COMPAQ
White Paper

December 2001

Prepared by:
Access Business Group
Compaq Computer Corporation

Contents

Wireless Security

Abstract: People and corporations are using wireless technologies at astonishing rates to take advantage of the benefits of wireless-enabled productivity to gain and maintain a competitive edge. Market researcher Cahners In-Stat estimates that 6.2 million wireless devices will be shipped worldwide this year (2001), and double that in two years.

This paper looks at the pieces of the "pipe" of access from the device to the corporate firewall in an attempt to bring an awareness to both the user and the corporate IT manager as to where the security vulnerabilities lie and what can be done to improve security. Many of the vulnerabilities can be alleviated easily by implementing policies for users and adding security layers to the pipe. To put the subject of wireless security into context, the paper is organized as follows: First, securing wireless systems in general is discussed, then securing each point along the access pipe is discussed.

Notice

Wireless Security
White Paper prepared by Access Business Group

First Edition (December 2001)
Document Number 161Z-1201A-WWEN

Introduction

Wireless networks connect computers in offices or homes to other computers, or to devices such as printers, by using radio or infrared signals instead of cables and jacks. Since wireless networks dispense with cables, users connected to wireless computer networks (or wirelessly connected to computer networks) can roam around with the machines they use to gain access to such networks. This ability to function in "untethered" mode is a great convenience.

Users and corporations are using wireless technologies at astonishing rates to take advantage of the benefits of wireless-enabled productivity to gain and maintain a competitive edge. Market researcher Cahners In-Stat estimates that 6.2 million wireless devices will be shipped worldwide this year (2001), and double that in two years.[1]

The pervasiveness of sending and receiving data via wireless networks to the Internet and corporate intranets has presented users of access devices and corporations with new concerns about vulnerability to security breaches. Wireless access technologies have been called "one of the newest and potentially most dangerous security holes in U.S. business."[2] Experts estimate that most of the wireless networks in operation today have no security whatsoever. This is so in part because many users are not aware of specific security vulnerabilities or don't understand the magnitude of potential loss and, therefore, do not put the appropriate measures in place. This paper will look at the pieces of the "pipe" of access from the device to the corporate firewall in an attempt to bring an awareness to both the user and the corporate IT manager as to where the security vulnerabilities lie and what can be done to improve security. Many of the vulnerabilities can be alleviated easily by implementing policies for users and adding security layers to the pipe.

To put the subject of wireless security into context, the paper is organized as follows: First, securing wireless systems in general is discussed, then securing each point along the access pipe is discussed.

A significant part of wireless network security overlaps with security designed for wired networks. This is particularly so where firewalls, virtual private networks, and corporate servers are concerned. Please see the Compaq Technical Guide titled "Safe Computing and E-Business: Protecting the Enterprise to Assure E-Business Success" (http://activeanswers.compaq.com/ActiveAnswers/Render/1,1027,1317-6-100-225-1,00.html February, 2000) for important detail on best practices and established technologies for managing corporate network security.

For complete wireless and mobile security solutions, please contact Compaq Global Services at http://www.compaq.com/services/index_infrastructure.html.

Security in General

It is important to realize from the outset that no single measure may be adequate to address security in wirelessly enabled networks. Both wired and wireless security implementations must be constantly evaluated and improved as people find new ways to gain unauthorized access to sensitive data. To plan a security business model, key elements of security must be considered as each point of access is examined.

[1] Lee Gomes, "Often unguarded wireless networks can be eavesdroppers' gold mine" (Wall Street Journal Online, April 27, 2001).
[2] Gomes.

Essential Elements of Security

The essential elements of security as it applies to wireless networks are:

- Privacy — assuring that only people who have permission to do so can view information and transactions. Privacy is preserved through a process that authorizes identified persons to see protected information and engage in transactions. Encryption is an important tool for preserving privacy.
- Authentication — the process of verifying that the parties to an electronic transaction, as well as persons seeking access to digital information, are who they say they are. Authentication verifies identity and is supported by digital signatures.
- Integrity — a process by which a security system seeks to preserve stored information and information that circulates in messages. Assuring that such information remains intact and unchanged (except by authorized parties) preserves its integrity.
- Non-repudiation -- a process that proves an entity took a course of action, and only that entity could have taken the course of action. This quality makes electronic transactions legally binding. Non-repudiation is supported by digital signatures and trusted timestamps.
- System Management -- all security technology must be managed. This means setting it up to be easy to use, while making sure it cannot be abused or used to hide criminal activity.

These essential elements should be the result of any combination of security implementations from the device across the “pipe” to the corporate firewall and servers.

The next section describes aspects of securing the “pipe”, the security issues that may arise with wireless networks at critical junctures along the pipe, and measures that can be taken to address those issues.

Security and the Pipe

A pipe is a conduit through which something flows. A wireless mobile business solution should include an end-to end security model for enabling secure data access by creating a secure pipe from the mobile user’s access device (the client) across various networks (air, broadband, dial-up) to the point where access is gained to the corporate network. From here the pipe leads through the corporate firewall to corporate applications. The end-to-end security model should also provide management mechanisms for performance and security.

Key elements of the pipe are the following:

1. Security at the mobile access device level or client **(Device Security)**
2. Security in wireless connectivity technologies **(Connectivity Technologies)**
   - WLAN, WPAN, WWAN, broadband, dial-up, RAS
3. Security at the point of access to the wired transmission path **(Access Point)**
   - WLAN hubs, telecommunications companies
4. Security at the corporate firewall and servers **(Corporate Access)**
5. Security of the corporate data inside the firewall **(Corporate Data)**

– (This aspect of security is not covered in this paper, since securing data from unauthorized access behind the firewall is not a wireless security concern, but a wired one.)

Figure 1 illustrates the pipe.

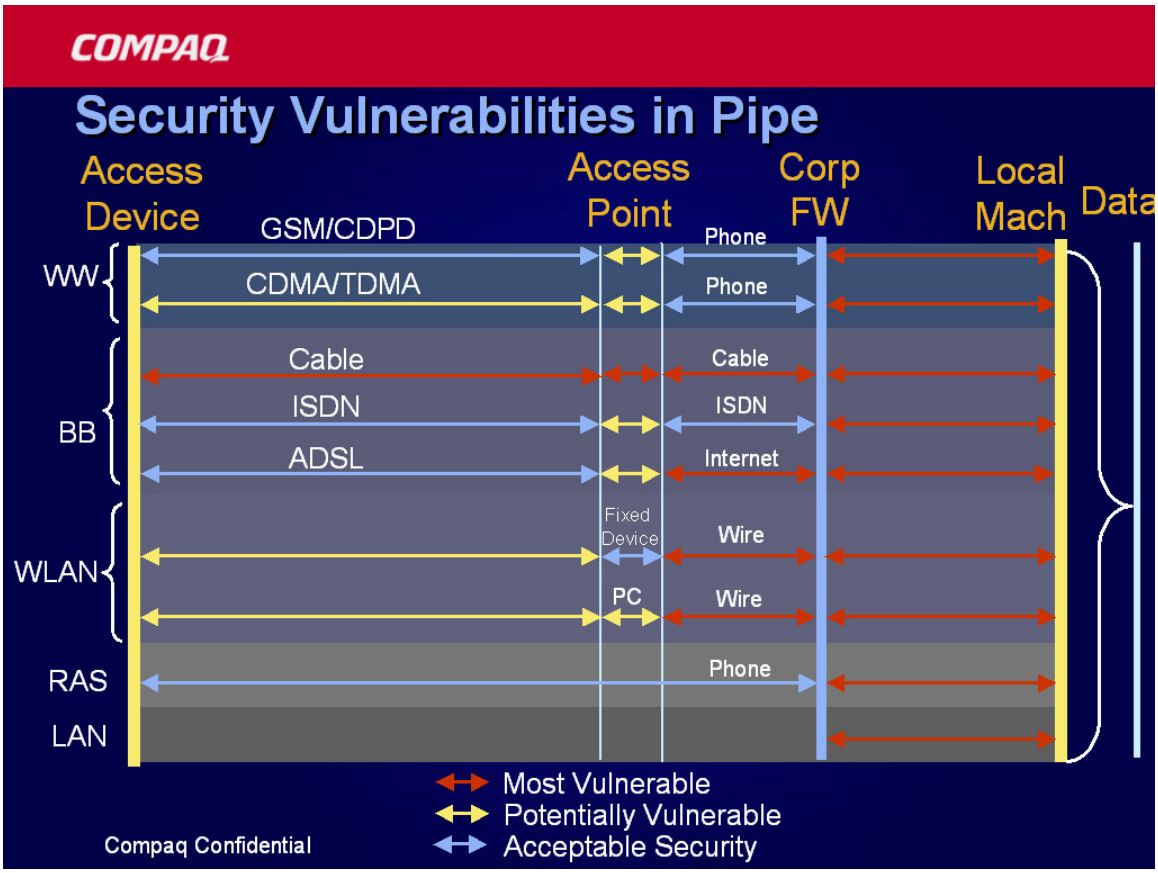


Figure 1: The Network Pipe

The vertical yellow lines in Figure 1 represent the pivotal points of data transfer. The horizontal lines represent data traveling from one place to the next either wired or wirelessly. The entire pipe must be considered in planning security models. Each element of the pipe, along with the security problems and solutions associated with it, is discussed in the next five subsections.

Device Security

Despite the growing popularity of handheld PCs, PDAs, and cellular telephones, the truly ubiquitous mobile computing device in the United States is still the notebook computer (in Europe it is the mobile telephone). Notebook computers are used for online connectivity, Internet surfing, organization of information such as contact lists and tasks, storage of vast amounts of data, hosting of numerous client applications, and creation of primary content such as documents, e-mail messages, and spreadsheets.

