Authentication and Privacy

Thomas M. Chen
Department of Electrical Engineering, Southern Methodist University, Dallas, Texas, USA

Nhut Nguyen
Network Systems Lab, Samsung Telecommunications America, Richardson, Texas, USA

Abstract
Authentication and privacy refer to the problems of ensuring that communication takes place only between the right parties without disclosure of information to unauthorized eavesdroppers.

Radio communication is highly appealing for the convenience of mobility—the freedom from a fixed location. For this reason, wireless services have been growing rapidly. In 2005, an ITU study found more than 2 billion cellular phone subscribers and more than 1.26 billion land phone lines in the world. It has become easy to find IEEE 802.11 wireless LANs in residences, hotels, stores, and corporate sites. Smart phones and a variety of wireless messaging devices can send SMS, e-mail, and browse the World Wide Web through a number of wireless services. IEEE 802.16 "WiMax" is starting to offer broadband wireless services in the local loop.

The enthusiasm for wireless services makes it easy to ignore the inherent insecurity of the radio medium. The most obvious risk is that radio signals can be received by anyone within range of the transmitter. Radio communications are easy to intercept, possibly by someone who is beyond sight. In contrast, it is more difficult to intercept wired communications. An eavesdropper must physically access a wired medium and therefore tends to be more visible. In wireless communications, the loss of privacy (or confidentiality) is always a possibility, which motivates the need to devise measures to protect privacy. The primary means used to protect privacy in wireless systems is cryptography, which is described in this chapter.

Another clear risk is impersonation where someone presents a false identity to attempt to access unauthorized services. For land line phones, impersonation is a much smaller risk because phones are typically in an indoor environment under private ownership. It is implicitly assumed that the owner is responsible for physical access. The identity of a land line phone user is associated with that fixed location. However, users in a wireless network are mobile, so their identities cannot be associated with a particular location. Instead, mobile users must carry their credentials (e.g., passwords) and present them to the network to verify their identity. It is important that authentication credentials are difficult to duplicate by someone else. Authentication of mobile user identities, also largely based on cryptography, is another topic covered in this chapter.

CRYPTOGRAPHY BASICS

Owing to the nature of radio signals, it is not feasible to prevent eavesdropping. It must be assumed that any radio transmission might be overheard by an unwanted third party. Encryption is a mathematical process for transforming the original data (called plaintext) into a form (ciphertext) that makes sense only to the intended receiver but not to an eavesdropper. Traditionally, cryptography is done on the basis of secret keys shared by both parties, which is the reason it is called symmetric cryptography. In the 1970s, a different approach called asymmetric cryptography was invented where the transmitter uses a public key and the receiver uses a secret key.

In symmetric cryptography, the secret key known only to the transmitter and receiver is used for both encryption and decryption (Fig. 1).[1] It is usually assumed that an eavesdropper may have knowledge of the encryption (and the reverse decryption) algorithm, and publicly known encryption algorithms are often used. Thus, the strength of the system depends on the difficulty for an eavesdropper to discover the key. Cryptanalysis refers to the process of breaking a cipher by discovering the secret key or the original plaintext (or both), based on at least observations of the ciphertext. Hence, strong encryption algorithms should leave no statistical structure in the ciphertext that could give clues about the plaintext or encryption key. In addition, strong algorithms should be resistant to brute force attacks where every possible key is tried. Therefore, longer encryption keys are better than short ones because it means a brute force attack must go through a larger number of possible keys. For example, doubling the key length from n to $2n$ bits would mean an increase from 2^n possible keys to $(2^n)^2$ possible keys.

Encyclopedia of Wireless and Mobile Communications DOI: 10.1081/E-EWMC-120043167

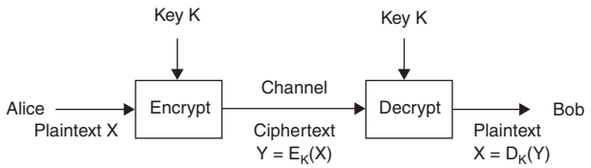

Fig. 1 Symmetric or secret key cryptography.

A large number of encryption algorithms are known, but among the most widely used is the DES adopted by the U.S. Government in 1976.[2] It was based on an earlier Lucifer algorithm developed by IBM. DES encrypts plaintext as separate 64-bit blocks using a 56-bit key. Basically, blocks go through 16 cycles, each cycle performing substitution and permutation operations. Each cycle can be viewed as "scrambling" the text more. Although the logical operations in each cycle are similar, each cycle depends on a different 48-bit subkey derived from the 56-bit key.

