A Primer on

Mobile Application Security

ArcStream Solutions

Ver 2.0

Table of Contents

Executive Summary

Companies across the world are turning to wireless technologies to mobilize their workforces and extend enterprise applications and data to the field. Mobility brings competitive advantages through personal contact, resource flexibility and streamlined processes enabling companies to enhance revenue generation, increase productivity and improve customer relationships. Already 40 million strong, the mobile worker population is growing 9% each year according to IDC. And, by 2004, Gartner Group estimates that 65% of Global 2000 companies will offer their mobile workforce some type of wireless access to critical business applications.

But where mobile workers roam, security issues follow.

Security is a major concern today for both wired and wireless systems. With ample *motive*, *means* and *opportunity*, security threats and incidents have skyrocketed.

- *The opportunity* arises from storing and transmitting more information electronically, inadequate security practices, and lax behavior by those responsible for safeguarding data, systems and assets.
- *The means* arise from the widespread use of interconnected, public networks with limitless access points and no pervasive security plan.
- *The motive* resides in "bad guys" armed with the same tools as security experts (powerful computers, sophisticated software and hardware) and exploiting flaws in widely installed software.

When it comes to wireless networks and applications, security issues are even more acute. In a recent poll by *CIO* magazine, IT executives using wireless technology prominently ranked security as their number two concern behind integration, and rightly so. Not only are wireless systems subject to the same security issues affecting wired systems, they also face a separate host of security challenges. Because wireless networks transmit data over open airwaves, they are especially vulnerable to interception, often by individuals who are "on the move" and difficult to pin down. Moreover, small, handheld devices lend themselves to theft and misuse. And shared, public infrastructures make it impossible to control and ensure consistent levels of security throughout.

Obtaining hard numbers on security incidents and associated costs is difficult, primarily because companies fear the consequences of disclosure: negative PR, stock value declines and follow-on attacks. But in a survey sponsored by the Computer Security Institute, 85% of respondents admitted suffering security breaches in the last 12 months and 64% acknowledged financial losses from those breaches totaling $400 million. With wireless networks, regular reports of unauthorized interceptions -- from credit card authorizations and pager messages over wireless networks, to email messages over wireless Internet connections, to law enforcement data over short-wave wireless networks -- show that security incidents are increasingly commonplace and potentially costly. In a sign of things to come, a recently filed California lawsuit for theft of trade secrets alleged that the perpetrator, sitting in an adjacent parking lot, used a laptop computer to gain access to and steal proprietary source code from the owner's wireless network.[1]

In the face of these concerns, technologists and security experts have not been idle. Over the years, they have developed a comprehensive suite of tools, techniques and technologies to solve many security issues ranging from authentication, to identification and data integrity. Using a combination of techniques, from cryptography, to authentication servers, firewalls, intrusion detection, biometrics, virus detection and virtual private networks, companies are now able to better protect their wireless applications, data and devices from security breaches.

The Mobile Security Challenge

Any company considering deploying mobile applications must address some basic security challenges. A mobile solution that extends enterprise applications and data to mobile devices needs to be at least as secure as the existing enterprise infrastructure. Security is only as strong as its weakest link. Security solutions for mobile applications must address the entire mobile path, from the back-end business application to the client device. They must also work seamlessly and in concert with overall corporate security policies.

When it comes to end-to-end mobile application security, there are three major concerns:

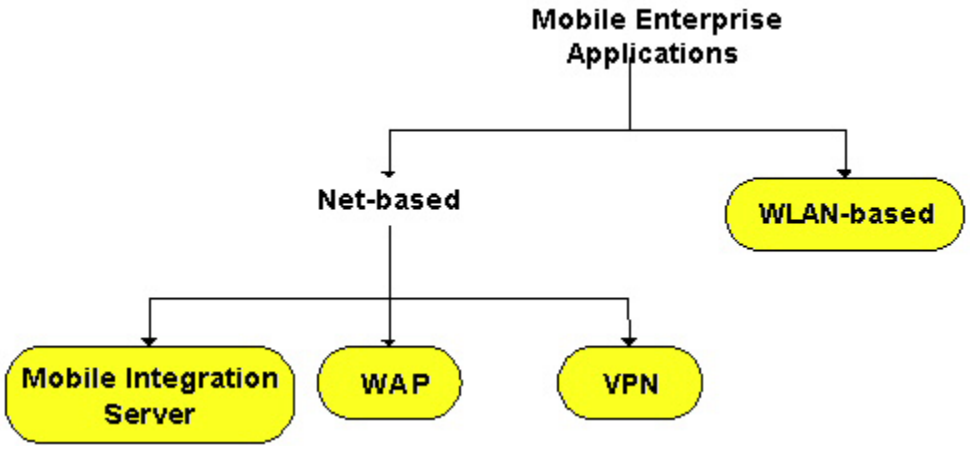
- **Message privacy** -- ensuring that sensitive data is not compromised during transit, usually accomplished using cryptography.

- **Authentication** -- ensuring that the identity of all users involved in the communication is correct, usually achieved using certificates or username/password techniques.

- **Device security** -- ensuring protection of data stored on a mobile device, usually accomplished through a combination of password protection and data encryption.

These security concerns are exacerbated by the proliferation of mobile application types and devices found within a typical enterprise. Members of an executive team may use Research in Motion (RIM) Blackberry devices, for example, to have real-time email access while a field service associate might use a synchronization-based application on a Palm device. Security solutions must work across all of these applications, device types and supporting platforms.

This white paper identifies, from a technical perspective, the main security challenges facing enterprises today when implementing and supporting the four types of mobile applications illustrated below: mobile server-based applications, WAP applications, VPN applications and WLAN-based applications. The paper begins with a discussion of cryptography, the primary security technique underlying all mobile communications. Next, the paper describes each of the four mobile application types and presents specific security issues and recommended solutions. Lastly, the paper gives a brief overview of some of the security challenges surrounding the use of mobile devices.



1. Cryptography

A Background

Cryptography forms the basis of all security solutions. Cryptography is the technique used to convert plain text into cipher text and vice-versa. In a secure communication channel, the parties involved usually rely on cryptography to protect data privacy.

Cryptosystems -- the processes that encrypt and decrypt data -- use mathematical algorithms to convert plain text, like the readable text on this page, to cipher text. Developed by cryptography experts, these algorithms are composed of complex mathematical functions to carry out their work. Rather than create their own algorithms, companies normally delegate the task to professional cryptographers whose trusted encryption algorithms have been scrutinized and battle-tested for years.

Algorithms commonly encrypt and decrypt data using keys. A key may consist of a number, text, or a combination of both. By using keys, the security of a system cannot be compromised, even if the algorithm is publicly available. Without the proper key, an attacker cannot possibly decrypt the data. Keys are generally easier to generate and maintain than algorithms.

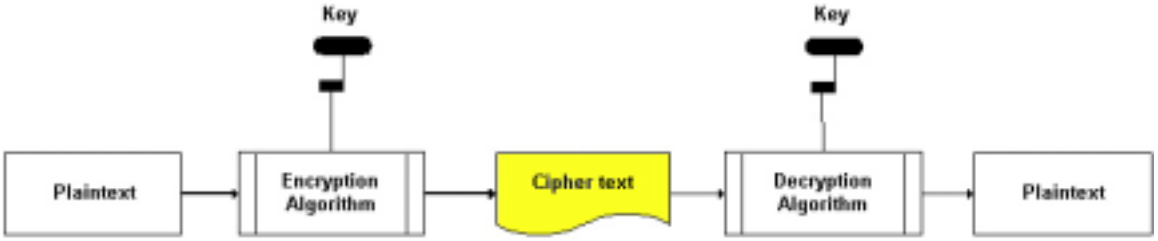


Figure 1 - How Cryptography Works

There are two kinds of cryptography, symmetric (private-key) and asymmetric (public-key).