Moreover, workers are using notebook computers more and more as desktop machines while in the office, then taking them home at the end of the day to continue working. Because of their usefulness, companies deploy millions of notebook computers to their employees. Companies treat the devices as critical resources by defining usage and security policies and by instituting measures to protect the hardware and the data that the devices hold. For information on Compaq notebook computers, see http://www.compaq.com/showroom/notebooks.html.

Mobile devices such as handheld computers, PDAs, and cellular telephones have traditionally been used for a subset of the tasks that notebook computers address. However, handheld computers and PDAs are beginning to be used by workers who are on the road or present in client offices to access many types of applications in real time. For information on Compaq handheld devices, see http://www.compaq.com/showroom/handhelds.html.

Device security concerns increase significantly where handheld mobile devices are concerned, because they are often owned and managed by individuals, as opposed to the companies they work for. Most companies, therefore, do not have in place the usage and security policies appropriate for such devices. The difficulty in managing individually owned handheld mobile devices and their rate of propagation causes them to pose a unique security threat.

The following subsections describe security problems specific to mobile access devices, the first link in the pipe on the client side, and possible solutions to those problems.

Usage in Public

Mobile devices employing a cellular service are used more frequently in public places (hotel lobbies, airplanes, and the like) than desktop devices, which makes it harder to prevent strangers from peering over the shoulders of mobile device users. If permitted to observe the user's computing activity for any period of time, the curious stranger may be able to read and record (or remember) sensitive information. This violates the security tenet of privacy.

The exposure to prying eyes that mobile devices incur has no technological solution. The only way for users to minimize this exposure is to exercise vigilance and common sense. Being selective in where and when they use their devices and reasonably alert in monitoring their surroundings are precautions that mobile device users can and should take. The smaller screens of handheld devices reduce this type of security risk.

Loss and Theft

Mobile access devices are more susceptible to loss and theft than larger stationary devices. If a device is lost or stolen, unauthorized persons may view confidential information stored on the device. They may also use the device to gain access to public and private networks in order to tamper with or steal information. The security tenets of privacy, authentication, and integrity are all potentially breached in such a situation.

Vulnerability to Hacking

Connecting to the Internet or to corporate networks by radio waves leaves data vulnerable to hacking because of the open-to-all nature of the transmission medium (air). Minimizing vulnerability to hackers can be accomplished when both access devices and portals themselves are protected by their own firewalls. Often firewalls are not installed due to the small storage size of some handheld access devices, and lack of enforcement of security and usage polices relating to such devices.

Available Device-specific Security Measures

Many security measures are available for mobile access devices. Some of these are outlined in the subsections below. For various reasons they are often not fully implemented.

Passwords

Mobile devices, especially handhelds, have small user interfaces and keypads, leading many users to choose simpler passwords. For example, keypads that associate multiple letters with each key require repeated presses to type certain letters. Users often choose passwords that use the first letter typed by a given key. This practice substantially reduces the number of possible passwords. Also, mobile device users often cache their passwords on the devices in order to automate connections to servers.

A further consideration is whether or not to permit single sign-on from the mobile device. While doing so is more convenient given the cumbersome nature of password entry on mobile devices, it raises the level of risk that intruders may penetrate the network.

The straightforward solution is to endure the trade-off in convenience and make password protection more robust by avoiding weak passwords, refraining from password caching, and avoiding single sign-on.

Smart Cards

Smart cards offer a partial solution to the problem of securing data transmissions to and from mobile devices. The smart card is a tamper-resistant piece of hardware on which passwords, private keys, digital certificates, and cryptographic algorithms can be stored. Simply keeping the smart card separate from the device, in a wallet for example, adds a level of security to the device in the event of theft. Moreover, a person attacking a smart card must not only possess the card but also have sophisticated tools and expertise.

There are two main types of smart cards: contact and contactless. The contact smart card consists of a plastic card with gold-plated contacts embedded in the plastic. These contacts are connected to an integrated circuit sandwiched between layers of plastic inside the card. The contactless smart card typically connects to the smart card reader through an internal antenna.

Smart cards are easy to use, and the newer, more complex ones offer relatively strong encryption. A smart card is most effective when paired with a personal identification number (PIN). Whereas a stolen smart card can be used just like a stolen password, the association with a PIN presents thieves with a further barrier to obtaining access to a wireless network, even with the card.

Smart card readers offer different levels of security. The basic smart card reader reads the smart card in conjunction with a PIN. The enhanced smart card reader also reads the card in conjunction with a PIN, but in addition does not allow the PIN back out to the serial port, thus preventing PIN information from being intercepted via the serial port. The enhanced reader typically can perform its own protocol and cryptological processing, unlike smart cards that do not perform such processing themselves.

A concern with smart cards (and certain other encryption devices) is their vulnerability to power analysis attacks if they fall into the wrong hands. Such attacks involve device power measurements and their analysis while the smart card is in operation. Mathematical analysis of the differences in power consumption during different operations of the smart card can make possible the decryption of the smart card's information. Other types of attacks include replay and micro-probing. Such vulnerability notwithstanding, smart cards are an important tool in improving authentication on mobile devices, making them less likely to be misused if they fall into the hands of strangers.

Biometric Technologies

Biometric devices use physical traits such as fingerprint, iris, face, and voice to identify an individual. Fingerprints are an accurate trait to use for computer-based identification, and solutions developed for fingerprints are currently the most cost-effective and easy to use.

Compaq partners with Identix, a leader in biometric identification technology, to produce Compaq Fingerprint Identification Technology (FIT) for the commercial market. A tiny camera in the Fingerprint Identification Reader captures an image of the fingerprint of a device's legitimate user. The information then goes through some complex algorithms to convert the image into a unique "map" of minutiae points (unique data points that describe the fingerprint). This map of minutiae points (not the actual fingerprint) is then encrypted and stored within the network. The user places a registered finger on the reader attached to his or her PC in order to log on to the network. The information is then extracted and compared to information on the computer. If the comparison is a sufficient match, the user is allowed to log in.

Where mobile devices are concerned, Compaq FIT is currently available only for Compaq *Armada* and *Evo* notebook computers. For more information on Compaq FIT,

see http://www.compaq.com/products/notebooks/security.html or http://www.compaq.com/products/quickspecs/10103_div/10103_div.HTML.

Multi-factor Authentication

Multi-factor authentication is one of the best ways to improve security at the device level. Corporations sensitive to security breaches are moving quickly to at least two-factor authentication – choosing two types of authentication as requirements for accessing data. Such security requires the user to authenticate him one's self in more than one way in order to improve security. The means of authentication may include the following:

- Something the user knows (password)
- Something the user has (tokens -- smart card)
- Who the user is (biometrics -- fingerprint identification)

Requiring at least two types of authentication is dramatically more secure than requiring only one.

File System Security

While desktop operating systems such as Windows 2000 offer an encrypted file system, this is not yet common on mobile platforms. If the data on a mobile device is sensitive, it is worth investigating security software that can encrypt such information. FileCrypto for PocketPC from F-Secure Corporation of Helsinki, Finland provides such encryption for mobile devices.

Key features of F-Secure FileCrypto for PocketPC are the following:

- Encrypts documents in selected folders on the fly
- Strong real-time encryption with 128-bit Blowfish
- Allows creation of user-specified encrypted folders
- Supports removable media
- Automatic installation through a host PC to the PDA device at next ActiveSync
- Minimum length and character set of pass-phrase can be defined
- ActiveSync protected by the same pass-phrase
- Automatic encryption at power-off
- Key recovery ensures that corporate data is not lost if the pass-phrase is forgotten

Compaq iPAQ Pocket PC's ship with F-Secure today. For more information on F-Secure products see http://www.fsecure.com.

SecurID

SecurID is a two-factor authentication technique that combines a user's PIN with the operations of an external authenticator device to produce a secure user login. The SecurID external authenticator may be implemented as a key fob, smart card, or software token. It generates a unique code every sixty seconds in strict synchronicity with the server. The user's login password combines the SecurID code with his or her PIN.

RSA Security did not develop a Pocket PC client, but instead incorporated SecurID into the EZOS WAP micro-browser called EzWAP.[3]

Device-Specific Firewalls

Industry best practices dictate the use of a device-mounted firewall when connecting to the Internet, especially through a wireless VPN connection. Software-based firewalls are available from third-party providers. One such product is Black Ice, available from Network ICE Corporation. Notwithstanding the protection offered, such firewalls are often not incorporated into the access device; either because of the small hard drives of handheld devices or through lack of a corporate security policy (or enforcement of same) requiring such use.

Connectivity Technologies

The second key juncture in the pipe, after wireless access devices, is a range of wireless connectivity technologies. These technologies provide the infrastructure, standards, and protocols that permit information to travel wirelessly between mobile clients and the wired lines that provide access to corporate servers. Different connection technologies are used at different times, depending on the availability and efficiency of each connection type at any given time.

- Internal users use a wireless connection at work to stay connected while they roam. For example, they can send and receive e-mail while attending meetings in conference rooms. Generally, wireless local area networks (WLANs) will facilitate this usage.

[3] EzWAP 2.0 is a platform-independent WAP micro-browser enabling a variety of computing systems…to access the mobile Internet environment. (http://www.ezos.com)

- Individual users can connect between various personal devices wherever they are, such as from a cell phone to a handheld to a desktop computer without cables to synchronize data or gain access to a wireless connection. Wireless personal area networks (WPANs) facilitate such connections between devices.
- External users increasingly want corporate connectivity anywhere at any time. For example, they can send and receive e-mail, access corporate data, the Internet and intranets, while sitting in airport lounges, traveling in a cab or sitting in front of a customer. Wireless local area networks (WLANs) and wireless wide area networks (WWANs) facilitate this usage.