In 2001, the U.S. Government adopted Rijndael as the AES, replacing DES.[3] It operates on data blocks of 128 bits. There are 9, 11, or 13 cycles for keys of 128, 192, and 256 bits. Each cycle or "round" involves substitution, shift, mixing, and XOR (exclusive or) operations. Although the logical operations are identical in each cycle, each cycle depends on a different subkey derived from the key.

A common problem for all symmetric key encryption algorithms is the need for every pair of communicating parties to share a secret key, protected against eavesdropping, before they have a secure channel. Surprisingly, there is a protocol invented by Diffie and Hellman (called the Diffie–Hellman key exchange) that allows two parties to share a secret number confidentially over an unsecure channel.[4] Alternatively, all parties could share secret keys with a trusted third-party key distribution center. When two parties need to communicate, they can both fetch a secret key securely from the key distribution center to use for the duration of their session. However, this scheme does not scale well with the number of users. As the population increases, the number of keys needed will increase exponentially, and the load on a key distribution center will grow similarly.

In 1976, Diffie and Hellman proposed public key or asymmetric cryptography (Fig. 2).[4] In public key cryptography, each party knows their own private key, and there is no need to share this key with anyone else. Everyone knows their public key, but the relationship between the public and private keys is designed to make it computationally difficult to discover the private key from the public key. Anyone can encrypt a message with the recipient's public key, and only the recipient with the private key can decrypt the message.

In 1977, RSA was the first practical public key cryptosystem invented by Rivest, Shamir, and Adelman, later patented in 1983.[5] The security of RSA basically depends on the difficulty of factoring a very large number into two prime numbers.

A public key cryptosystem such as RSA comes in handy for digital signatures. A digital signature attached to a message serves the same purpose as a handwritten signature on a physical document. It verifies the originator of the message. This is possible because RSA happens to have the property that the public and private keys are interchangeable. Thus, a digital signature could be created if Alice encrypts a message with her private key, and attaches this signature to the message (Fig. 3). Bob can decrypt the signature with Alice's public key, and compare the decrypted message with the received message. A match would imply that the signature could have come only from Alice because only Alice has the private key corresponding to her public key. It also verifies that the message was not modified during transmission. In practice, digital signatures are produced in a more efficient way using a hash function such as MD5 to produce a hash or message digest of the message first before encryption. A message could be very long, whereas a message digest is a short fixed length, so it is much more efficient to encrypt a message digest. The recipient can decrypt the digital signature to recover the message digest. This is compared with a hash of the received message. A match implies that the message was not altered and came from the sender.

An association between users and their public keys is often handled by certificates. A certificate is essentially a digital document binding a user's identity and public key together, verified by a digital signature of a trusted third party called a certificate authority.

Finally, secret keys are useful in authentication protocols. Suppose that two parties want to verify each other's identity, and they share a secret key. Each party

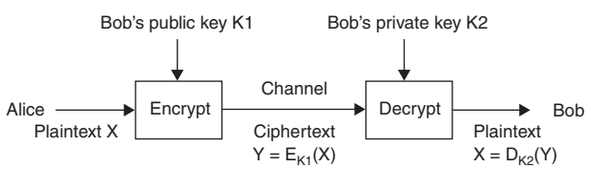

Fig. 2 Asymmetric or public key cryptography.

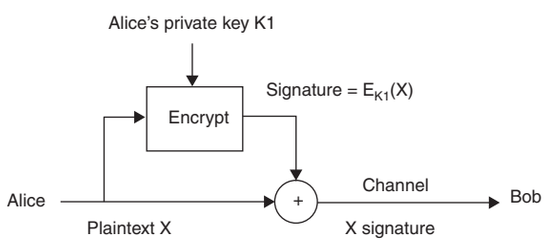

Fig. 3 A digital signature.

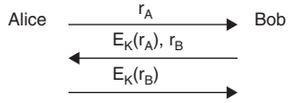

Fig. 4 Challenge-response authentication with a shared secret key.

can prove its identity by demonstrating possession of the secret key, without revealing the secret key itself (which could then be stolen), through a basic challenge-response protocol (Fig. 4). Alice issues an unpredictable (random) challenge to Bob. Bob demonstrates his knowledge of the secret key by encrypting the challenge. Bob can verify the identity of Alice in the same way with another challenge.

