Bulletproof Wireless Security : GSM, UMTS, 802.11, and Ad Hoc Security



* **Author:** Chandra, Praphul
* **Date:** 2005
* [Detailed Record](http://eds.b.ebscohost.com.libproxy.chapman.edu/eds/detail/detail/bmxlYmtfXzEzMDI0MF9fQU41?sid=3dc29e48-946c-456a-b712-c3bcd3680378@sessionmgr101&vid=0)

Denial of Service (DoS) attacks in the resent past have exploited weaknesses in network security protocols to completely bring down servers and networks, thus brining this problem into the security domain.

T summarize, a secure communication network provides the following facilities to its users:

 Confidentiality: The non-occurrence of the unauthorized discloser of information. No one except the sender and the receiver should have access to the information being exchanged.

 Integrity: The non-occurrence of the unauthorized manipulation of information. No one except the sender and the receiver should be able to modify the information being exchanged.

 Authentication: The receiver’s ability to ascertain the origin of a message. An intruder should not be able to masquerade as someone else.

 Nonrepudiation: The receiver’s ability to prove that the sender did in fact send a given message. The sender should not be able to falsely deny later that he sent a message.

 Service Reliability: The ability to protect the communication session against denial of service attacks

Note.. If the message is encrypted, an intruder may have access to the data being sent but does not have access to the “information” being sent. In this case, an intruder may still be able to modify the data, leading to a modification in the information.

Cryptography is the art and science of keeping messages secure.

The process of converting plain text messages in cipher text is called encryption.

The secret method of encryption and decryption is call an algorithm/cipher.

Practical limitation for this methodology include, a predetermined algorithm, there must be a separate algorithm for each customer.

When a cipher uses a key to encrypt and decrypt messages, the secret to be shared moves from the algorithm to a number (key).

* Keys need to be distributed in secret, since the security of the system lies in the secrecy of the keys. Since there is no inherent support for key distribution, keys are usually distributed by some other means (like couriers, for example). This means that the system is as secure as the courier, Furthermore, key distribution can be a daunting task for large networks like the Internet.
* Once the key is stolen, the whole security system breaks down—there is no graceful death.
* Assuming a separate key is used for each pair of nodes, the total number of keys required for an n-node network is n(n-1)/2. (eq for an polygon?) This quantity grows dramatically with increasing n.

Symmetrical is two way decryption where both sender and receiver need the key(SKC)

In Asymmetrical Communication is one way and uses a mathematical trapdoor idea. It is near impossible to find a function f(x) just given x. However, as long as you know F(x), or the equation that equals y it is very easy. Asymmetric key cryptography is also called Public Key Cryptography (PKC) since either the encryption key or the decryption key may be made public depending on whether you need confidentiality or nonrepudiation. PKC’s strength is that the fact that it can be carried out In the unsecure channel does not compromise the security of the system.

F(x) ----x easy, x----f(x) very hard, f(x) + Y ---- x easy.

A hybrid is a cryptography that uses PKC or key distribution but SKC for message encryption. This the much slower cryptography PKC distributes a new key on a per communication basis, then actual messaging uses that same key during the communication as SKC, which is much faster. Thus there is a distinct new key for every session. This achieve confidentiality in both direction automatically.

Integrity. Security is taken out of the hands of the people and is automatic.

How does cryptography satisfy the integrity requirement of a communication network? For the receiver the ensure that the message sent by the source has not been modified or tampered with, cryptography exploits one-way hash functions. These are one way functions with the additional property that they take an input of variable length but produce an output of fixed and much shorter length. For cryptography, there are two desirable features in one-way hash functions. First, a small change in the the message should produce a large change in the hash of the message. This means one small change renders the entire message invalid.

Today just using a user name and password are not sufficient for security. Encryption, challenge and response, and other types of security are needed. When connections or Items should only be made once we can include a including a timestamp in the message, hash the message and encrypt it with its private key. Basically, the authentication mechanism spreads its scopr to include a timestamp in the digital signature. One check, One digital signature.

Firewalls,

 Firewalls have become an integral part of network security today. Ideally, every node which connects to the network should be responsible for its own security. In most cases, however, it is not only easier but also more secure to isolate your Local Area Network. From the Internet. A firewall is basically a se of Hardwar and / or software that isolates a LAN from the rest of the Internet. Firewalls exist because nodes are usually unwilling or incapable of protecting themselves. Most Computers are sold with a whole bunch of unsecure applications, due to programming bugs, features that override existing security measures. Web servers and other computers that have high traffic find protection difficult. Placing a web server inside the firewall means that if the web server is compromised, it can then be used as a launching pad for attackes on other hosts in the LAN. The typical solution for this problem involves the use of two or more firewalls. The demilitarized Zone is a region between the internal firewall and te external firewall.

Defense against DoS where a server is over whelmed by denighing service. This can bring down a server. Protection works by having multiple resourses where one is needed. If one is brought down then other is still active.

Network Security Protocols

The three areas of security; authentication, encryption, and message integrity can be overcome by Cryptography.

For SKC or Symmetric Key Cryptography, the tern key establishment can be clearly broken down into two components. Key generation and key distribution. For Public Key Cryptography (PKC), however, the term key establishment is a little more complicated. In the case of two users communication with each other over an unsecure channel, the use of PKC key establishment protocols results in both users establishing the public-private key pair. Specifically, when the PKC establishment protocol ends, each user has a private key, known only to themselves. Which has never been transmitted onto the medium and public key.