A brief description of these connectivity technologies follows and detailed papers that exist on each technology are referenced below. The following three subsections comment briefly on the three types of wireless networks and provide an illustration of each type.

Wireless Local-area Networks

A wireless local-area network (WLAN) is a type of LAN that uses high-frequency radio waves rather than wires to transmit data among its nodes. It is a flexible data communication system implemented as an extension or alternative to a wired LAN within a building or campus. Users of a WLAN can enjoy connectivity to the network without having to plug cables into Ethernet jacks in every office and conference room.

Figure 2 illustrates a WLAN.

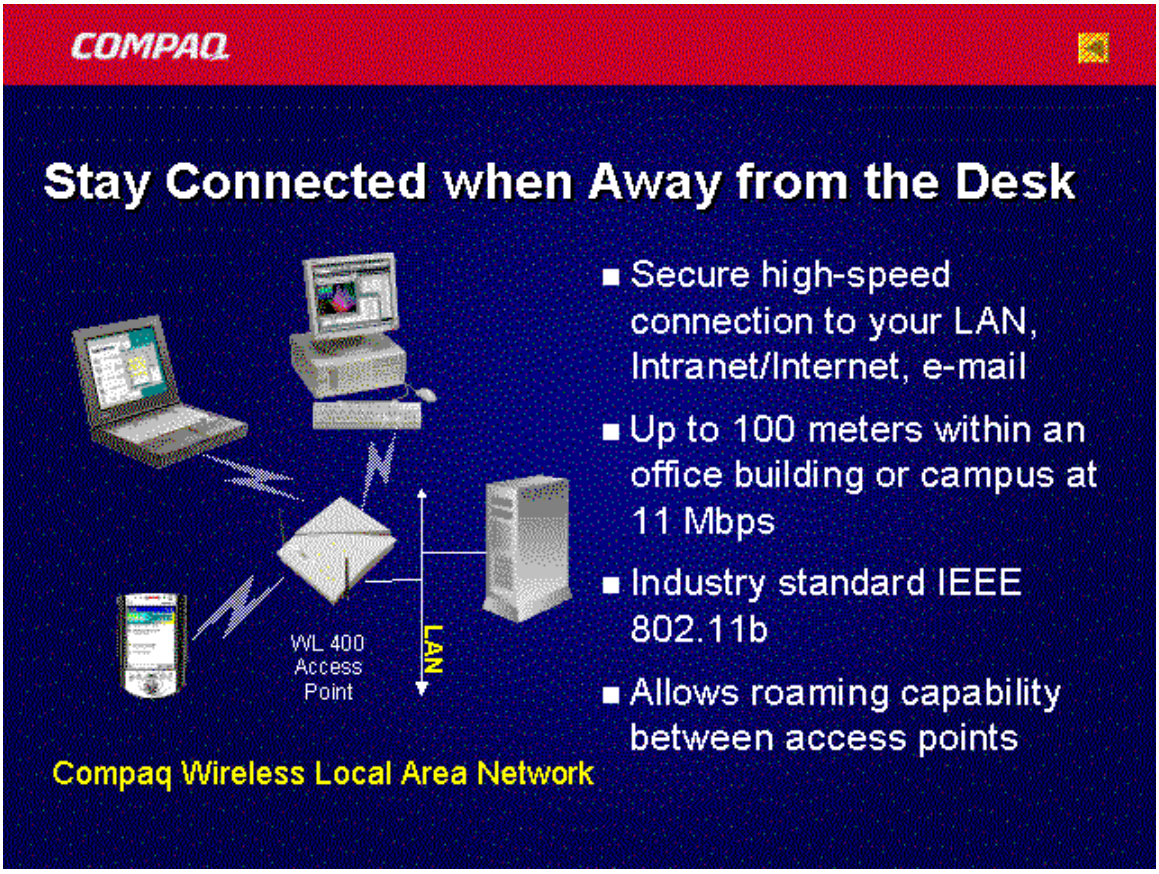


Figure 2: Wireless Local-area Network

Wireless Personal-area Networks

Wireless personal-area networks (WPANs) can use Bluetooth, a radio frequency (RF) specification for point-to-multipoint voice and data transfer. They can also use infrared technology. A WPAN permits personal devices such as handheld PCs to connect wirelessly to peripheral devices such as printers or other personal devices.

Figure 3 illustrates a WPAN.

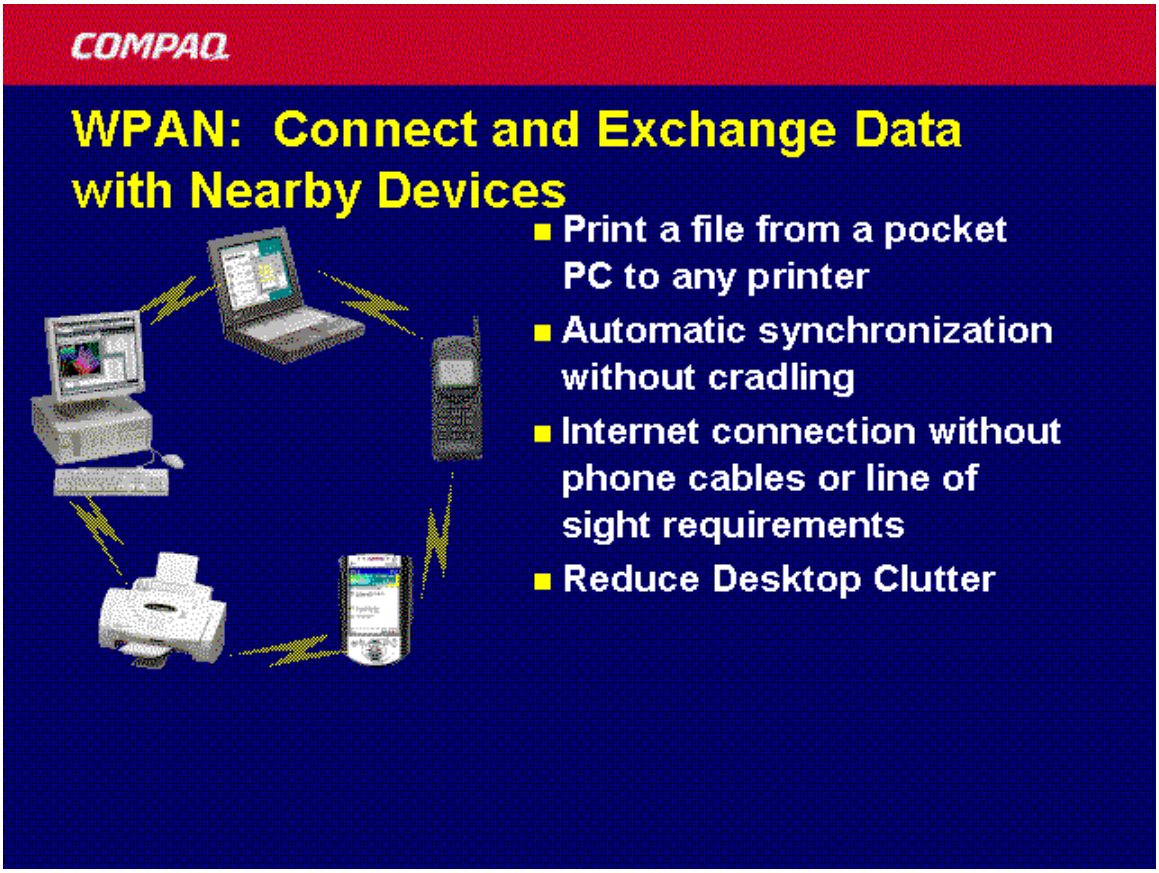


Figure 3: Wireless Personal-area Network

Wireless Wide-area Networks

Historically, wireless wide-area networks (WWANs) have been used to support voice transmission for mobile telephones. WWANs use one of three digital wireless telephone technologies: GSM, CDMA, and TDMA.

The Global System for Mobile communication (GSM), developed in Europe, is the most widely used of the three digital wireless telephone technologies. Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) were developed in the United States and are widely used there. GSM is a TDMA technology. The official names for CDMA and TDMA are IS-95 and IS-136, respectively. Japan's NT DoCoMo uses I-mode technology in its market.

Compaq provides turnkey solutions: clients with enabling technologies, airtime provided by carriers, area network coverage, and optimized features. Compaq WWANs using CDPD and GSM technologies are available now. WWAN via CDPD, for example, provides packet-switched connections to the Internet, Internet e-mail, enterprise intranet and corporate e-mail. Compaq offers an optimized MS Exchange e-mail solution with InfoWave. Nationwide (U.S.) coverage is available. Wireless WAN via GSM, as another example, provides circuit-switched connection to the Internet, Internet e-mail or enterprise modem pool. As with CDPD, an optimized MS Exchange solution is provided with InfoWave.

Figure 4 illustrates a WWAN.