B Symmetric cryptography

With symmetric cryptography, the sender and receiver share the same secret key to encrypt and decrypt the data. The security of a symmetric cryptosystem is dependent upon the strength of the algorithm, the length of the secret key, and the ability of both parties to keep the key secret. The process by which keys are exchanged and distributed must itself be secure to ensure the integrity of the secret key.

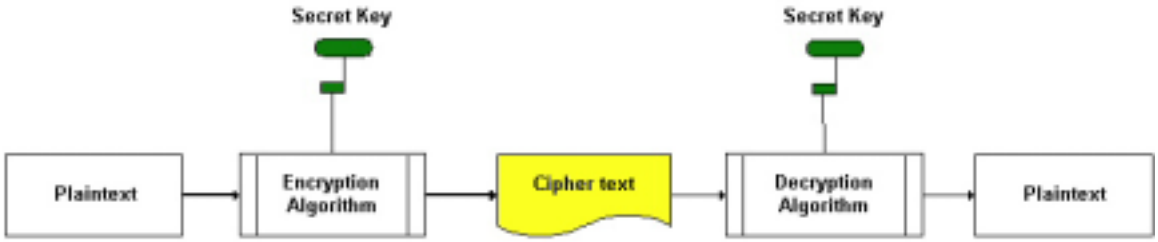


Figure 2 - Symmetric Cryptography

Two basic types of symmetric algorithms exist: block ciphers and stream ciphers.

(i) Block ciphers

A block cipher is the most common type of symmetric-key encryption algorithm. Block ciphers break plain text into fixed-length blocks of data, usually a 64-bit block size, and encrypt each block into a cipher text of the same length using the shared, secret key. The same plain text will always be encrypted to the same cipher text if the same key is used.

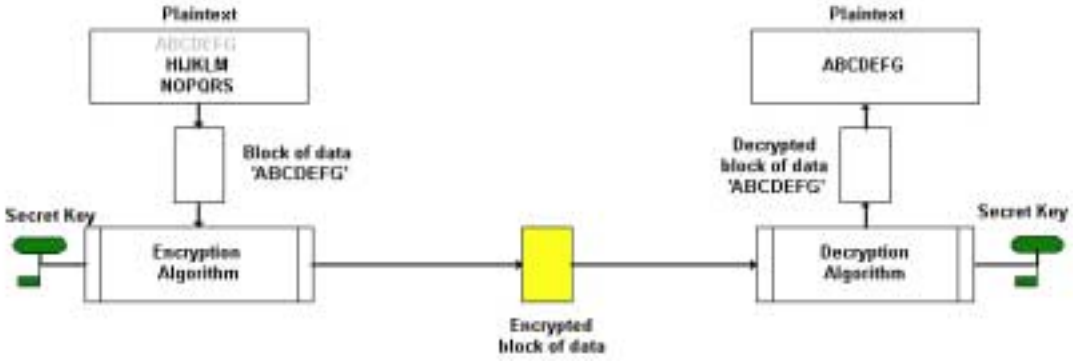


Figure 3 - Block Cipher Encryption

DES
Data Encryption Standard (DES) is the standard encryption method for symmetric cryptosystems based on block ciphers. It was developed by IBM in 1974 and adopted as a national standard in 1977. DES is specified in the American National Standards Institute (ANSI) X1.92 and X3.106 standards and in the Federal Information Processing Standards (FIPS) 46 and 81. DES encrypts 64-bit blocks of plain data using a 56-bit encryption key

(ii) Stream ciphers

Unlike block ciphers, stream ciphers operate on smaller units of plain text, usually bits. Stream ciphers encrypt the plain text data using a stream of keys that are generated using a standalone, shared key. The cipher text is decrypted using the same key stream on the other side of the communication link.

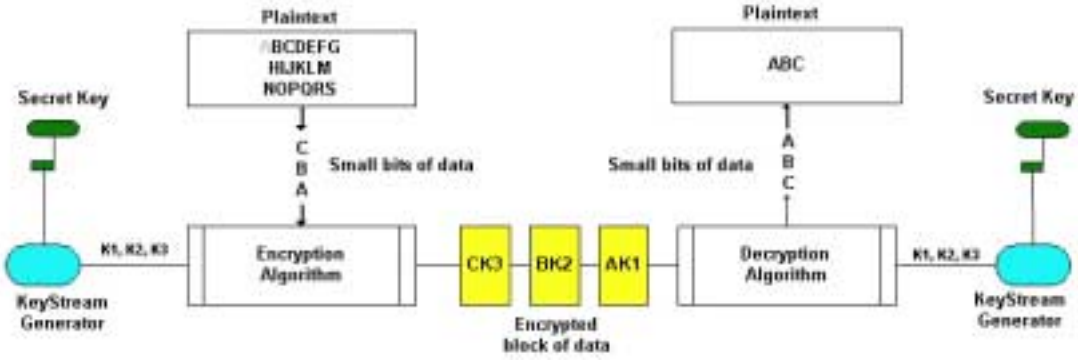


Figure 4 - Stream Cipher Encryption

The most important part of a stream cipher-based symmetric cryptosystem is the key generator or key stream generator -- the component responsible for generating the pseudo random key stream. If the key stream generator produced perfectly random keys, the security of stream ciphers would be unbreakable. But it can't do so because the key stream generator at the other end of the communication link must be able to generate the exact same keys in order to decrypt the cipher text. As a result, the key stream generator usually produces a key stream that is very close to random, but is actually deterministic and capable of

being reproduced at decryption time. The closer the key stream generator's output is to random, the harder it is to break.

(iii) Block Ciphers Versus Stream Ciphers

Block ciphers are usually preferred over stream ciphers for the following reasons.

- **Key Management --** Stream ciphers generate a different key for every encryption whereas block ciphers use the same key. For large amounts of data, such as credit card numbers stored in databases, key management is much easier with block ciphers.

- **Standardization --** DES, Triple DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard), all block ciphers, have been endorsed by the National Institute of Standards and Technology (NIST) as standards for symmetric cryptography. These algorithms enjoy great industry acceptance and interoperability.

C Asymmetric Cryptography

Unlike the single, shared key used in symmetric cryptography, asymmetric cryptography consists of a private and a public key pair. The public key is distributed to the party at the other end of the communication link, and the corresponding private key is kept secret. Using asymmetric or public-key cryptography, the server and the client use different keys to encrypt and decrypt the data. This technique avoids the secret key distribution problem associated with symmetric cryptography. Public-key cryptography (PKC) ensures that a message encrypted with a public-key can be decoded only with the matching private key and vice-versa.

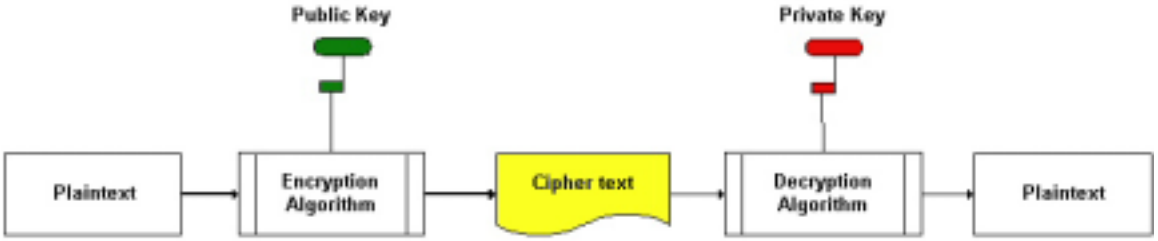


Figure 5 - Asymmetric Cryptography

Along with encryption, Public-key cryptography can also be used to authenticate and identify the parties in a communication. Digital authentication and digital certificates accomplish these functions, and are described below.

(i) Digital Authentication

Along with data encryption, PKC is often used for authentication. Referred to as digital authentication, this technique relies on a mathematical function called a one-way hash. A one-way hash is a mathematical number with the following characteristics:

- The value of the hash is unique for the hashed data. Any change in the data, even deleting or altering a single character, results in a different value.
- The contents of the hashed data cannot be deduced from the number.