This protocol works with public keys as well (Fig. 5). Alice generates a challenge and encrypts it with Bob's public key K1. Bob can decrypt it with his private key and then encrypt the challenge with Alice's public key K2. Alice can decrypt this to recover the original challenge, which verifies the identity of Bob because only Bob could have decrypted the first message. Obviously, Bob can authenticate the identity of Alice similarly with a separate challenge.

PRIVACY AND AUTHENTICATION IN IEEE 802.11 WIRELESS LANs

IEEE 802.11 wireless LANs have been commercially successful. Approved in 1999, IEEE 802.11a specifies 25–54 Mbps data rate in the 5 GHz band, and 802.11b specifies 6–11 Mbps data rate in the 2.4 GHz band. Another flavor 802.11g backward compatible with 802.11b, but with data rate increased to 25–54 Mbps, was approved in 2003. Currently, an 802.11n standard is being drafted for data rate of 200–540 Mbps.

Security has been a longstanding weakness of 802.11 wireless LANs. Traditionally, authentication and privacy have depended on preshared secret keys. Security has been recognized as an important problem and there are ongoing efforts to improve the standards.

Authentication

IEEE 802.11 specifies two types of authentication: open system authentication (OSA) and shared key authentication (SKA). A host first learns the name or service set identifier of networks within its range. After choosing a network to join, it issues an authentication request message specifying the authentication scheme. The access point can accept or reject the requested authentication scheme in its response.

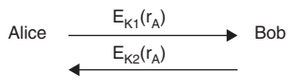

Fig. 5 Challenge-response with public keys.

By default, an access point uses OSA which essentially provides no authentication of hosts. In SKA, authentication depends on a host knowing a preshared secret key (the method of exchanging secret keys is not specified in 802.11). Knowledge of the secret key is demonstrated through a challenge-response protocol (Fig. 4). The access point sends a random 128-bit challenge to the host. The host encrypts the challenge using wired equivalent privacy (WEP) (discussed below) with the secret key and an initialization vector (IV) of its choosing. The host sends the encrypted challenge and IV to the access point for decryption. If the access point can recover the secret key, it verifies that the host knows the secret key and allows access to the wireless LAN.

Problems with the authentication protocol are known. In actuality, the challenge-response protocol verifies only that the host is one in a group of hosts who all know the same key. The 802.11 does not specify a way for hosts to obtain unique secret keys. Thus, an access point cannot authenticate the exact identity of a host. Also, authentication is unidirectional; there is no provision for hosts to verify the identity of an access point.

Privacy

The original security scheme included in IEEE 802.11 wireless LAN standards was WEP, approved in 1999. It was recognized that wireless networks are inherently vulnerable to eavesdropping. WEP was intended to provide privacy comparable to traditional LANs using the RC4 algorithm to encrypt data packets sent out from an access point or wireless network card. RC4 is a stream cipher that generates a pseudorandom bitstream called a keystream which is combined with the plaintext using bit-by-bit XOR to produce the ciphertext. The keystream must be pseudorandom because the decryptor generates the same keystream to XOR with the ciphertext to recover the plaintext.

In WEP, the RC4 cipher uses a seed constructed from a secret key (preshared password) and a 24-bit IV to encrypt each packet. The IV prevents repetition in the keystream from packet to packet when the same secret key is used. The IV is prepended to each packet and sent in plaintext to synchronize the decryptor at the receiving host. Unfortunately, the 24-bit IV length means that there is a 50% chance of seeing a repeated IV after 5000 packets. In 2001, it was shown that a passive eavesdropper could recover the RC4 key after observing a sufficient amount of traffic (a few million frames). Alternatively, an attacker could send packets on the wireless LAN to stimulate reply packets. These attacks were implemented in software such as Aircrack and WEPCrack. By 2003, a number of shortcomings in WEP were widely recognized.

An interim replacement for WEP called Wi-Fi protected access (WPA) was published by the Wi-Fi Alliance and deployed commercially in 2003. IEEE 802.11i, also known as WPA2, was approved in 2004. The key establishment procedure and authentication are the same in WPA and WPA2. These depend on another standard IEEE 802.1X and an authentication server to share a secret 256-bit pairwise master key (PMK). In the first step, the access point asks for identification information from the host, such as user name and MAC address. The access point receives this information and forward it to the authentication server. The authentication server can use any number of authentication protocols to verify the identity of the host. During the authentication process, the access point simply passes messages between the host and authentication server.