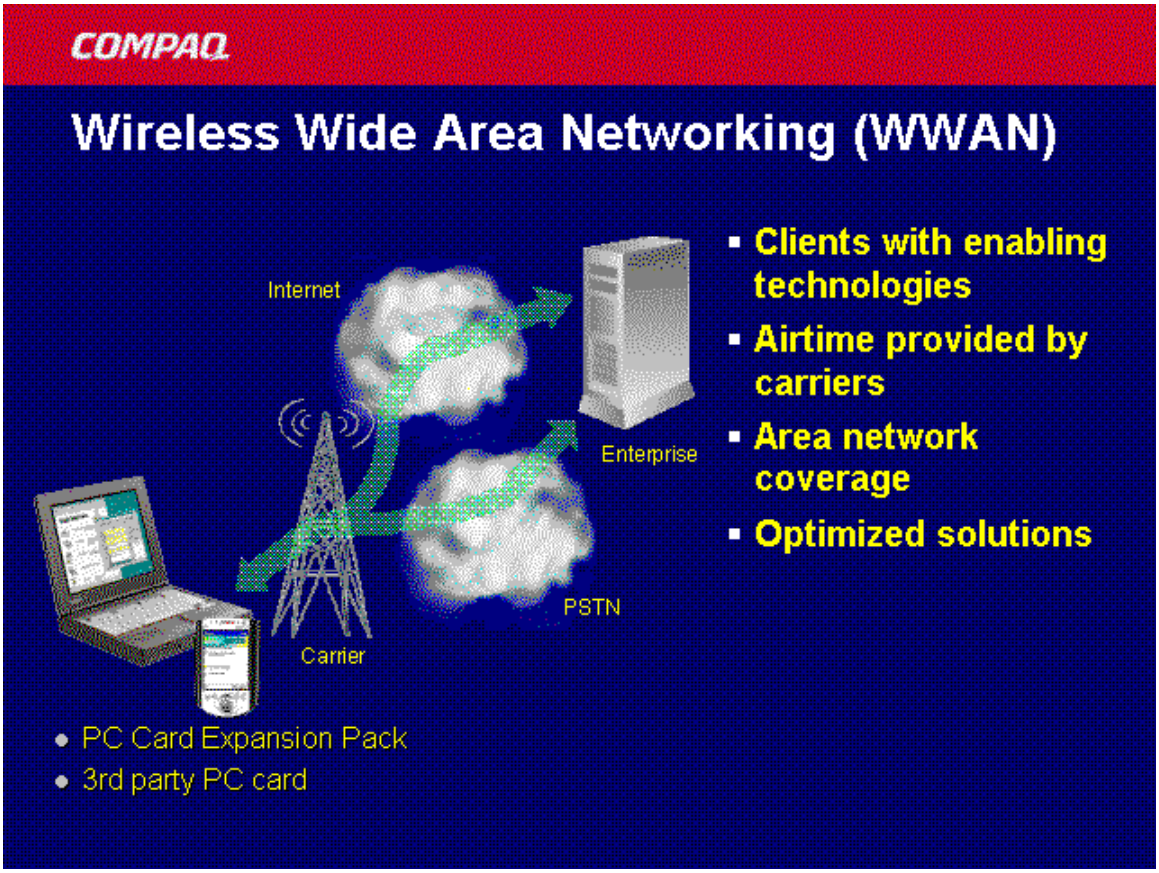


Figure 4: Wireless Wide-area Network

Whether it is a WLAN, a WPAN, or a WWAN, a wireless network uses radio waves to transmit information. Radio waves travel over an unshielded medium, which is air. Because all wireless networks operate on the same frequency and with the same equipment, and because it is difficult to control how far radio waves travel, hackers can access the data as it is transmitted through the air when the data is not properly encrypted. Such eavesdropping and possible theft of information violates privacy. Gaining access to corporate passwords, logging on to servers, and taking over a website (impersonation, which violates authentication and possibly integrity), or even shutting the network down (sabotage, which overwhelms all the elements of security) are vulnerabilities exposed with data traveling over radio waves.

The discussion that follows concentrates on the segment of the network pipe in which information must travel over public highways and suffer the potential for exposure. Transmission via one of several connectivity technologies from the access device to the carrier (or WWAN access point) is dependent to a certain degree on the type of network used in WWAN connectivity.

GSM and CDPD networks are the most secure due to the heavier underlying encryption native to the network technology; that is, the airtime provider supplies the user with encryption of signals, resulting in an inherently more secure system than those where such encryption is not provided. Conversely, CDMA/TDMA networks are slightly less secure since they include only digital encoding without encryption.

The following sub-sections discuss these vulnerabilities in more detail and suggest solutions to mitigate risk associated with WWAN connectivity.

For simplification, the next section is titled "Eavesdropping," but with the understanding that, as commented above, eavesdropping can lead to or imply a broad range of mischief for a wireless network. This simplification is helpful in describing the two primary technologies that help forestall eavesdropping and its destructive ramifications. Those technologies are encryption and tunneling. Encryption and tunneling effectively "hide" information as it travels by making it unreadable, and thus unusable, to casual or not-so-casual observers. It is necessary at this juncture, however, to be clear that technologies used to secure one piece of the pipe may need to be deployed across multiple points in the pipe. For example, it may be necessary to load software on the device and on the server, as well, to better secure the connectivity channel.

Eavesdropping

To prevent eavesdropping and its concomitant ills, the information that travels over a wireless network must be rendered unreadable or invisible to observers. Two key technologies make such information unreadable or invisible. Those technologies are encryption and tunneling. These technologies include Public Key Infrastructure (PKI) and Virtual Private Networks (VPNs). Popular PKI vendors like Baltimore Technologies, Inc. and Entrust do not have PKI support for access devices. Smaller companies have point solutions to specific applications that run on the various operating systems.

Public Key Infrastructure

Most approaches to achieving security for the wireless exchange of information over networks involve the use of public key cryptography, also known as public key encryption. The framework on which public key cryptography is built is known as a public key infrastructure (PKI).

Figure 5 illustrates the basics of public key cryptography. In Figure 5 the originator encrypts the data using a public key, so that the data is scrambled when it is sent over the network. The recipient receives the scrambled data and decrypts it using the recipient's private key.

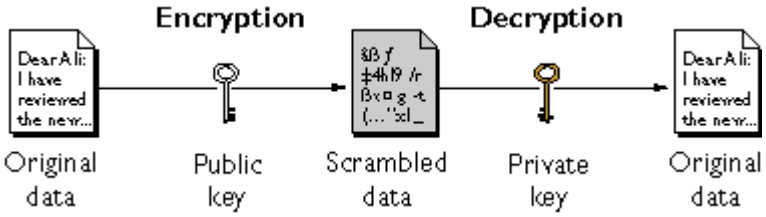


Figure 5: Basics of Public Key Cryptography

Core elements of a PKI are:

- Asymmetric keys
- Digital certificates
- Digital signatures

The following paragraphs describe and illustrate these elements.

A "key" is a numeric value of variable length that an encryption algorithm uses to convert unencrypted text into encrypted text. Public key cryptography uses a pair of asymmetric keys for encryption and decryption. An "asymmetric" key system uses a different key for encryption and decryption. (By contrast, a "symmetric" key system uses the same key for encryption and decryption.)

Each pair of keys in an asymmetric key system consists of a public key and a private key. The public key is distributed widely. The private key is always kept secret. Data encrypted with the public key can be decrypted only with the private key. Conversely, data encrypted with the private key can be decrypted only with the public key. Most asymmetric encryption uses the RSA algorithm developed in 1977 by Rivest, Shamir, and Adleman, or derivatives of that algorithm.

Figure 6 illustrates symmetric and asymmetric keys.

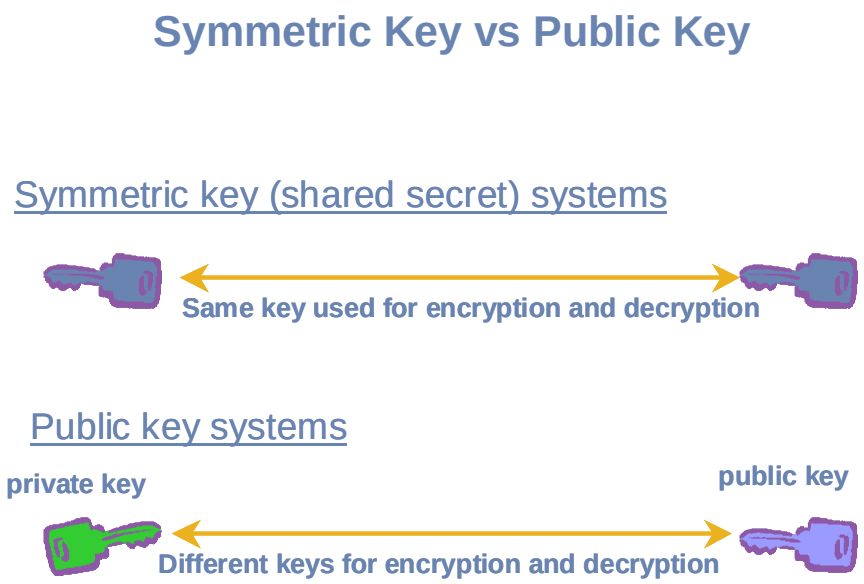


Figure 6: Symmetric and Asymmetric Keys

Digital Certificates

Digital certificates are electronic files that can be used as unique identifiers for people and resources over networks. A digital certificate binds a user's identity to a public key, thus establishing trust. Digital certificates can also be used to help secure confidential communication between two parties. A certificate typically includes the following information relating to its owner and to the Certificate Authority (CA) that issued it:

- The name of the holder and other uniquely identifying detail such as the URL of the Web server using the certificate and the holder's e-mail address
- The holder's public key, which can be used to encrypt sensitive information for the certificate holder
- The name of the Certification Authority (CA) that issued the certificate
- A serial number
- The validity period (or lifetime) of the certificate (a start and end date)

When the issuing CA creates the certificate, it digitally signs the information on the certificate. The CA's signature on the certificate is like a tamper-detection seal; any tampering with the contents is easily detected.

Figure 7 illustrates digital certificates.