One-way hashes are also known as message digest, fingerprint or cryptographic checksum. They are created using a hashing algorithm. Many different hashing algorithms are available, but the two most widely used are:

- MD5, a 128-bit algorithm created by Ron Rivest which has never been broken
- SHA-1 (Secure Hash Standard), the current approved hash algorithm, stronger than MD5 and producing a message digest of 160-bits.

The following diagram represents the steps involved in the digital authentication process:

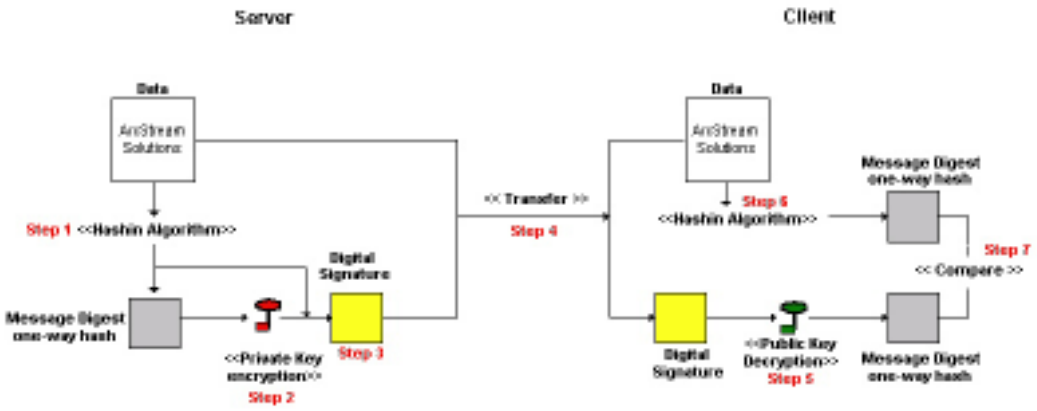


Figure 6 - Digital Authentication

Step 1: The signing software, usually the server, creates a one-way hash of the initial plain text data
Step 2: The server then uses its private key to encrypt the hash
Step 3: The encrypted hash is bundled with the hashing algorithm to produce a "digital signature." These PKC-based digital signatures have the same legal weight as inked signatures on paper, thanks to the recently passed U.S federal E-SIGN bill, which took effect on October 1, 2000.
Step 4: The digital signature and the original plain text data is transferred to the client
Step 5: The client uses the server's public key to decrypt the hash
Step 6: The client then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the plain text data.
Step 7: The client compares the two hashes. If the two hashes match, it guarantees that the data has not changed and the public key matches the private key of the server.

(ii) Digital Certificate

By matching the unique public and private keys, the digital authentication process authenticates the host but doesn't confirm its identity. To confirm the identity of the host, digital authentication is usually supplemented by the use of digital certificates.

A digital certificate is an electronic document used to identify the host and associate the host's identity with its public key. Digital certificates are validated and issued by certificate authorities (CA) that are generally third-party organizations like Verisign and others. In a public-key infrastructure, a CA issues, manages and revokes certificates for its community of end users, and is ultimately responsible for end user authenticity. Various kinds of certificates are in use, the most prevalent of which is International Telecommunications Union X.509 version 3.

The digital authentication process shown in figure 6 diagram represents a server authentication process. The same process is used to authenticate the client or other hosts involved in a PKI. Digital authentication is useful in a variety of circumstances including:

- A digital signature on an email message, combined with a digital certificate identifying the sender, provides strong evidence that the person identified by that certificate did indeed send the message.

- A digital signature on an HTML form, combined with a digital certificate identifying the browser client, provides evidence that the person identified by that certificate did agree to the contents of the form.

Two popular asymmetric cryptosystems using public keys are RSA and Elliptic Curve Cryptography (ECC). RSA has been widely used for years on PC-based networks, while ECC is gaining in popularity on device and application-constrained networks, such as wireless networks with mobile devices.

(iii) RSA

RSA is the most widely used public-key cryptosystem offering both encryption and digital signatures (authentication). Developed in 1977 by, and named after, Ron Rivest, Adi Shamir, and Leonard Adleman, the encryption system is now owned by RSA Security. The company licenses the algorithm technologies and also sells development kits, and makes the mathematical details of the algorithm used in obtaining the public and private keys available at its web site.

Web browsers from Netscape and Microsoft use the RSA algorithm. It also forms the basis of many standard Internet security protocols including S/MIME (Secure Multi-purpose Internet Mail Encryption), SSL (Secure Sockets Layer), IPSec (Internet Protocol Security), TLS (Transport Layer Security) and is part of many official standards worldwide including:

- The ISO (International Standards Organization) 9796
- ITU-T X.509 security standard
- Society for Worldwide Interbank Financial Telecommunications (SWIFT) standard
- French financial industry standard
- ANSI X9.31
- X9.44 draft standard for the U.S. banking industry

(iv) ECC

ECC provides an alternate but equally secure public-key cryptosystem as RSA. ECC provides similar levels of security compared to RSA, but with significantly reduced key sizes. This improvement translates into faster processing, and lower memory and bandwidth requirements, making ECC an ideal choice for mobile enterprise applications with limited memory, bandwidth and computational power. ECC is gradually becoming the de-facto standard for security on constrained devices.

To understand the benefits that ECC can bring to mobile applications, consider the following table developed by Certicom Corp., one of the major proponents of ECC.

RSA Key Size	Time to Break (MIPS years)	ECC Key Size	RSA: ECC Key Size ratio
512	10^{4}	106	5:1
768	10^{8}	132	6:1
1024	10^{11}	160	7:1
2048	10^{20}	210	10:1
21000	10^{78}	600	35:!

2. Mobile Server based Applications

A Background

Mobile server-based applications encompass all kinds of connected and disconnected mobile applications that use enterprise data in real-time or that synchronize with enterprise servers either locally or remotely. These applications usually consist of a mobile integration server that sits within the enterprise LAN and acts as the management and synchronization conduit for mobile devices. Example mobile integration servers include:

- Blackberry Enterprise Server
- AvantGo Mobile Server
- XTNDConnect Synchronization server
- HotSync server from Palm Inc.

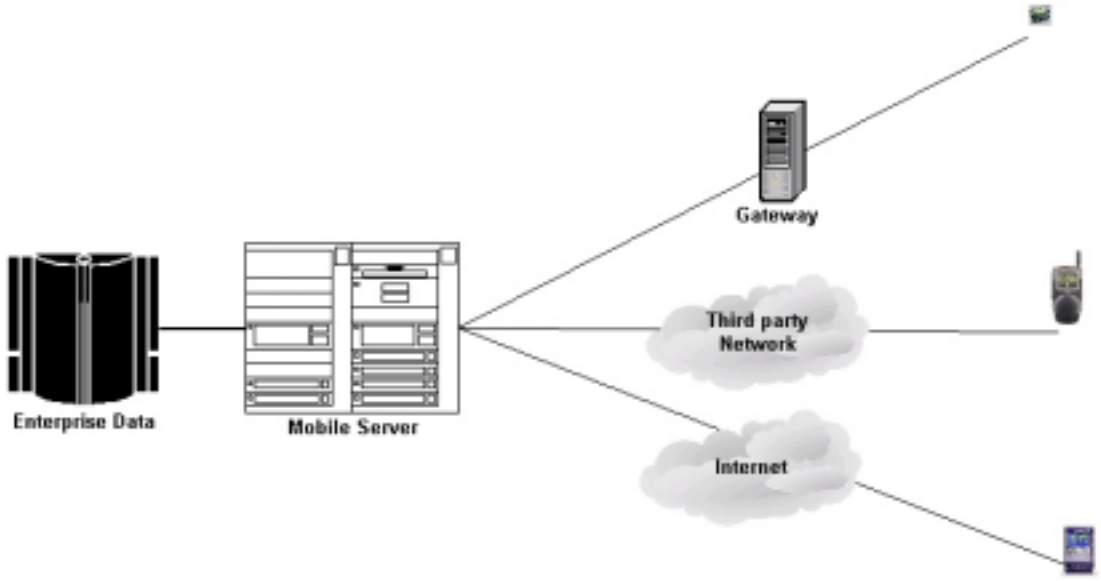


Figure 7 - Mobile Server-based Application Architecture

B Mobile Server Security Challenges and Solutions

Like any server exposed to the Internet or an outside network, such as Web servers, FTP servers or email servers, mobile integration servers and the applications residing on them have heightened security requirements. Any time a server is exposed to the outside world, concerns arise over the security and integrity of data transmitted to and from the server. Network attacks and weaknesses in the schemes used to distribute and handle cryptographic keys are the primary security concerns facing mobile servers.