Trusted Certificate Authority. A third party that takes any middle man attack out and provides SSl encryption keys to the sender, and vouches for them with all users while provided decryption keys unique to them.

RSA

 The DH public key algorithm above is the oldest key establishment protocol still in use today. Another important (an more recent) key establishment protocol is the Rives Shamir Adelman (RSA) protocol. Which is based on the difficulty of factory the product of two large primes. However, RSA is a much more generic and powerful protocol. Because it can be used for encryption and integrity(digital signatures) also. This system power is the fact that it is based on prime numbers, not just any prime numbers but ones that have a bit length of 256 or more. While it may be easy to find lower prime numbers, those with a bit length of 256 are extremely difficult. For this reason RSA uses “probable prime” numbers. Basically these are numbers found using Fermat’s Little Theorem. Fermat wrote in the margin of a book that the more general equation *a*n + *b*n = *c*n had no solutions in positive integers, so basically the primes RSA uses basically cannot found by using the formula *a*n + *b*n = *c*n . However, RSA algorithm too would suffer from the man-in-the-middle attack if used per se. To circumvent this loophole, the RSA algorithm is used with PKI where the public keys of all communication parties are stored at the central trusted certificate authority.

Authentication Protocols

 The term Authentication refers to the process of verifying that a node or user is who they claim to be. One of the primary uses of authentication in networking is to implement access control reliably. Controlling access to the network is one of the primary defense mechanisms in network security. If you allow only people you trust to access the network, you have an inherent protection built into the system. Authentication implements access control by securely identifying users or nodes trying to access the network.

Address-Based Authentication

 For any network to be able to route messages, calls or packets, it is imperative that each node in the network be assigned a unique address. The format of this address depends on the routing protocol being used in the network. Given that each node has an address, a first-step approach to controlling access into the network in to allow only a predetermind set of addresses to access the network. In other words, this approach authenticates the use or node on its address.

At the point, it is important to distinguish between a use and a node, A user is a human, whereas a node is the machine the use is using to connect to the network. The address used for this approach usually rrefers to the address of the node. In IP networks, for example, this address may be the message authentication code (MAC) address. Media Access Control address. Or the IP address. So , an address-based authentication scheme in an IP network may be implemented by the switch or router allowing only a preconfigured set of MAC or IP addresses to access the network.

The loopholes are based on the fact that the assumpti0ns that the scheme makes are easy to violate. First, it assumes that there is a st5rict one-to-one relationship between a user and a node. This may not be true where a single node is used by multiple users or where a single user can use multiple nodes. This means that authenticating a node based on its MAC address does not really authenticate the user.

Another weakness of this is Spoofing a MAC address. This may be a little more difficult since some network access devises now have a build in mechanism to protect against such alterations, but most do not. Spoofing an IP address ion the other hand is almost trivial since IP-address discovery uses address resolution protocol (ARP), which works on an inherent assumption of trust on all nodes in the local area network (LAN).

Although address-based authentication is not sufficient by itself, it forms a good additional obstacle or deterrent when used along with other access control mechanisms like authentication protocols.

Passwords for Local Authentication (Login)

System wide policies that limit the number of simultaneous connections to one account will limit reflection attacks.

Lambers hash pg 46

The drawbacks of Labports hash are that there is no mutual authentication and the user can only login a finite number of times before reconfiguration.

Authentication using PKC pg 48

SKC has the abvious advantage that it is much less computations intensive. This feature not only makes it much more “cheaper” and “lighter” but also makes it more resilient to DoS attacks. However, there are two major drawback to using SKC for authentication. First note that Bob needs to store the keys of all users that wich to talk to him in a database, or the system needs to employ a KDC as the central repository of all keys. In either case if the key database is commprimised, the security of the whole system is compromised. Compare this to the PKC approach where the CA stors only the public key of allusers and the access to tht CA database does not itself break the security of the system. The second drawback of using the SKC for authentication is that it allows One to collect <plaintext, ciphertext> pairs encrypted with the chared secret. One can do this b y claiming to be a user and sending the plaintext as a challenge to the Server. The Server would then respon with the encrypted challenge. The collected <plaintext, ciphertext> pairs database may then be used for dictionary attacks.

Disadvantages to PKC is a computationally intensive exersize makin it a much less attractive option especially for protable devices which have limited computing power. Another problem which stems from this is that PKC usually makes the syustme much more stateful, making it more vulnerable to DoS attacks.

Hijacking pg 49

Kerberos protocall, what I will use. pg52

AES algorithm is 128bit

RC4 is a stream ciper one bit at atime.

* Ubuntu uses **XTS** is counter-oriented chaining mode. It's an evolution of XEX (actually: "XEX-based tweaked-codebook mode with ciphertext stealing"), while XEX ("xor-encrypt-xor") is a non-trivial counter-based chaining mode; neither of which I can claim to completely understand. XTS is already very widely supported and looks promising, but [may have issues](https://en.wikipedia.org/wiki/Disk_encryption_theory#XTS_weaknesses). The primary important details are these: No fancy IVs are necessary (plain or plain64 is fine), and half of your key is used by XTS, meaning your original key must be twice as long (hence 512-bit instead of 256-bit).

Layer 2 Security level

Remote Dial in pg 70

EAP-TLS protocols

Layer 3 security level.

Layer 2 connects to the LAN Layer 3 connects to the Server.