-end principle”. Roughly stated, transparency “refers to the original Internet concept of a single universal logical addressing scheme, and the mechanisms by which packets may flow from source to destination essentially unaltered.” [rfc2775] The end-to-end principle holds that functions of data transmission other than transport, such as data integrity and security, are best left to the transmission endpoints, themselves. This allows applications to be ignorant of the transport mechanisms, and transport systems to be ignorant of the data being transported. Gateways, by their nature, violate one or both of these principles.

Gateway deployment strategies

At the basic network level, gateways are viewed as servers or end-systems. But gateways create their own overlay networks and may be involved in ISO level 2 and level 3 routing. The use of gateways can greatly complicate problems of network management. Their deployment should be carefully considered within a comprehensive network coverage and security strategy.

The main reason for using a wireless security gateway is that intruders may gain access through an insecure wireless access point and mount an attack on the internal network. As indicated earlier, 802.11b, Bluetooth, and WAP are all potentially insecure. Access points with stronger security are possible using Cisco or 802.1x protocols. Typically, a large site or campus, will need many access points for good coverage. The cost of numerous high-end access points and the problem of managing them, especially when they are not all from the same vendor, is a major concern. A common strategy is to use simple (“thin”) access points and put one or more security gateways between all wireless access points and the wired network. Then even if anyone can establish a connection to an access point, they will be challenged at the gateway. The gateway might use IPSEC, VPN, and/or LDAP encryption and authentication. Cisco also has LEAP which they are pushing as PEAP for a standard. There are several products that include SSL VPNs and gateways [Ave04].

Several strategies are available to ensure that access points connect only to a gateway. Access points could be physically wired on a separate subnet where gateways provide the only bridge to the main wired network. Over a large area, the need to maintain two wired networks, one for access points, may be impractical. Multiple smaller networks can be used, each with its own gateway. Multiple gateways can share a common, central management tool – like CA or HP OpenView. They may also be arranged in master/slave relationships, i.e., for configuration and fail-over. Another alternative is to use access points that VPN tunnel to a single gateway, using the regular wired network as the transport medium.

Gateways can grant different users different levels of trust. The easiest way to set this up is to differentiate users by their IP address, and grant different levels of service (i.e., bandwidth) and different kinds of access (i.e., specific protocols like ftp and http, and specific destination hosts) using ISO level 2 (IP address) and level 3 (protocol type) filtering. Access classes can be grouped by role, and identified by predefined ranges of IP address.

By grouping IP addresses, the IP address can also be used to distinguish between wired and wireless clients, e.g., to deliver content appropriate to small or large screens, or to put a WAP service behind the gateway or firewall. Other parameters, such as signal strength will be harder to expose.

Basing access privilege on statically-assigned IP addresses makes systems difficult to manage and upgrade. Imagine having to change thousands of statically assigned IP addresses to accommodate a new access policy. A better approach uses DHCP and MAC addresses. The DHCP servers are configured with fixed MAC to IP address mappings

which are much easier to maintain and can be upgraded as needed. The dynamically assigned IP address serves as a kind of token to gain specific levels of access. To hide these IP addresses from snoops, use one of the newer (or evolving) standards for level 2 encryption in the client and access point (i.e., Tunnelled Transport Layer Security).

Gateway services

Any system granting access to clients should include a separate method for authenticating the user. MAC addresses can be spoofed. The gateway may provide its own authentication service, or act as a proxy for a remote authentication service available elsewhere on the network. Various authentication services can serve this function, including RADIUS and Windows Active Directory. Using an underlying operating system's authentication may allow the user to log in to both the network and a machine with a single sign-in. 802.1x proposes this approach. A "captive portal" directs every http request from a not yet authenticated user to the authentication service (and blocks all other types of requests).

There are situations where wireless clients are not capable of performing a standard authentication behavior. Sensors on a shop floor or in a wireless automotive network might be examples. In these cases, with very limited privileges, statically assigned access may be justified. But the security implications must be carefully considered and strong encryption should be used.

Roaming is another issue that gateways can address. Roaming users may move out of range of their current access point and into range of several alternative access points. Handover delays may affect streaming applications like VoIP and video. Secure access points might require the user to be re-authenticated, while gateways offer other options. The 802.11 Fast Roaming Study Group and 802.21 working group are looking for standard ways to address roaming, as is a partnership among Proxim, Avaya, and Motorola.

WAP devices use WTLS instead of SSL, due to the assumed WAP client's resource constraints. The basic WAP configuration involves a WAP gateway that translates between the various WAP protocols and the corresponding Internet protocols. The WAP gateway translates between WTLS and SSL by decrypting the message as it comes in and then re-encrypting it in the other protocol before passing it on. Decrypting the message in the WAP gateway is only one of many WTLS vulnerabilities [Juu01b, Saa99]. Better security can be achieved by using an encryption protocol in the layer above WTLS/SSL that works directly between the client and server endpoints.