(i) Challenge: Network Attacks

Network attacks, or spoofing data packets, occur when an unauthorized person attempts to intercept data packets in transit to or from a network server.

Solution: To protect against network attacks, enterprise applications built using a mobile integration server usually rely on symmetric cryptography. The only way to break a symmetric cryptosystem is to use a brute-force attack, which involves trying all the possible keys that can be used for encryption. Assuming the strength of the encryption algorithm is perfect (i.e. that there are no back-doors or flaws to be exploited), the complexity of a brute-force attack depends on two factors:

- Number of keys to be tested
- Time required for each test

The number of keys to be tested depends on the length of the key. For an 8-bit long key, there are 2^8 (256) possible permutations, and 2^{56} possible permutations for a 56-bit key. DES, the standard algorithm for symmetric cryptography, is based on a 56-bit key solution. A supercomputer that can test a million keys per second will take 2,285 years to try all the keys of a 56-bit key solution. Recently, however, security professionals have discovered a low-cost ($1 million) computer, named DES-cracker, which can crack a 56-bit DES key in as little as 3.5 hours. These advances in computing power have rendered DES a very weak security mechanism, and it is not recommended as an encryption algorithm for enterprise applications. Triple DES, a more secure variation of DES, should be used instead. The encryption method used by Triple DES is similar to DES, and the plain text is encrypted thrice using three 56-bit keys providing much more secure and robust encryption. Triple DES has been endorsed by NIST as the current standard, and is also favored by the banking industry to transfer confidential financial data electronically.

DES-based encryption algorithms like DES and Triple DES have been a standard since 1977. Currently, a replacement encryption algorithm called Advanced Encryption Standard (AES) is under development. AES promises to be at least as secure as Triple DES and much faster.

(ii) Challenge: Key Distribution

Secret key distribution is a well-known security and management challenge for symmetric cryptosystems like DES and Triple DES. Both the client and the server in the symmetric cryptosystem use the same secret key to encrypt and decrypt the data. If they are in separate physical locations, the administrators must trust a courier, a phone system, or some other medium to exchange the secret key yet prevent unauthorized disclosure. If anyone overhears or intercepts the key in transit then the security of the system is compromised.

Solution: A couple of solutions exist for the key distribution issue: manual secure key exchange and hybrid cryptosystems.

- **Manual secure key exchange**
  Symmetric cryptosystems should be supplemented with a completely secure means of key distribution. The simplest of key distribution schemes is to allow the shared key to be exchanged only within corporate firewalls. The secret key can be generated on a user desktop on the corporate LAN and distributed to the mobile device through a serial port connection. The same key is then copied over to the mobile application or email server. Enterprise servers such as Blackberry enterprise email server provide a well-defined and semi-automated procedure for such a key distribution system.

- **Hybrid cryptosystem**
  Both symmetric and asymmetric cryptosystems have drawbacks. Symmetric cryptosystems present a key distribution problem whereas asymmetric cryptosystems are usually very computationally expensive and vulnerable to chosen plain text attacks. When combined, however, these two cryptosystems offset each other's weaknesses. The combined system is known as a hybrid cryptosystem. Hybrid cryptosystems use public-key cryptography for digital authentication and to establish and distribute secret keys for symmetric cryptography, then fall back on the faster symmetric cryptography system for data security. The following diagram represents the communication between enterprise mobile servers and mobile handheld devices using a hybrid cryptosystem.

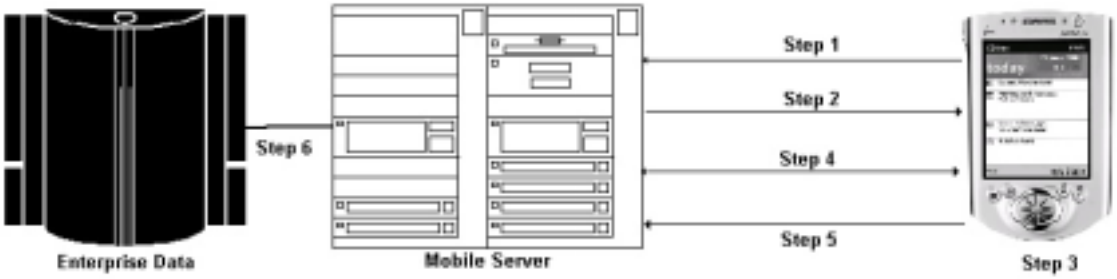


Figure 8 - A Hybrid Cryptosystem

Step 1: The mobile handheld connects to the enterprise mobile server
Step 2: The mobile server sends a digital signature and hashed message to the client device for server authentication
Step 3: The client device authenticates the server using the digital authentication process
Step 4: The client and the server exchange a secret session key. Instead of sharing a pre-defined secret key, the secret key is generated for every client session. This method greatly reduces the risk of discovering the secret key by a brute-force attack.
Step 5: The client encrypts the user credentials with the secret key and sends the encrypted data to the server for authentication
Step 6: The server authenticates the user against the user database (NT domain, Exchange, Lotus Domino). If authenticated, the client and server use the secret key to encrypt all data (DES, 3DES) for that particular session.

3. WAP-based Applications

A Background

Wireless access protocol (WAP) is an open specification that offers a standard method to access Internet-based content and services from wireless devices such as mobile phones. WAP was invented and is driven by the WAP Forum -- a group originally formed by Nokia, Ericsson, Motorola and Phone.com in 1997. The WAP Forum now has 500 member companies who make up 95% of handset manufacturers, carriers equating to 100 million subscribers worldwide including infrastructure providers, software developers and many other companies providing solutions in the wireless space. The benefits of using WAP include:

- Non-proprietary method to access Internet-based content and services
- Network independent
- Extensive industry adoption

The WAP model is very similar to the traditional Internet model. The mobile device contains an embedded WAP browser software that connects to a WAP gateway. The WAP gateway is a software infrastructure residing between the wireless network and the Internet. It optimizes the transmission of content for the wireless network and makes requests for information from web servers in the normal form of a URL. The content for WAP devices is stored on enterprise web servers. WAP content is written in a markup language called wireless markup language (WML) and is formatted suitably for the mobile phone or PDA's small screen and low bandwidth/high latency connection.

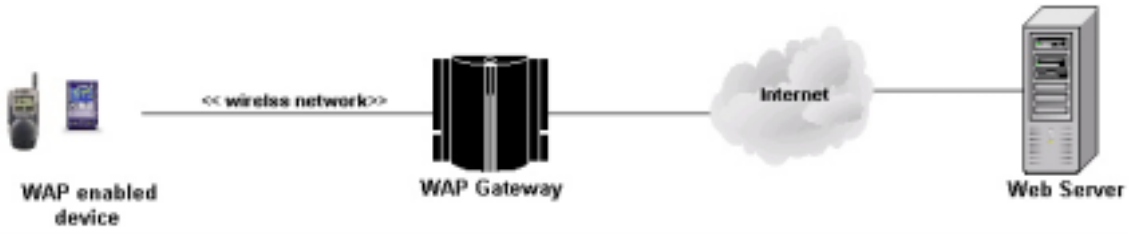


Figure 9 - A Simple WAP Architecture

B Wireless Transport Layer Security (WTLS)

The WAP protocol is a multi-layered architecture, illustrated as follows:

WAE - Application layer
WSP - Session layer
WTP - Transaction Layer
WTLS - Security Layer
WDP - Transport layer
Bearers (CDMA, GSM, etc.)