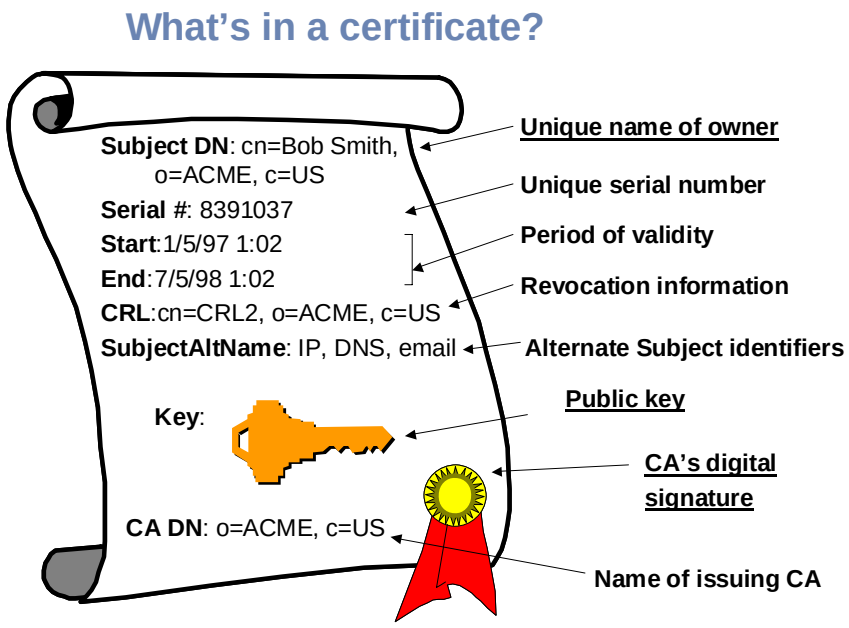


Figure 7: Digital Certificates

Digital Signatures

Digital signatures are intended to be the legal equivalent of handwritten signatures. The signer generates a "hash value" or "digital fingerprint" of the document or message to be signed.[4] The hash value is unique to the document or message. The hash value is then converted into a digital signature by the user's private key. The digital signature is sent to the recipient for verification. The recipient verifies the digital signature by generating a hash value of the original message, decrypting the original hash value in the digital signature with the public key, then comparing the original hash value with the recipient's hash value. If the two hash values match, the signature is deemed authentic. Another way to verify a digital signature is through a Certification Authority (CA). A CA is usually a trusted third party able to verify that the private key used to generate the digital signature belongs to the signer, and that the public key is indeed associated with the digitally signed document or message.

Figure 8 illustrates digital signatures. In Figure 8 the original data is hashed using a one-way algorithm. The hash is encrypted using the originator's private key. The original data along with the digital signature is sent over the network to the recipient, who decrypts the digital signature using the public key. The recipient compares the one-way hash from the digital signature to the one-way hash from the original data. If the two match, the data has not been compromised and the identity of the originator is confirmed.

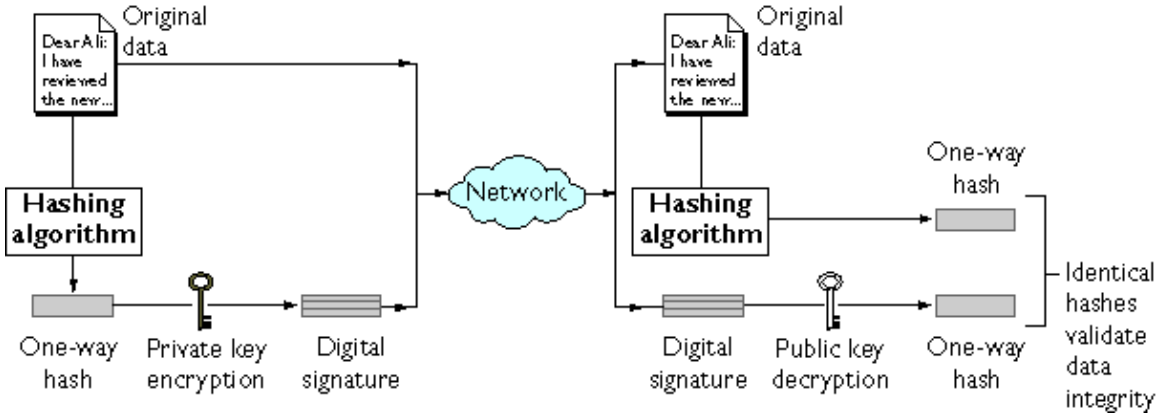


Figure 8: Digital Signatures

[4] Hashing is the process of transforming a string of characters into a fixed-length numeric value or "key" that represents the original string.

Virtual Private Networks

Virtual Private Networks (VPNs), also known as "tunnels" and commonly used over the Internet for wired networks, can keep a wireless network hidden from prying eyes. Security experts recommend that companies use an additional authentication system such as a VPN before allowing data to cross from a wireless network to an intranet or other corporate system. VPNs have the following characteristics:

- User Authentication. The VPN must verify the user's identity and restrict VPN access to authorized users. The VPN must also provide audit and accounting records to show who accessed what information and when.
- Address Management. The VPN must assign a client's address on the private network and assure that addresses are kept private.
- Data Encryption. The VPN must encrypt information transmitted on the public network.
- Key Management. The VPN must generate and refresh encryption keys for the client and server.
- Multiprotocol Support. The VPN must handle common protocols used on the public network.

Figure 9 (next page) illustrates a VPN used in conjunction with firewalls.

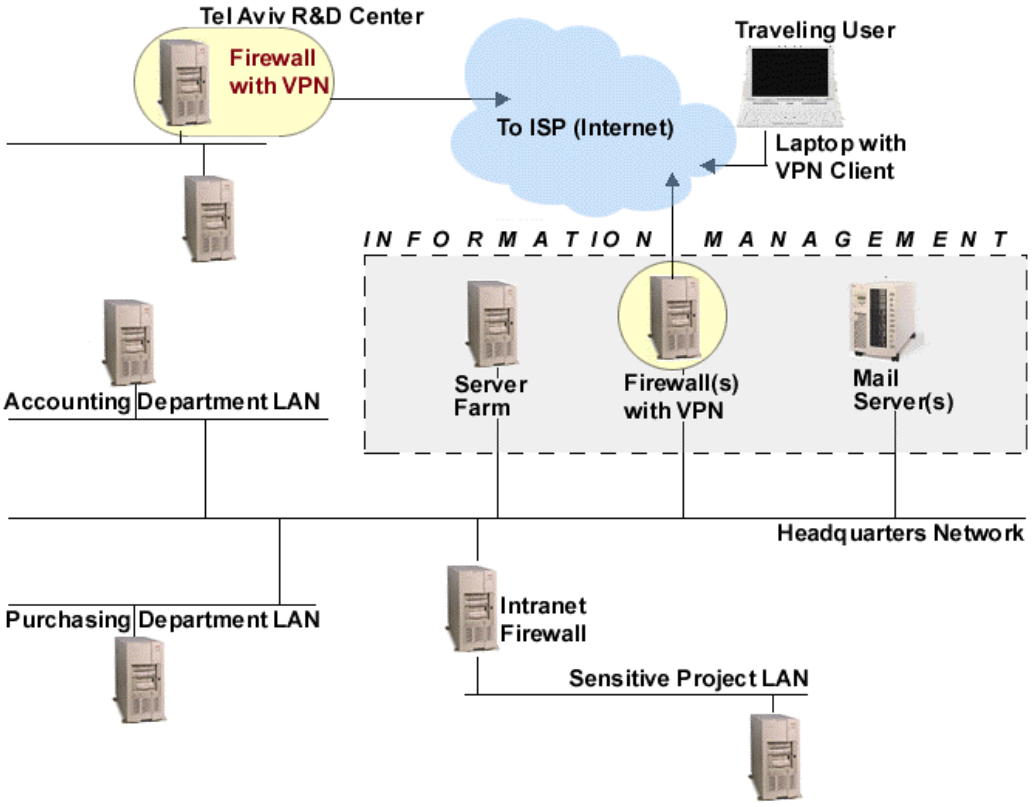


Figure 9: Virtual Private Network (VPN)

Several VPN protocols are available. They include the Point-to-Point Tunneling Protocol (PPTP) from Microsoft, the Layer Two Tunneling Protocol (L2TP), the Layer Two Forwarding protocol (L2F) from Cisco Systems, and the Internet Protocol Security protocol (IPSec).

The PPTP protocol lets corporations extend their corporate network through private "tunnels" over the public Internet. In effect, the corporation converts a wide area network (the Internet) into a single large local area network. By making secure use of the public network, the corporation no longer has to lease its own lines for wide-area communication. This is the definition of a virtual private network.

L2TP is an extension of PPTP that is used by an internet service provider (ISP) to enable VPNs over the Internet. L2TP merges the best features of PPTP and L2F. Its two main components are the L2TP Access Concentrator (LAC), a device that physically terminates a call, and the L2TP Network Server (LNS), a device that terminates and possibly authenticates the Point-to-Point Protocol (PPP) stream.

L2F is a technology that, according to developer Cisco Systems, will enhance the ability of service providers to build Virtual Private Dial-Up Networks (VPDNs). Cisco has submitted L2F to the Internet Engineering Task Force (IETF) for approval as a standard. Northern Telecom Inc. and Shiva Corporation have announced their support for L2F.

IPSec is a developing standard for security that operates at the network or packet-processing layer of network communication. By contrast, earlier security schemes inserted security at the application layer of the communications model. IPSec offers strong encryption, but degrades the performance of the computer it runs on because of the high CPU overhead associated with the encryption and decryption algorithms. The greater speeds of new generations of processors will reduce the toll that IPSec takes on machine performance.

IPSec is especially well suited for implementing VPNs and for remote user access through dial-up connection to private networks. IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

With IPSec, the sending and receiving devices share a secret key, also known as a symmetric key. These keys can be exchanged via public key cryptography. This exchange takes place through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), (now also known as Internet Key Exchange – IKE), which allows the receiver to use public and private keys and authenticate the sender with digital certificates. IPSec also has the advantage that security arrangements can be handled without requiring changes to the computers of individual users. Cisco Systems has been prominent in proposing IPSec as a standard, and includes IPSec support in its network routers.