PKI-based encryption is the logical candidate for end-to-end encryption, e.g., for M-Commerce applications. But PKI is resource intensive. The special processing could be handled by a SIM/WIM smartcard, but smartcards add cost to small devices. Research is currently underway to use a remote server to perform the heavy processing part of the RSA/ECC algorithm implementation, while still holding all key parameters in secrecy by the client [eti].

Resource overhead for even basic internet connectivity can be an issue for very small devices, such as those imagined for wearable and ubiquitous computing. A special class of gateway, called personal mobile gateway (PMG), has WAN capability (e.g., GSM/GPRS) and shares it with other little devices with PAN connectivity (i.e., Bluetooth, 802.11, 802.15). The delegation can be general, or specific to the type of applications needed (SMS, voice, digital photos, video, etc.) Security issues at this level are beyond the scope of this discussion.

Government wireless installations are required to meet the NIST FIPS 140-2 standard for cryptographic modules [nis]. RADIUS does not meet this standard. For such applications a FIPS 140-2 compliant gateway and corresponding authentication server software must be used. The physical vulnerability of gateways in unattended locations may also need to be addressed. By encasing the gateway's circuitry in a special hardened plastic security potting resin, any attempt at physical tampering will be easily recognized.

In any discussion of security and gateways the limitations of gateways must be emphasized. Gateways form part of a perimeter defense for wired networks. They do not solve the vulnerability of any network to insiders with malicious intent. In addition, while the gateway strategy addresses the threat to the network from malicious wireless devices, it doesn't protect wireless devices from malicious access points.

The future

There is serious concern about the vulnerabilities of wireless systems. The easy access to the medium by attackers is a negative aspect compounded by the design errors in the early protocols [Arb03, Juu01b, Saa99]. The US Department of Defense recently issued Directive 8100.2 that requires encrypting all information sent in their networks according to the rules of the Federal Information Processing (FIP) standard [dod]. The provision also calls for antivirus software. It is interesting to observe that their concern is again mostly about transmission and they don't seem to be worried about the other aspects of security.

On the other side, Ashley et al. arrived to the conclusion that WAP provides excellent security [Ash01]. It is true that Wi-Fi is becoming more secure and Bluetooth appears reasonably secure but they (and WAP) cover only some of the security layers. A basic security principle indicates that security is an all-layer problem, one or more secure layers is not enough [Fer04a]. While some of the layers are still insecure, it is not possible to have true security.

Third generation systems will have voice quality that is comparable to public switched telephone networks. Voice over IP will bring its own set of security problems. The new systems will have also higher data rates, symmetrical and asymmetrical data transmission rates, support for both packet and circuit switched data services, adaptive interface to the Internet to reflect common asymmetry between inbound and outbound traffic, more efficient use of available spectrum, support for wide variety of mobile equipment, and more flexibility. All of these are the potential sources of new security problems.

As mentioned earlier, web services are not delivered directly to portable devices but transformed in the gateway. Most of the use of web services for mobile systems is now between servers [Gra04]. However, this situation is changing and predictions indicate that web services in cell phones will be arriving soon. In fact, Nokia just announced a Service-Oriented Architecture for smart mobile phones [Yua04]. Security will be an important issue for this generation of smart and complex devices.

Security patterns is a promising area to help designers build secure systems [Fer04b]. Several patterns have been found in the Bluetooth architecture, including versions of the Broker, Layers, Lookup, and Bridge patterns [Gam95]. However, no security patterns for wireless systems have been found yet. This is an area to explore.

References

- [a5] Cracking the A5 algorithm, <http://jya.com/crack-a5.htm>
- [Alf00] M. Alforque, "Enhancing the Security of a Windows CE Device," Microsoft Developers Network, <http://msdn.microsoft.com/library/enus/dnce30/html/winsecurity.asp>
- [Arb03] W. Arbaugh, "Wireless security is different", *Computer*, IEEE, August 2003, 99-102.
- [Ash01] P. Ashley, H. Hinton, and M. Vandenwauver, "Wired versus wireless security: The Internet, WAP, and iMode for e-commerce", *Procs. 17th Ann. Comp. Sec. Applications Conference*, 2001.
- [Ave04] Aventail, "Practical solutions for securing your wireless network", White paper, 2004. <http://www.aventail.com>
- [cer] Certicom, <http://www.certicom.com>
- [Cha01] D.W. Chadwick, "An X509 role-based PMI", 2001, http://www.permis.org/files/article1_chadwick.pdf
- [Che04] B. Chee and O. Rist, "The Wi-Fi security challenge", *InfoWorld*, May 17, 2004. <http://www.infoworld.com>
- [Cox04] J. Cox, "Vendors offer tools to control, secure WLANs", *Network World*, 6/7/04, <http://www.nwfusion.com>
- [dod] <http://www.dtic.mil/whs/directives/corres/html/81002.htm>
- [Dog02] A. Dogac and A. Tumer, "Issues in mobile electronic commerce", *Journal of Database Management*, Jan.-March 2002, 36-42.