Figure 10 - The WAP Protocol

WTLS is the security layer specification of the WAP protocol. The primary goal of WTLS is to provide privacy, data integrity and authentication for the WAP protocol. The WTLS specification has been adapted from the transport layer security (TLS) specification. TLS is formulated by the Internet Engineering Task Force (IETF) and is based, in turn, on secure sockets layer (SSL) developed by Netscape. WTLS is customized for wireless networks that require support for both datagram and connection-oriented protocols.

Authentication is an optional feature in WTLS and is carried out via certificates. Currently, X.509v3, X9.68 and WTLS certificates are supported. Privacy in WTLS is implemented by means of encrypting the communication channel. The encryption methods used, and all other necessary values, are exchanged during the mobile client-server handshake. Most bulk encryption algorithms, like DES with 40- and 56-bit keys and Triple DES, are supported by WTLS.

C WAP Security Challenges and Solutions

WAP security issues center on encryption and a phenomenon known as the "WAP GAP." The variety of mobile devices supported by WAP makes it difficult for the protocol to provide consistent and high levels of security across all device types. Moreover, if implemented according to the WAP specification, the handoff performed between the WTLS security layer and the SSL layer at the WAP gateway creates a momentary lapse ("gap") in security, a lapse that has now been rectified by several commercial software solutions.

(i) Challenge: Weak Encryption

Because the WAP protocol has been developed to support a wide range of mobile devices, it allows the client and server to negotiate and choose from many encryption methods. WAP servers provide support for many kinds of algorithms, including those that can accommodate weak mobile devices with limited processing power, memory and bandwidth. This accommodation can result in weak encryption and poor security.

Solution: The only solution to this encryption challenge is to avoid using weak mobile devices for secure enterprise applications. The WAP server for enterprise applications should be configured to use only strong encryption methods and deny access to devices requesting weak encryption.

(ii) Challenge: WAP GAP

The "'WAP GAP'" is a security concern raised by many security professionals. WTLS protects the communication between a WAP handset and the WAP gateway, and SSL usually protects the connection between the WAP server and the web server. There is a split second, however, when the data must be decrypted and then re-encrypted to switch from one protocol (WTLS) to the other (SSL). Security could be compromised if someone were able to crash the machine in the split second between decryption and re-encryption, causing a memory dump to disk. This situation is known as "WAP GAP."

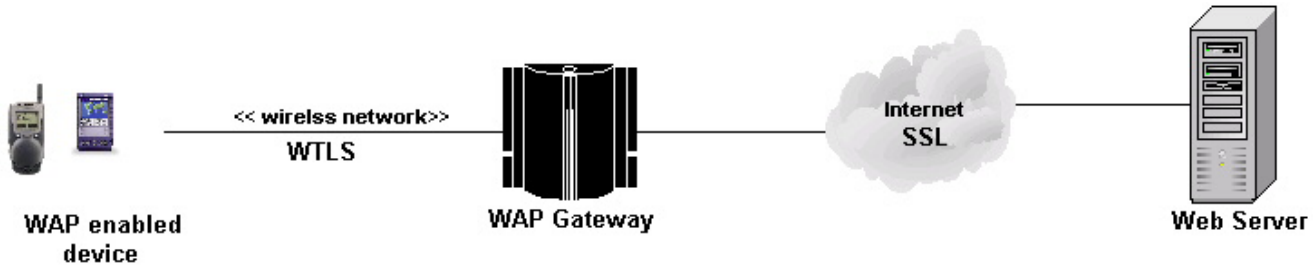


Figure 11 - The "WAP GAP"

Solution: Many vendors such as phone.com, Cylink and RSA provide custom WAP gateway software that takes care of the "WAP GAP" security issue by enabling end-to-end encryption between the web server and the WAP client. These gateway software solutions use designs that are currently under discussion at the WAP forum but are not yet part of any approved WAP specification. Moreover, the "WAP GAP" is not vulnerable to easy attack as it takes place within the secure premises of the service provider hosting the WAP gateway. Enterprises usually inspect security settings around third-party WAP gateways thoroughly before hosting their WAP applications on them.
Only if the security requirements of an enterprise WAP-based wireless application are extremely high, should a company use a custom WAP gateway. For example, a wireless application transmitting publicly available stock quotes would not need a custom WAP gateway whereas an application transferring financial funds would.

4. Virtual Private Networks

A Background

Virtual private network (VPN) technology helps provide secure network connectivity to the enterprise LAN over public lines like the Internet. VPN consists of compatible software or hardware at both ends of the communication link. VPNs have proven popular because they offer operational savings while maintaining the security associated with a private network infrastructure. VPNs are most commonly used for:

- Remote access
  Enterprise VPNs allow mobile workers to access a corporate LAN over the Internet by dialing into their local Internet service provider (ISP).

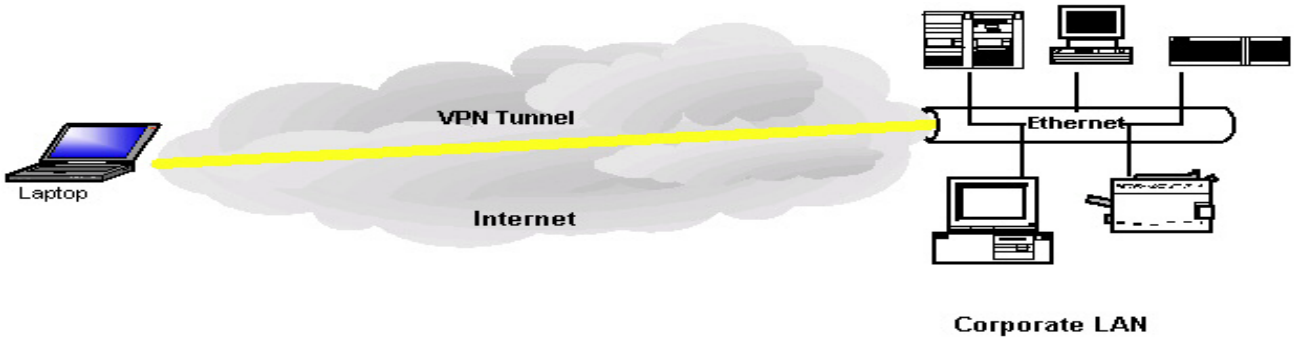


Figure 12 - Remote Access VPN

- LAN-LAN communication
  Small branch offices without a constant Wide Area Network (WAN) connection to the corporate LAN can use VPN to access an enterprise intranet.

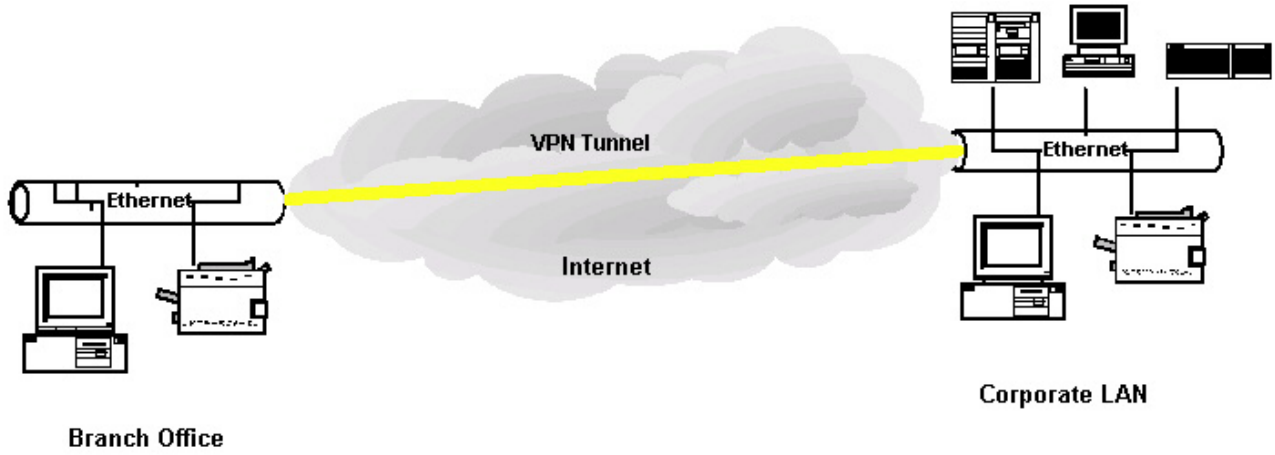


Figure 13 - LAN-LAN VPN

- Controlled access within an intranet
  Enterprise LANs also utilize VPN technology to implement controlled access to individual subnets on the private network. In this mode, VPN clients connect to a VPN server that acts as a gateway to computers behind it on the subnet. This type of VPN use does not involve ISPs or public network cabling.