VPN software is often never turned on. A further difficulty is that many mobile devices simply do not support VPNs at this time. Additionally, VPNs were not designed with wireless networks in mind, and are therefore more prone to failure due to unreliability and low bandwidth. Both the mobile device and the server must support a common VPN protocol. Frequently, the mobile device does not have VPN client software installed. If it does have such software, the device is still likely to be limited in the VPN protocols that it supports.

The following VPN products, however, are available from third parties for the Compaq *iPAQ* Pocket PC:

movianVPN by Certicom:

- Based on IPSec
- Uses Certicom ECC for IKE
- Connects to back-end VPN products from: Alcatel, Check Point, Cisco, Intel, Nortel, Radguard, Symantec

Check Point VPN Client:

- In development
- Not based on IPSec
- Will support only Check Point VPN products

VGate by V-One:

- Works only with V-One VPN appliance gateway
- Supports many strong, third-party authentication schemes

SecureTunnel by Traxit:

- Provides VPN functionality by performing packet switching at remote hosting center
- Designed to provide direct, end-to-end connectivity and authentication (mobile client directly to application server)

Security Specific to WWAN Carrier Technologies

All digitized mobile telephone and wireless packet data networks use some form of encryption. GSM uses a smart card to protect its keys. The smart card contains both the international mobile subscriber identity (IMSI) and the subscriber identification key. When the user makes a connection with a mobile base station, a session key is negotiated and all transmissions, both voice and data are encrypted.

GSM documents specify the rough functional characteristics of its protocols, including the secure encryption of transmitted digital messages. However, apart from the protocols, details of the algorithms are kept secret. Most security specialists will argue that secrecy is not an effective approach, since only the close scrutiny of a large set of experts can ensure that there are no obvious weaknesses in the technique. Nonetheless, GSM contains three secret algorithms that are given only to vendors with established need-to-know, such as carriers and handset manufacturers. The three algorithms are:

- A3: Authentication algorithm
- A5: Ciphering/Deciphering algorithm (currently A5/1,A5/2, provides over-the-air voice privacy)
- A8: Cipher Key Generator (essentially a one-way function), and session key generation

The smart card contains A3, A5 and A8; the base station is equipped with A5 encryption, and is connected to an authentication center using A3 and A8 algorithms to authenticate the mobile participant and generate a session key.

Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) use the Cellular Message Encryption Algorithm (CMEA) specified by the Telecommunications Industry Association (TIA).

The encryption techniques used by WWANs have proven to be effective but not infallible. Both GSM and CMEA algorithms have reportedly been cracked. However, their effectiveness lies in making prohibitively expensive the monitoring and interception of random or bulk transmissions over a WWAN.

Besides encryption, the IS-95 standard of CDMA uses a transmission technique called "spread spectrum" that was developed by the military with a view to making interception more difficult. Spread spectrum deliberately varies the frequency of the transmitted signal, resulting in a much greater bandwidth than the signal would otherwise have. (Conventional wireless signals do not change frequency except for small, rapid fluctuations that occur as a result of modulation.)

Wireless Access Protocol

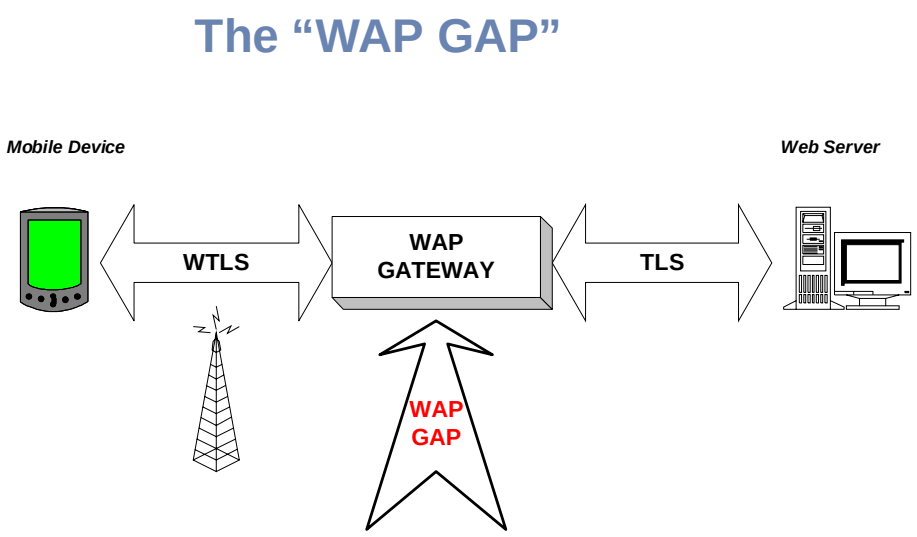
The Wireless Access Protocol (WAP) is designed specifically for the mobile environment. Wireless Transport Layer Security (WTLS) is the security level for WAP applications. WTLS is based on Transport Layer Security (TLS), a security layer used on the Internet and equivalent to Secure Socket Layer (SSL)

WTLS was developed to solve problems specific to mobile network devices, including their limited processing power, memory capacity, and bandwidth. WTLS is designed to provide adequate authentication, data integrity, and privacy protection. WTLS offers three classes of authentication:

- Class 1 authentication is anonymous, meaning neither party to the link is authenticated;
- Class 2 authentication authenticates only the server;
- Class 3 authentication requires both client and server to authenticate themselves by means of a signed digital certificate.

Version 1.1 of WAP used WTLS server certificates to authenticate a WTLS server to a WTLS client, and to provide a basis for generating a key with which to encrypt a session between the server and client. WAP 1.2 adds support for WTLS client certificates, which authenticate a WTLS client to a WTLS server. WAP 1.2 also adds a function that allows a WAP client to digitally sign a transaction, thus providing for non-repudiation. WAP 2.0 was released in June 2001 and adds support for Wireless Public Key Infrastructure (WPKI) by describing methods for the secure download of digital certificates. WAP 2.0 is based on standard Internet TLS, and designed so as to eliminate the "WAP gap." (See below for more on WAP 2.0.)

Figure 10 illustrates the wireless access protocol.



- Security protocol must be translated from WAP “WTLS” to standard Internet “TLS”
- Data is unencrypted for a brief period of time

Figure 10: Wireless Access Protocol (WAP)

WAP does not provide end-to-end encryption between the wireless client and the application server. The wireless transport layer security (WTLS) on which WAP is based encrypts information only as it travels from the wireless client to the WAP gateway. The WAP gateway often re-encrypts the information, using Secure Socket Layer (SSL), as it continues to the application server. However, this does not change the fact that there is not end-to-end encryption in the information’s trip from wireless client device to application server. This characteristic is often called the "WAP gap."

The newest ratified version of WAP is 2.0 (June 2001).WAP 2.0 is radically different from previous versions and represents a strong flow of convergence with the IETF and W3C. The WAP gateway is optional and WAP has now adopted the Internet standards TCP, HTTP, and TLS with wireless-specific profiles. Similarly, WML is effectively a profile of XHTML. Much work has been done, as well, on end-to-end security.

It may be some time, however, before implementations of WAP 2.0 appear on the market. Such implementations may appear first on the PocketPC rather than on telephones, since all they would require is a software change rather than new hardware.

Infowave

Infowave provides an encrypted end-to-end security model from the mobile user through the wireless data network and Internet to the corporate server. Infowave is a gateway solution that controls all traffic to and from wireless users. Infowave requires that a single configurable port be opened in the firewall and set up as follows:

- The port must allow only User Datagram Protocol (UDP) traffic.[5]
- The port must admit traffic only to the machine that is running the Wireless Business Engine (the Wireless Business Engine is the only software listening to the port). In addition, incoming packets must be encrypted with the server's public key, and must contain a valid logon packet with NTLM logon credentials to be processed. Otherwise, the packets are discarded.

The Infowave security model is based on the following elements:

- Authentication — proves the identity of the user
- Authorization — determines what the user is allowed to do
- Encryption — assures the privacy of transmissions
- Data Integrity — assures that the information has not been altered
- Non-Repudiation — prohibits the user from denying the transmission after the fact

Figure 11 illustrates the Infowave security flow.

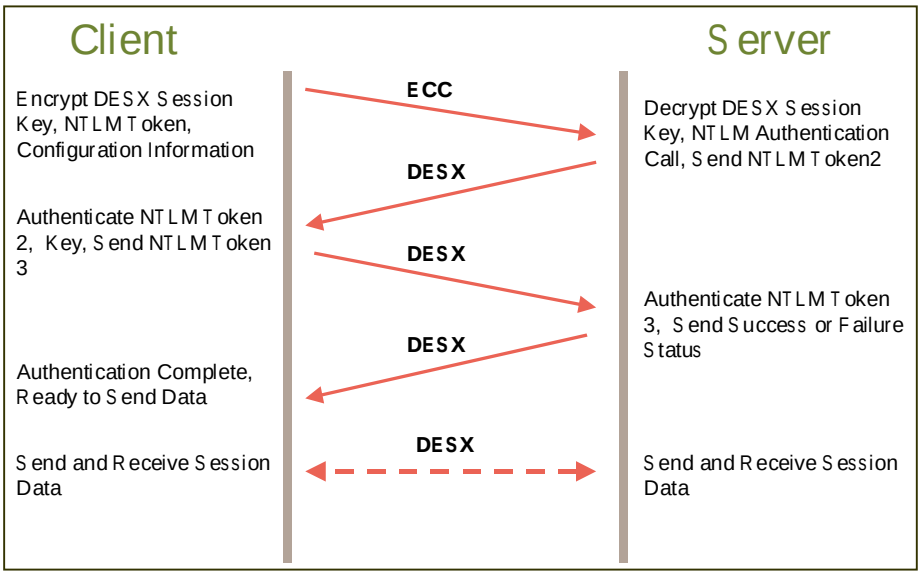


Figure 11: Infowave Security Flow

More detail on each element of the security model follows.