After a PMK is established between a host and access point, the PMK is used to derive 128-bit pairwise transient keys (PTKs). There are four PTKs which are mixed by an algorithm, along with MAC addresses and nonces from the host and access point, to finally generate per-packet encryption keys. Different from WEP, packets are encrypted by AES used in counter mode.

PRIVACY AND AUTHENTICATION IN IEEE 802.16 WIRELESS METROPOLITAN AREA NETWORKS (WIMAX AND MOBILE WIMAX)

Privacy and authentication in WiMax and mobile WiMax networks are protected by the privacy sub-layer of the MAC layer in the protocol stack.[6] The privacy sub-layer in the 802.16 protocol stack defines security procedures that use X.509 certificates as the main mechanism for subscriber stations (SSs) authentication and other cryptography based security functions.[7]

Privacy

Symmetric encryption is used to protect privacy of data exchanged between an SS and a base station (BS). Messages are encrypted using traffic encryption keys (TEKs) generated by the BS and sent to the SS using the privacy and key management (PKM) protocol. PKM exchanges are authenticated using the HMAC-SHA1 algorithm. Traffic encryption keys are encrypted using the 3DES encryption algorithm. Keying information to protect PKM exchanges are derived from a shared authentication key (AK) established between the SS and the BS using public key cryptography as part of the authorization process.

In WiMax standards, the cryptographic algorithm specified for message encryption is DES with cipher block chaining (DES-CBC). Mobile WiMax enhances encryption strength with the introduction of the AES in Counter with CBC-MAC (AES-CCM) algorithm.

Authentication

The BS authenticates an SS using the PKM with SS's certificate as credential and as part of the authorization process. In the early 802.16 standards, the SS did not authenticate the BS. The authorization process starts when the SS sends an Authentication Information message (informative) and then an Authorization Request message to the BS. The Authorization Request message includes the X.509 certificate of the SS along with other security information. The BS verifies the certificate to decide if the SS is authorized to access network resources and then uses the public key contained in the certificate to establish and encrypt an authorization key (AK) using the RSA algorithm. The encrypted AK is sent back to the SS along with other security information. The correct use of the AK to derive other keying information (e.g., the key encryption keys, used to encrypt the TEKs) establishes the authenticated identity of the SS to the BS.

The privacy sub-layer of the early 802.16 standards has a few deficiencies, noticeably the lack of BS authentication, and the cryptographically weak 56-bit keys based DES algorithm that is used for message encryption. These deficiencies were addressed in the newer 802.16e (mobile WiMax) standards with the PKMv2 protocol which includes the extensive authentication protocol (EAP) based mutual authentication and stronger encryption algorithms such as AES.[6]

PRIVACY AND AUTHENTICATION IN GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS NETWORKS

Privacy

In a GSM network, the main mechanisms used to protect privacy are cryptography-based ciphering and temporary identity information.[8]

Ciphering

To protect the privacy of signaling and media information being transmitted over the air interface, a symmetric ciphering process is used. This privacy protection mechanism is active when the ciphering feature for a mobile subscriber is activated by the network.

The network uses a random number RAND and the subscriber specific secret key Ki to generate a ciphering key Kc using the cryptographic A8 algorithm. Each subscriber is assigned a unique secret key Ki that is stored both in the SIM card attached to a mobile station (MS) and in the authentication center (AuC) of the network. The random number RAND is then sent to the MS.

The MS uses the received random number RAND and the subscriber specific secret key Ki stored in the SIM card

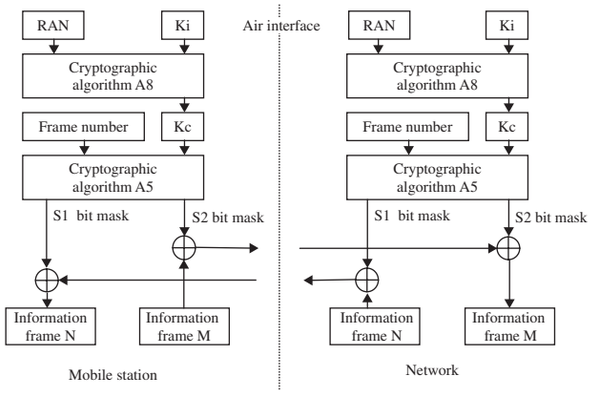

Fig. 6 Ciphering for privacy in GSM networks.

to generate a ciphering key Kc using the same cryptographic A8 algorithm. Note that since the inputs (Ki and RAND) and the key generation algorithm (A8) are the same, the generated ciphering key Kc is identical on both the MS and the network (hence symmetric ciphering.)