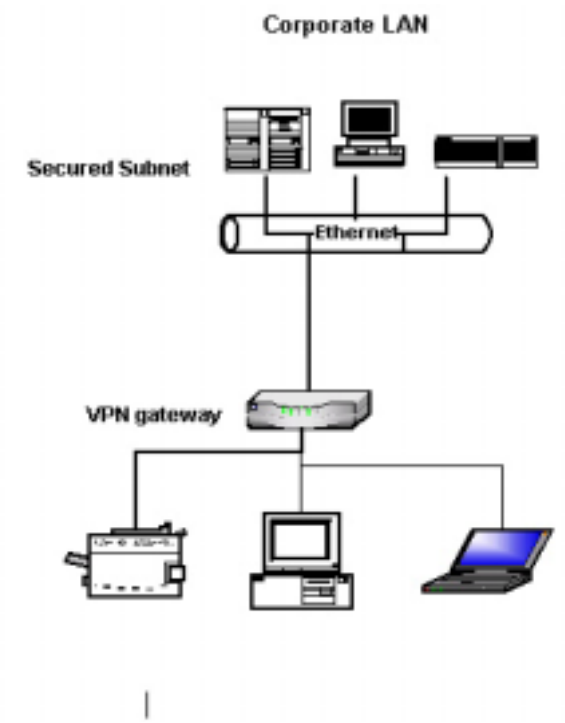


Figure 14 - VPN with Controlled Intranet Access

B VPN technologies

VPN is based on a technology called tunneling. A VPN tunnel works by encapsulating data within Internet protocol (IP) packets to transport information that does not otherwise conform to Internet addressing standards. The entire process of encapsulation and transmission of packets is called tunneling, and the logical connection through which the packets travel is called a tunnel. A tunnel is usually a connection through the Internet.

Tunnels allow remote users to become virtual nodes on the corporate network. From the user's perspective, the nature of the physical network being tunneled through is irrelevant because it appears as if the information is being sent over a dedicated private network. Tunneling server and client software is required at both ends to provide authentication and encryption. For a tunnel to be established both tunnel server and client should use the same tunneling protocol. Three of the most commonly implemented tunneling technologies are point-to-point tunneling protocol (PPTP), layer 2 tunneling protocol (L2TP) and Internet protocol security (IPSec).

(i) PPTP

PPTP is a proposed VPN standard by Microsoft. With PPTP, which is an extension of the Internet's Point-to-Point Protocol (PPP), any user of a PC with PPP client support is able to use an ISP to connect securely to a server elsewhere in the user's company. PPTP uses Microsoft Challenge-Handshake authentication protocol (MS-CHAP) for authentication and Microsoft Point-to-Point encryption (MPPE) for encryption.

- MS-CHAP -- an authentication mechanism to validate user credentials against Windows NT domains.

- MPPE -- an encryption method that uses the RSA RC4 encryption algorithm, operating at the strongest encryption level allowed by the U.S. government -- 128-bit keys in North America and 40-bit keys elsewhere. When MS-CHAP version 2 is used, separate RC4 encryption keys are derived for each direction, and, by default, the encryption keys are changed on every single packet. These factors make even well-resourced brute-force attacks extremely difficult to undertake.

(ii) L2TP

The L2TP technology combines the best of PPTP and layer 2 forwarding (L2F) technologies. L2F is a proposed transmission protocol by Cisco Systems. L2TP provides tunneling over any media that provides packet-oriented point-to-point connectivity, which includes WAN technologies such as X.25, Frame Relay, and asynchronous transfer mode (ATM).

When used over IP networks, L2TP is very similar to PPTP. An L2TP tunnel is created between an L2TP client and an L2TP server. The client may already be attached to an IP network that can reach the tunnel server, or a client may have to dial into a network access server to establish IP connectivity.

L2TP includes the authentication mechanisms within PPP, mostly challenge-handshake authentication protocol (CHAP). L2TP does not include encryption or processes for managing the cryptographic keys required for encryption in its specifications. The current L2TP draft standard recommends that IPSec be used for encryption and key management in IP environments. Future drafts of the PPTP standard may do the same.

(iii) IPSec

IPSec is designed by the Internet Engineering Task Force (IETF) as an end-to-end mechanism for ensuring data security in IP-based communications. The overall IPSec architecture has been defined in a series of request for comments (RFCs), notably RFCs 1825, 1826, and 1827.

IPSec consists of two security, and a key-management, protocol:

- Authentication Header (AH) -- a protocol providing data origin authentication and connectionless integrity.
- Encapsulating Security Payload (ESP) -- a protocol providing data confidentiality, connectionless integrity and data origin authentication.
- Internet Key Exchange protocol (IKE) -- a protocol used to negotiate the cryptographic algorithm choices to be utilized by AH and ESP.

IPSec guarantees interoperability between products supporting the IPSec protocol. The IPSec protocols are built around standardized cryptographic technologies. For example, IPSec uses:

- DES and other bulk encryption algorithms for encrypting data
- Keyed hash algorithms (HMAC, MD5, SHA) for authenticating packets
- Digital certificates for validating public keys

C Wireless VPNs

Wireless VPN solutions extend the enterprise-wired VPN infrastructure to allow wireless client access. The growth in deployment of enterprise VPNs and the simultaneous proliferation of mobile applications is driving the convergence of these two technologies. Enterprise VPNs are evolving to include handheld devices like PDAs and smart phones. In wired VPN solutions, remote users access the enterprise VPN gateway by dialing into the local ISP. Similarly, a VPN gateway can be accessed wirelessly from a variety of handheld device types — cell phones, PDAs, or pagers — as long as they support IP. A wireless VPN is not very different from a wired VPN. The IP-enabled wireless client device sends data over a wireless network to its service provider. The service provider transfers the wireless data and connects to the VPN gateway through the Internet.

Wireless VPNs present several issues over wired VPNs, including:

- Vast range of devices
- Various client operating systems
- Different connectivity options
- Proprietary wireless networks

D VPN Security Challenges and Solutions

Most organizations with an existing, wired VPN have adopted sufficient measures to secure their infrastructure. Issues arise when this infrastructure is extended to allow access by wireless clients. The wireless extensions must have security that is at least as robust as the wired network to avoid compromising the entire setup.

(i) Challenge: Ensuring the Security of an Existing VPN Infrastructure

When an existing, wired VPN is extended to permit wireless access, care must be taken to ensure that the security of the existing network remains intact. A wireless implementation with weak security protections has the potential to undermine the security of the entire network.