[5] UDP is an alternative to Transmission Control Protocol -- TCP, and does not provide the service of dividing messages into packets and reassembling them at the receiving end. It is useful when very small messages are exchanged.

Authentication

Infowave uses NTLM challenge/response authentication. Infowave sends no user information over the link other than the encrypted NTLM token.

Authorization

Once it has authenticated the user, the Infowave server determines what resources the user is authorized and licensed to access. The Infowave server grants or denies access to the Exchange mailbox, for example. It also sends an authentication request back to the Infowave client software. The authentication request is processed using the NTLM credentials cached on the client device.

Encryption

For asymmetric encryption, Infowave uses the Elliptic Curve Cryptography (ECC) encryption algorithm from the Certicom *Security Builder* toolkit. The Infowave server maintains a private and public key pair that is generated on installation. Infowave clients know the server's public key and use it to perform the symmetric key exchange for all data transfers. ECC is significantly faster than the standard RSA encryption algorithms, and is well suited to mobile devices. The Wireless Business Engine is designed to support a number of different encryption algorithm combinations. The Certicom ECC/DESX combination is the currently implemented algorithm pair, but an arbitrary number of algorithms can be supported.

For symmetric encryption, Infowave uses DESX, a strengthened variant of the Data Encryption Standard (DES) method of encryption that originated at IBM in 1977. Infowave randomly generates a DESX symmetric key pair on each client every time the client logs on. This key pair is used to encrypt session traffic.

Data Integrity

Infowave compresses, encrypts, and delivers data using its wireless protocol. The Infowave server analyzes the data to determine the best compression algorithm. The combination of encryption and compression ensures that data cannot be altered during transmission. If data shows signs of having been altered, the receiving side of the exchange does not accept it.

Non-repudiation

If the Infowave client software falls into unfriendly hands, the attacker can gain knowledge only of the Infowave server public key and the number of the access port. The breach of this information is not critical. Without knowing the user's Windows NT domain name, user ID, and password, the attacker can get no further than the Infowave server. The Windows NT domain name is combined with other information and encrypted with the server's public key, which keeps an attacker from impersonating a valid user.

Possible Security Problem

There may be a significant problem with Infowave security in that the client is not able to validate the public key of the Infowave server (WBE). This implies vulnerability to a "man-in-the-middle" attack where a client request is intercepted and then relayed to the server. The man in the middle can then eavesdrop on the entire transmission.

According to Infowave, this design decision was made to support server public key download at the cost of the potential security hole mentioned above. At the time the design was implemented, the client-side libraries did not support signing of the server public key. This will be changed in future versions.

Infowave further notes that the engineering effort required to perform the above attack is prohibitive. It is not sufficient to just capture data and analyze it. The attacker would need to build working versions of both the IStack transport layer (Infowave proprietary) and the WBE authentication and session protocols (also Infowave proprietary) in order to carry out this attack. One of these servers would be required for each client impersonated, since the WBE server only supports one connection for each IP address. This attack would also require re-configuring the client to communicate with the attacking server, or alternatively impersonating this IP address on the Internet.

Access Points

The third key juncture in the pipe, after mobile access devices and wireless connectivity technologies, consists of access points.

The term “access point” is used to describe the point in the pipe where the data leaves the connectivity medium (WLAN and WWAN) and reaches the point at which data travels to the wired lines or Internet. In the case of WLANs, for example, the Access Point is a piece of hardware, a hub, which transfers data to the local area network via an Ethernet connection in an office building. In the case of WWANs, the Access Point is the telecommunications company which routes the data to the phone line which enters the corporate data network and/or the Internet.

WLAN Access Points

Certain weaknesses of Wired Equivalent Privacy (WEP)[6] will be remedied in IEEE extensions to the WEP specification that include 802.11i and 802.1x. 802.1x can be included in any access point and will permit authentication to any authentication database (EAP RADIUS server). The 802.11i Security Subgroup is working to specify stronger encryption algorithms for future use in 802.11 networks. Compaq is an active participant in this effort. In the current draft specification, a strengthened version of the RC-4/per-frame IV encryption algorithm, and a 128-bit AES encryption algorithm are proposed. Per-user authentication eliminates the WEP key-distribution problem (mentioned further below). The 801.11i standard ratified in 2001 will be the future encryption standard. A fully secure solution will involve the use of 802.11i with its AES-based encryption algorithm along with 802.1x as the key distribution and network access mechanism.

802.1x is not limited to wireless networks. It can be used to authenticate user access to any closed network. For example, a company may have a private network, which should be accessible only to employees, with more public segments that can also be made available to customers. Without 802.1x it would be necessary to isolate these two networks, which could lead to significant duplication of effort and equipment.

[6] Wired Equivalent Privacy (WEP) is an optional IEEE 802.11b feature used to provide data security equivalent to that of a wired LAN without privacy-enhancing encryption techniques. According to the 802.11b standard, WEP data encryption is used to prevent access to the network by intruders using similar WLAN equipment and to prevent capture of WLAN traffic through eavesdropping.

The fundamental approach used by 802.1x is to authenticate users at the edge of the private network. It would be conceivable to perform this processing at other points within the core of the network, for example using MAC addresses. However, it would be difficult to protect all authenticated end stations from unauthenticated stations, since intruders could bypass authentication at least on their own segments. It is significantly less complex, and more scaleable, to ensure security if the authentication is performed on the external boundary of the network. It is possible to develop a tiered authentication scheme in which the public is able to access the external network. All employees can access the corporate network, and individuals can access their restricted departmental LANs.

A typical bridge would connect segments that are private and presumed to already be secure, such as those on the corporate network. An 802.1x bridge can connect these segments, too, but its added value lies in its ability to optionally authenticate a port before allowing it to connect.

What this means is that the bridge is configured with both controlled and uncontrolled ports. Those that are uncontrolled do not need to authenticate and would see the device as though it were a traditional bridge. Devices connecting to the controlled ports would not be able to access any of the connected segments (neither the segments on the uncontrolled ports nor the segments on authenticated controlled ports) until they were authenticated successfully.

The scenario sounds simple in principle. Where it becomes slightly more complicated is in the actual authentication. Conceptually it would be feasible to let the bridge perform the authentication using a cache of authentication information. However, that would be unnecessary overhead for the bridge and would mean that authentication information would need to be replicated to all bridges, which is neither efficient nor secure.

Instead, the bridge (called the Authenticator) may relay authentication requests from a client (called the Supplicant) to an Authentication server. This is very similar to the RADIUS model of authentication and, in fact, it is expected that many Authenticators will be RADIUS clients -- and many Authentication servers therefore RADIUS servers.

There are three players in this topology. The Authenticator sits in the middle with both controlled and uncontrolled ports. The Authentication server is connected to an uncontrolled port. The Supplicant is connected to a controlled port.

The authentication process would run along these lines:

- The Supplicant connects to a controlled port
- Either the Authenticator or the Supplicant initiates authentication
- A challenge is sent from the Authentication server to the Supplicant via the Authenticator
- The Supplicant signs, or otherwise cryptologically processes, the challenge.
- The Supplicant sends the result back to the Authentication server via the Authenticator
- The Authentication server sends the status (success or failure) back to the Supplicant via the Authenticator
- The Authenticator intercepts the status and, if successful, opens the port.

There are a few issues to consider in this process:

- The only traffic that the Authenticator may relay from/to a controlled port is authentication requests/responses

- For security reasons, the authentication information must be cryptologically secure. This implies that the Authenticator cannot decrypt the credentials.
- The model must be extensible to new authentication mechanisms as they are invented and implemented.

In order to ensure that the Authenticator can always identify and interpret new authentication mechanisms, any authentication types must be encapsulated using the Extensible Authentication Protocol (EAP) as specified in RFC 2284. EAP already supports multiple authentication schemes including smart cards, Kerberos, Public Key Encryptions, and One Time Passwords. Many others can be added.

The biggest security consideration of 802.1x is that its sole purpose is authentication. It does not provide integrity, encryption, replay protection or non-repudiation. These would need to be implemented with complementary schemes such as IPSec.

There are also other points of vulnerability that must be addressed in any implementation of 802.1x:

- Piggybacking on an authenticated port – Multiple end stations on a port must be detected and disconnected
- Interception of credentials – Passwords must always be encrypted
- Subversion of authentication negotiation – It should not be possible to provoke a lesser form of authentication by interfering with the authentication process

802.11b WLANs are ideal candidates for 802.1x authentication since they represent a completely uncontrolled periphery. While it is possible to restrict physical access to wired LANs, this is not feasible in a wireless environment. It is much more difficult to monitor and enforce the air space around office buildings than the ports and wiring within them.

This vulnerability is currently addressed using Wired Equivalent Privacy (WEP), which is available on 802.11b Access Points. If WEP is in use, then all stations must configure a symmetric passphrase in order to connect. All transmission is then encrypted with 40-128 bit encryption.

Recently, there have been alleged cryptological weaknesses with the WEP algorithms that have cast a shadow on its use. Beyond these there is a fundamental problem with key distribution and update. Since WEP keys are typically symmetrical (the same on the Access Point and all connecting stations) they must be changed in unison. Clearly this is difficult to orchestrate when large user populations are involved.

There have been solutions, including automating regular key changes, for example, using logon scripts; however, they are non-standard and require additional work. There are also problems ensuring that employees who leave the company no longer have access to the network, since they could “remember” their WEP key.

Another aspect of the problem arises when users connect to multiple different wireless LANs (e.g. in public areas or at customer sites). Current WEP implementations require that the user manually change the WEP key each time a new network is selected, which is tedious and interferes with any automated key changes.