[eti] http://www.eti.hku.hk/eti/web/p_s_wiress.html

[Far01] R. Farrow, "Wireless security: A contradiction in terms?", *Network Magazine*, Dec. 5, 2001. Also in : <http://www.networkmagazine.com/article/NMG20011203S0008>

[Fer99] A.D.Fernandes, "Elliptic-Curve Cryptography", *Dr. Dobbs Journal*, December 1999, 56-63.

[Fer02] E.B.Fernandez, "Web services security", chapter in *Web Services Business Strategies and Architectures*, P. Fletcher and M. Waterhouse (Eds.), Expert Press, UK, 290-302.

[Fer04a] E. B. Fernandez, M. Thomsen, and M.H. Fernandez, "Comparing the security architectures of Sun ONE and Microsoft .NET", in "*Information security policies and actions in modern integrated systems*", book by C. Bellettini and M.G.Fugini (Eds.), 2004.

[Fer04b] E.B.Fernandez, "A methodology for secure software design", *Procs. of the 2004 Int. Conf. on Software Engineering Research and Practice (SERP'04)*,

[Fol01] S. Foley and R. Dumigan, "Are handheld viruses a significant threat?", *Comm. of the ACM*, vol. 44, No 1, January 2000, 105-107.

[Gam95] E. Gamma et al., *Design patterns –Elements of reusable object-oriented software*, Addison-Wesley 1995.

[Gho01] A.K.Ghosh and T.M. Swaminatha, "Software security and privacy risks in mobile e-commerce", *Comm. of the ACM*, vol. 44, No 2, February 2001, 51-57.

[Gra04] P. Gralla, "Mobile web services: Theory vs. reality", <http://SearchWebServices.com>, 10 February, 2004.

[hac02] "The GSM security technical whitepaper for 2002", http://www.hackcanada.com/blackcrawl/cell/gsm/gsm_security.html

[ibm] IBM Corp., AlphaWorks Web Services Toolkit, <http://www.alphaworks.ibm.com/tech/webservicestoolkit>

[IM02a] "Security in a Web Services World: A Proposed Architecture and Roadmap: A Joint White Paper from IBM Corporation and Microsoft Corporation," Microsoft Developers Network, 7 April 2002, <http://msdn.microsoft.com/library/en-us/dnwssecur/html/securitywhitepaper.asp>

[ipv] IPv6 home page, <http://www.ipv6.org>

- [isa] “Security of the WEP algorithm”, <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
- [Iss] Internet Security Systems, X-Force Database, <http://xforce.iss.net/xforce>
- [jav] “Java APIs for Bluetooth Wireless Technology (JSR-82) Specification”, <http://jcp.org/en/jsr/detail?id=82>
- [Juu01a] N.C.Juul and N. Jorgensen, “Security limitations in the WAP architecture”, Workshop at OOPSLA 2001, <http://www.dnainland.fi/oopsla/wap.pdf>
- [Juu01b] N.C.Juul and N.Jorgensen, “WAP may stumble over the gateway (security in WAP-based mobile commerce)”, <http://www.dat.ruc.dk/~nielsj/research/papers/wap-ssgr.pdf>
- [Mit] The Mitre Corporation, Common Vulnerabilities and Exposures List, <http://cve.mitre.org>
- [nis] <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- [rfc2775] <http://www.faqs.org/rfcs/rfc2775.html>
- [Rie00] M.J.Riezenman, “Cellular security: better, but foes still lurk”, *IEEE Spectrum*, June 2000, 39-42.
- [Rob99] S. Robinson, “Researchers crack code in cell phones”, *The New York Times*, Dec. 7, 1999.
- [Saa99] M.-J.Saarinen, “Attacks against the WAP WTLS protocol”, *Proceedings of Communications and Multimedia Security '99*, <http://www.jyu.fi/~mjso/wtls.pdf>
- [shi] <http://shibboleth.internet2.edu/>
- [Sta99] W. Stallings, *Cryptography and network security: Principles and practice* (2nd Edition), Prentice-Hall, 1999.
- [Sta02] W. Stallings, *Wireless Communications and Networks*, Prentice-Hall, 2002.
- [Var00] U. Varshney, R.J.Vetter, and R. Kalakota, “Mobile commerce: A new frontier”, *Computer*, IEEE, October 2000, 32-38.
- [Vau04] S.M.Vaughan-Nichols, “Wireless middleware: Glue for the mobile infrastructure”, *Computer*, IEEE, May 2004, 18-20.

[Yua02a] M.J.Yuan, "Access web services from wireless devices", *Java World*, August 2002, <http://www.javaworld.com/javaworld/jw-08-2002/jw-0823-wireless.html>

[Yua02b] M. J. Yuan, "Securing wireless J2ME: Security challenges and solutions for mobile commerce applications," *IBM DeveloperWorks*, (1 June 2002), IBM. <http://www-106.ibm.com/developerworks/wireless/library/wi-secj2me.html>

[Yua04] M.J.Yuan, "SOA and web services go mobile, Nokia-style", July 6, 2004, <http://www.sys-con.com/story/?storyid=45531&DE=1>