Solution: To ensure that a wireless VPN does not undercut the security of an existing VPN, enterprises should deploy VPN clients for mobile devices that support the existing enterprise VPN's gateways and protocols. Integrating the infrastructures in this way ensures that the existing VPN remains secure, and allows the enterprise to continue leveraging the investment made in its original implementation. MovianVPN client by Certicom Corp. supports a range of VPN gateways and client mobile devices such as:

Gateways supported:

- Alcatel PERMIT Enterprise 1520
- Check Point VPN-1
- Cisco VPN Concentrator Series 3000
- Intel NetStructure 3130
- Nortel Contivity Extranet Switch 2600
- Radguard clPro 5000
- Symantec (AXENT) PowerVPN

Mobile devices supported:

MovianVPN is available for multiple IP-enabled devices running Palm OS 3.5 or Windows CE 3.0, and future versions will support additional platforms such as Symbian-based devices. Examples of popular devices currently supported include:

- Casio Cassiopeia
- Compaq iPAQ and AERO
- HP Jornada 540 and 680
- NEC MobilePro 770
- Palm III, V, Vx Series

(ii) Challenge: Wireless VPN Security

The wireless VPN solution for the enterprise should provide equivalent security as the wired VPN solution, that is, end-to-end security without any intermediate security gaps.

Solution: MovianVPN offers security for wireless VPNs. It establishes a secure IPSec tunnel to encrypt all traffic between the device and the gateway to decrease the risk of eavesdropping, interception, or tampering. The MovianVPN client implements industry-leading standards including relevant algorithms and protocols from the IETF, IEEE, ANSI, and FIPS organizations. It implements both symmetric and asymmetric algorithms to enhance support of legacy VPN systems. ECC is used to provide fast Internet Key Exchange (IKE) negotiations where supported by the gateway, a solution ideally suited for securing wireless devices limited by low processing speed, network bandwidth, and battery power. MovianVPN also provides the flexibility to choose a level of authentication compatible with the organization's security policies.

5. Wireless LAN (WLAN)

A Background

Enterprises usually implement wireless LANs to extend their wired LANs. WLANs give users the ability to access enterprise LAN resources, such as printers, shared file systems, and servers while they are mobile. WLANs have proven successful within enterprises that benefit from providing real-time data to mobile users over a small coverage area.

WLANs use radio waves to communicate information from one point to another without relying on a physical connection. In a typical WLAN environment, a transmitter/receiver device called an Access Point (AP) connects to the wired network from a fixed location using standard cabling. The AP receives, buffers and transmits data between the WLAN and the WLAN adapter cards on the mobile device. The following diagram illustrates a basic wireless network:

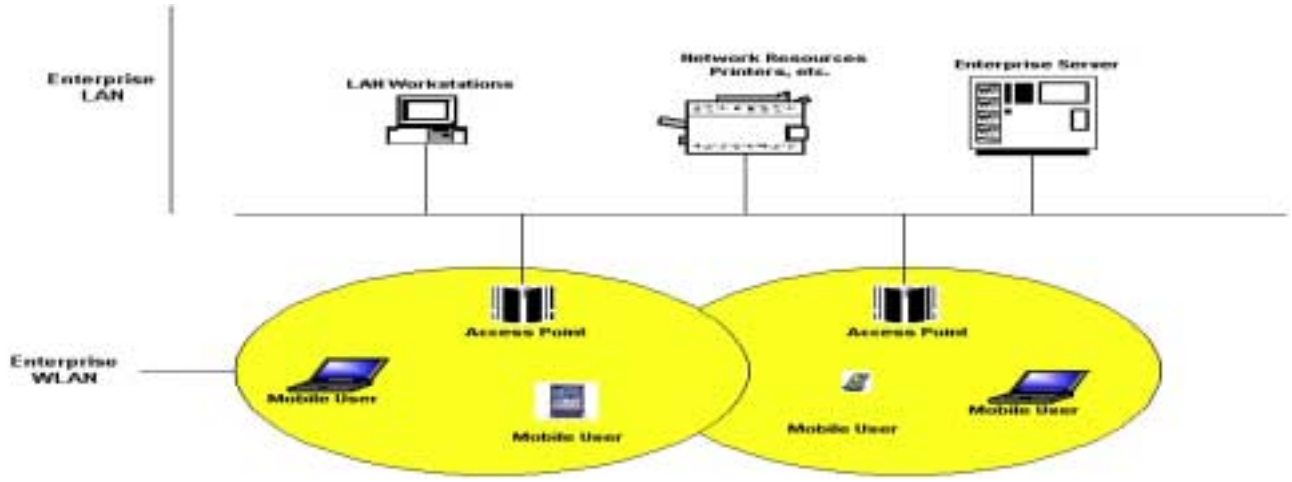


Figure 15 - Basic Enterprise LAN / WLAN

B The 802.11b Specification

In an effort to define a standard for WLAN products, the IEEE released a family of specifications called 802.11, 802.11a and 802.11b. Almost all wireless Ethernet LAN implementations are based on the 802.11b specification. This specification uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) as the path-sharing protocol. If a source station, such as a laptop computer, has a data packet to send, the station checks the system to see if the path medium is busy. If the medium is not busy, the packet is sent; if the medium is busy, the station waits until the first moment that the medium becomes clear. Testing is done repeatedly by the source station via a short test message called RTS (ready to send). The data packet is not transmitted until the destination station returns a confirmation message called CTS (clear to send). If two stations send data at exactly the same time, CSMA/CD prevents the loss of data that might otherwise occur, and provides a system for retrying. It operates at frequency in the 2.4-GHz region of the radio spectrum. Data speeds are generally around 11 Mbps, although speeds up to about 20 Mbps are realizable with 802.11b. The 802.11b standard is backward compatible with 802.11.

C Wired Equivalent Privacy (WEP)

WLAN security is an important issue, not only to secure the wireless network but also to secure the wired enterprise LANs with which it connects. Normally, an intruder intent on breaching a wired enterprise LAN would need physical access to the network. Once a WLAN is deployed, however, an intruder can use it as a conduit to enter and breach a wired LAN without ever coming into physical contact with the network. To secure an enterprise wireless implementation from these types of issues, the 802.11b specification defines three basic security solutions as follows.

- **SSID (System ID)**
  SSID is an identifier code that a network administrator can enter into the setup of all the APs and network interface cards (NICs) that will participate in the WLAN network. This identifier is attached to the packets sent over the WLAN. All the APs are programmed to accept only packets containing the authorized SSIDs.

- **Media Access Control (MAC) Filtering**
  Access to the enterprise WLAN can also be restricted by the unique MAC address of the client device's 802.11 network card. Every AP in the network needs to be programmed with the list of MAC addresses associated with the client computers. If a client's MAC address is not included in this list, the AP denies the client request.

- **WEP**
  To provide WLANs with an equivalent level of privacy as wired LANs, the IEEE 802.11b specification defines an encryption standard named WEP. In a WEP-enabled WLAN, each device on the wireless network is assigned encryption keys called WEP keys. Each device encrypts data with these keys before it is transmitted through the airwaves. If a device receives a packet that is not encrypted with the appropriate key, the device discards the packet. WEP uses the RC4 algorithm with a 40-bit key. WLAN products that support keys longer than 40 bits are also available.

D WLAN Security Challenges and Solutions

The three security solutions proposed by the 802.11b specification as outlined above fail to secure a WLAN in all circumstances. The SSID and MAC filtering approaches are rudimentary at best and not strong enough for enterprise WLANs. Further, the WEP approach contains a security flaw that permits several types of WLAN attacks to proceed, demanding WEP-based solutions that go beyond the 802.11b standard.

(i) Challenge: SSID and MAC filtering administrative overhead

SSID and MAC address filtering provide rudimentary security, and are best suited for home networks. Programming APs manually with a list of SSIDs and MAC addresses gives rise to administrative overhead and limits the scalability of the security solution.

Solution: For large WLAN configurations, SSID and MAC address filtering are not recommended. Instead, organizations should use WEP-based dynamic session keys, as described in the next solution.

(ii) Challenge: WEP Security Flaw

Recently, a group of computer scientists at the University of California, Berkeley, discovered flaws in WEP. The complete report can be found at http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html. According to the report, the following types of attacks are possible on WLANs secured *only* by WEP security:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plain text.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attacks that, after analysis of about a day's worth of traffic, allow real-time automated decryption of all traffic.