802.1x solves all of these problems. It is not necessary to distribute any keys. The user can authenticate to a central Authentication server, which stores per-user credentials that can be disabled or modified as needed.

This does not mean that there is no longer a need for WEP in an 802.11b LAN. As mentioned above, 802.1x only provides authentication. It does not encrypt the over-the-air transmission. It is therefore still possible for hackers to eavesdrop on conversations and intercept sensitive information.

The ideal combination is to use 802.1x for authentication to the network, and WEP to ensure privacy of the transmission. This does not address the cryptological weaknesses of WEP; however, it does open the door for future versions of WEP to focus on privacy rather than authentication.

WWAN Access Points

Telecommunications companies are responsible for the security of the data while the data passes through their routers. That data is as secure as the trust management of privileges of the employees working for the carrier itself. This level of security cannot be improved upon by the corporation or by the access device user. Specific security provided for WWAN technologies is described above under the section titled *"Security Specific to WWAN Carrier Technologies."*

Generally speaking, when data travels along the phone lines to the corporate firewall, the data is secure barring phone line tapping. This is not a unique security problem and will not be discussed in this paper, which is focused on wireless security.

Corporate Firewalls

The fourth key juncture in the pipe, after mobile access devices, wireless connectivity technologies, and access points, centers on corporate firewalls.

A firewall is a set of related programs located at a network gateway server, which protects the resources of a private network from users from other networks. (The term also implies that a security policy is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and to control what outside resources its own users can access.

A firewall, working closely with a router program, examines each network packet to determine whether to forward it to its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed on a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are several firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol (IP) addresses. For mobile users, firewalls allow remote access to the private network through secure log-on procedures and authentication certificates.

A number of companies make firewall products. Features include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface (GUI) for controlling the firewall.

Figure 12 (next page) illustrates a corporate network with firewalls.

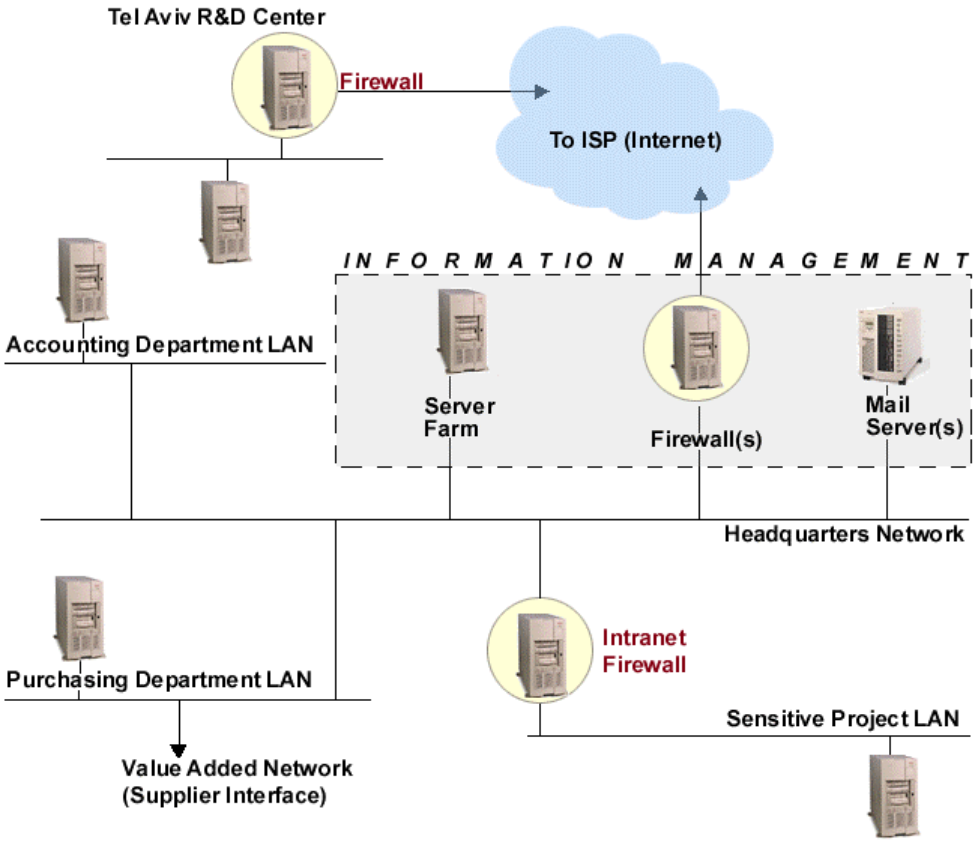


Figure 12: Corporate Network with Firewalls

"On its own, a firewall is a particularly dangerous single point of failure for network protection. Intrusion Detection Systems (IDS) provides an effective secondary protection measure to prevent security policy failure. IDS technology is also useful in detecting some types of malicious behavior by insiders. IDS can be both network based and host based."[7]

Application and Data Servers

The fifth and final key juncture in the pipe, after mobile access devices, wireless networking technologies, access points, and firewalls, centers on the application and data servers that reside inside corporate firewalls. The security vulnerabilities associated with using data servers, desktops with hard drives containing data, and application security are the same for wired and wireless access. Therefore, no attempt is made here to explore the security issues associated with internal data control. It is important, however, to recognize this end of the pipe as a point of entry to data that is being transmitted wirelessly. Corporations are continuously exploring ways to secure data on users' internal machines in multiple ways: for example, by implementing locked door policies and by multi-factor authentication requirements.

[7] *Safe Computing and E-Business: Protecting the Enterprise to Assure E-Business Success*. See this technical guide for more information on firewalls.

See “Safe Computing and E-Business: Protecting the Enterprise to Assure E-Business Success” (http://activeanswers.compaq.com/ActiveAnswers/Render/1,1027,1317-6-100-225-1,00.html) the Compaq technical guide cited at other places in this paper, for detail on security measures recommended for corporate servers.

Conclusion

Pre-wireless technologies such as networked desktop computers, extranets, firewalls, and virtual private networks (VPNs) all have certain vulnerabilities to intrusion and attack. Such attacks, however, can be traced to a physical location, and the risks they pose can be overcome if the security holes are anticipated. With wireless connectivity, however, the ability to trace a breach in network security to a physical location is severely limited at present. A lost or stolen mobile device may compromise the network. Issues such as subscription fraud, eavesdropping, and denial-of-service attacks acquire even greater weight because of the difficulty in tracing them to a physical location.

In general, it may be considered both a blessing and a challenge that wireless users have benefited from the security lessons learned from wired technologies in the 1990's. Whereas security around new technologies in the nineties traditionally arrived as an afterthought, wireless users expect security to be built into the system from the beginning. Products without security will not survive. This paper has shown, however, that users of wireless networks are not taking full advantage of available security mechanisms. This paradox is in line with a traditional response to new technology in which excitement trumps caution for a time.

It is imperative for users to make use of the security technologies and techniques available for both wireless and wired networks. The following principles apply:

1. A security policy must address every essential element of security (Privacy, Authentication, Integrity, Non-Repudiation)
2. A security policy must be applied at every point in the wireless access pipe (device, connectivity technology, access point, corporate access, and corporate data.
3. A security policy must be consistently enforced for all users, regardless of device or method of access.
4. Multiple technologies or security policies should be applied for greater security at key points in the pipe and should address the key essential elements of security.

Bibliography

Angelo, Michael, "Wireless Security Presentation from Michael Angelo" (Unpublished Compaq White Paper).

Davies, Joy, "Wireless Security: Financial Industry Service and Solutions" (Compaq PowerPoint Presentation, October 9, 2000).

Gomes, Lee, "Often unguarded wireless networks can be eavesdroppers' gold mine" (Wall Street Journal Online, April 27, 2001).

Gregory, Scott, "Mobile Device Security Overview: Fundamentals, Solutions, Opportunities" (Compaq PowerPoint Presentation, January 25, 2001).

Grupposo, Diana, "Business Value of Security Solutions" (Compaq White Paper, November 2000).

Hayes, Quentin, "Elements of Security for Clients and Servers: A Technology Paper," (Compaq White Paper, December 18, 2000).

Hunt, Steve, "Wireless Security Risks are Manageable" (IntraGiga, February 26, 2001).

IBM Security Website, http://www-3.ibm.com/security/technologies/techintro.shtml.

Inskeep, Chris, "Safe Computing and E-Business: Protecting the Enterprise to Assure E-Business Success" (Compaq Technical Guide, February 2000).

"MultiPort Bluetooth Communication (Compaq White Paper, March 2001), http://www.compaq.com/support/techpubs/whitepapers/14zn-0501a-wwen.html.

"MultiPort Technology Overview" (Compaq White Paper, March 2001), http://www.compaq.com/support/techpubs/whitepapers/14zm-0501a-wwen.html.

"MultiPort Wireless Local Area Networking" (Compaq White Paper, May 2001), http://www.compaq.com/support/techpubs/whitepapers/14zl-0501a-wwen.html.

Rhoton, John, "Wireless Security" (TLG Knowledge Brief, April 2001)

"Technical White Paper Discussing Encryption Definitions and Methods Used in Data Communications Systems" (Technical Communications Corporation, 1996), http://www.tccsecure.com/whtppr.htm.

Thorsberg, Frank, "Half of U.S. Broadband Users Unprotected" (PCWorld.com, July 16, 2001), http://www.pcworld.com/news/article/0,aid,55154,00.asp.

Verton, Dan, "Your Wireless LAN Can Be Hacked" (Computerworld, July 13, 2001), http://www.pcworld.com/news/article/0,aid,55146,00.asp.

Winter, Ed, "Compaq WiFi: IEEE 802.11b Security Layers" (Compaq White Paper, March 29, 2001).

"WLAN Security," (Orinoco Sales Bulletin 034/A, February 2001).