Solution: WEP is not intended as a complete security solution for an 802.11b WLAN, but should be supplemented with additional security mechanisms to build a comprehensive security solution that meets organizational needs. Custom security solutions built on top of WEP provide the required additional WLAN security. The weakness of most WLANs is in their use of static WEP keys shared among users. Custom security solutions based on dynamic WEP keys augment 802.11b WEP by creating per-user, per-session, dynamic WEP keys.

With security solutions based on dynamic WEP keys, a wireless client associated with an AP cannot gain access to the network until the user performs a logon. When the user enters a username and password into a logon dialog box, an AP via a Remote Access Dial-in Service (RADIUS) server performs user authentication and derives a dynamic WEP key for the current client session.

RADIUS servers implement RADIUS protocol and are responsible for receiving user connection requests, authenticating users, and then returning all configuration information necessary for the client to deliver service to the users. A RADIUS access server is generally a dedicated workstation connected to the network. Almost all network vendors have adapted RADIUS to support their communications servers. RADIUS servers can integrate with existing user databases such as Windows 2000 Active Directory Services. The following diagram gives an overview of the solution:

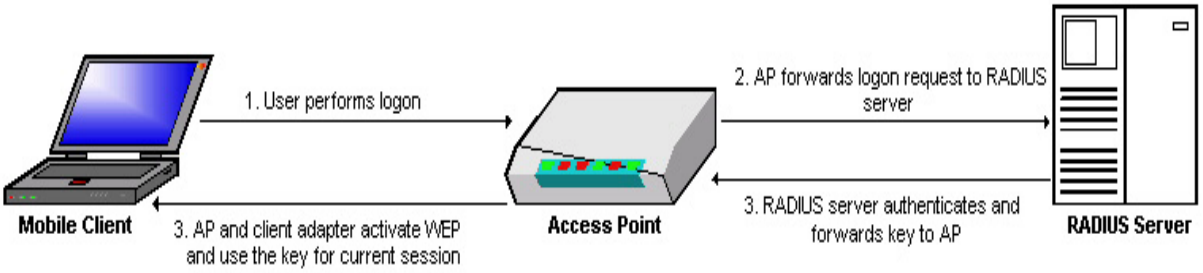


Figure 16 - RADIUS Server Authentication

The following are the key enhancements added by such solutions to 802.11 WLAN security:

- Two-way authentication based on device-independent items such as usernames and passwords known by users but not stored on any hardware
- WLAN encryption using WEP keys generated dynamically upon user authentication, not static keys physically associated with a client device
- Session-based, dynamically generated WEP keys, where a new key is generated for every client session
- Ability for IT administrators to configure re-authentication policies, which forces users to re-authenticate more often and obtain new session keys

Cisco Aironet and Lucent Agere ORiNOCO security solutions based on dynamic WEP keys address almost all concerns raised by researchers at University of California, Berkeley. It is recommended that organizations implementing WLANs supplement WEP security with such proprietary vendor security solutions.

6. Mobile Devices

A Background

A myriad of mobile devices is available on the market today, and corporations can expect to encounter and support a large variety within their enterprise portfolios. Mobile users have relied on devices such as laptops, cell phones and pagers for years. Joining these traditional devices today are data-enabled phone handsets, personal digital assistants (PDAs) such as Palm and Handspring, Pocket PCs running Microsoft's WinCE operating system, souped up pagers such as RIM's Blackberry, and dozens more. Many of these devices support various third-party applications and hardware add-ons to give them greater features and functionality.

The very properties that make a mobile device mobile, such as small size and low weight, come at the cost of functional capabilities, such as processing power and size. Except for laptops, most mobile devices have constrained processing power, display capabilities, memory and bandwidth. Every mobile application and security solution must take these constraints into consideration. That is why solutions such as ECC, with its shorter key encryption approach, are gaining in popularity for mobile implementations.

B Device Security Challenges and Solutions

Securing handheld, mobile devices and the data contained on them is a tricky proposition. These devices are especially susceptible to theft and misuse, which heightens their security requirements. At the same time, device constraints prohibit the implementation of more robust, programmable security solutions.

(i) Challenge: Handheld access control and data security

Client devices are fraught with security issues. Their small, physical size makes them easy prey for thieves. Unlike servers or networking equipment, they normally are not kept in a secure location. Users are often lax about safeguarding their devices and frequently misplace them. Theft and misplacement are problematic because client devices often contain locally stored snapshots of sensitive enterprise data, including passwords and other keys necessary to gain access to enterprise applications and data. For a comprehensive end-to-end security solution for mobile applications, it is vital to secure the data stored on the handheld device.

Solution: Complete handheld security is achieved by two key security measures: authentication and encryption. Authentication allows only authorized users access to data stored on the handheld. Authentication mechanisms built into the handheld device are often supplemented with third-party authentication systems depending on the security requirements of the application. Encrypting data stored on a device provides additional security in the event that a hacker gets a memory dump of the handheld's memory. A combination of strong authentication and encryption systems on the handheld device prevents unauthorized access to handheld data if the device is ever lost or stolen. Various third-party authentication and encryption products are available for popular handheld devices like Palm and Pocket PC. The choice of technology depends upon the security requirements of the application. Listed below are types of security measures and available products.

- **Password Authentication**

  Third-party password-based authentication systems are used to provide low to medium security for handheld data. They disallow access to the handheld data, synchronization process or IrDa port unless a valid password is entered. Most of these solutions can be set to limit the number of password attempts. If the specified limit is exceeded, all handheld data is cleared. This technique prevents brute-force attacks on, and inhibits unauthorized use of, the device. The real user can easily restore original data by performing a synchronization operation with the new device. Most of the applications providing password authentication store passwords in an encrypted form on the device. Following is a brief list of companies, by web site address, providing password authentication products for various handheld devices:

www.asynchrony.com
www.trustdigital.com
www.jawzinc.com
www.iscomplete.com

- **Signature Authentication**
  Signature-based authentication systems for handheld devices use biometric signatures for user authentication. Initially, a user will sign his or her name a few times, creating a signature recognition template. This template is encrypted using technologies such as Triple DES and stored on the device. When the user later signs his or her name during logon, the signature is compared against the template stored on the device for authentication purposes.

  Communication Intelligence Corporation (CIC) (**www.cic.com**) provides a product called Sign-On, which incorporates CIC's patented biometric signature technology called SigCheck. This product uses a collection of biometric data of the signatory -- dynamic characteristics such as pen velocity, acceleration, stroke sequence, and muscle memory -- to create a highly secure means of confirming the user's identity and guarding against signature forgeries. All signature data and templates stored on the device are encrypted using Triple DES. Documents and records secured using CIC's technology enjoy both legal (under the U.S. E-SIGN bill) and FDA (Food and Drug Administration) acceptability. For example, pharmaceutical companies can use CIC's technology to secure and sign clinical drug trial documents in compliance with FDA regulations.

- **Biometric Authentication**
  Biometrics involves using some aspect of the human body -- fingerprints, retinal scans or DNA -- to authenticate a person. Because these biological attributes are unique to each person, they can be used to identify an individual definitively. Applied Biometrics Product Inc. (**www.appliedbiometrics.net**) provides a very secure authentication solution for devices by using the handheld user's fingerprints for authentication. Applied Biometrics's custom algorithms transform a visual fingerprint image into a mathematical template representing the user's fingerprint. This template is stored on the device and compared with the active user's fingerprint during the logon process. This stored template cannot be reconverted into the original fingerprint image, providing an extremely secure solution as it is virtually impossible to forge a user's fingerprints.

7. References

1 Recounted by Mark Seiden, security expert and Director of Security for Security Labs, May 2001.

- RSA Security's official guide to Cryptography – ISBN 007213139X
- Applied Cryptography – ISBN 0471117099

- www.microsoft.com
- www.proxim.com
- www.lucent.com
- www.cisco.com
- www.slashdot.com
- www.dell.com
- www.hut.fi/~jtlaine2/wtls/
- www.cic.com
- www.appliedbiometrics.com
- www.certicom.com
- www.rsasecurity.com
- www.blackberry.net

Trademarks