The generated ciphering key Kc and the frame number of the information frame being transmitted over the air interface are used as input to the ciphering algorithm A5 to generate an encryption bit mask S2. The length of the bit mask is the same as information frame length.

The MS encrypts the information frame to be transmitted by XOR'ing the information frame with the bit mask S2 before sending it out on the air interface.

On the receiving end (the network), a decryption bit mask S2 is generated using the same inputs (Kc and frame number) and cryptographic algorithm A5. As the inputs and the algorithm are the same, the bit masks generated by the MS and the network are identical.

The network decrypts the received frame by XOR'ing it with the decryption bit mask S2 to get the original information frame.

The same process is used on the reverse direction, i.e., the network encrypts and the MS decrypts, but with a different bit masks S1. The bit mask S1 is generated using the same A5 algorithm with the frame number and the ciphering key Kc as the inputs (Fig. 6).

Temporary identify information

To further protect the privacy of subscriber identity, a security mechanism that utilizes temporary identity information is used.

Upon successful registration to the network, a subscriber is assigned a temporary international mobile identification (TMSI) by the visitors location register (VLR) of the serving network. In subsequent transactions between the MS and the serving network, the subscriber is identified by this TMSI instead of the permanent and private international mobile station identification (IMSI). The mapping between a TMSI and the IMSI of a subscriber is known and valid only in the serving network. An attacker who captures TMSI information that is exchanged over the air interface cannot derive the subscriber's identity from TMSI information.

AUTHENTICATION

Authentication of a mobile subscriber in a GSM network is performed using a challenge-response protocol.[8]

The network sends a random number RAND as a challenge to the MS. The MS uses the received random number RAND and the secret key Ki stored in the SIM card as input to the cryptographic algorithm A3 to generate an authentication response (AUTHR) and sends it back to the network.

The network compares the received response with the expected response (SRES) for the challenge RAND. The expected response was generated using the same cryptographic algorithm A3 and the same random number RAND sent to the MS.

If the received response matches with the expected response, the MS is authenticated and the network allows the MS to proceed. Otherwise, the authentication process fails and the MS requests are rejected by the network.

Generating the random number RAND, the ciphering key Kc, and the expected response SRES for many MSs using cryptographic algorithms is time and resource consuming. Thus, generating these values by the network which serves thousands of subscribers in real time is not practical. Instead, a prefabricated approach that utilizes the concept of authentication triplet is used in GSM networks.

An authentication triplet contains the random number RAND, the ciphering key, Kc, and the expected response SRES. In the GSM networks, authentication triplets are generated by a network element named AuC. Physically, the AuC usually co-resides with the home location register (HLR). A subscriber record in a HLR/AuC may contain a number of pre-calculated authentication triplets to be used for that subscriber.

The network, specifically the MSC/VLR, uses one authentication triplet for each authentication procedure and the subsequent encryption of the session. When the network authenticates a mobile subscriber, an authentication triplet must be retrieved from the HLR/AuC by the MSC/VLR and used. To reduce traffic between network elements, authentication triplets are usually retrieved by the MSC/VLR in bulk in advance. Also, if the MSC/VLR detects that the number of triplets for a subscriber is below a set threshold, it can initiate a procedure to contact the HLR to replenish the authentication triplets so that it does not have to contact the HRL/AuC when it needs to authenticate the mobile subscriber.

Note that the authentication process described above is a one-way authentication only. During the authentication process, only the mobile subscriber is authenticated by the network but the network is not authenticated by the mobile subscriber.

PRIVACY AND AUTHENTICATION IN SECOND GENERATION CODE DIVISION MULTIPLE ACCESS NETWORKS

Privacy and authentication procedures in 2G CDMA networks are based on the cellular authentication and voice encryption (CAVE) algorithm and are specified in the Interim Standard-41 (IS-41) standards of the TIA.[9]

Privacy

With CDMA technology, information to be transmitted over the air interface is spread out using a pseudo-noise (PN) code. As all users use the same radio frequency spectrum over the air interface in CDMA networks, this code is needed to identify a particular pair of users of the radio frequency spectrum. Thus, the CDMA technology has an inherent privacy mechanism built-in: the receiver can only get the transmitted information if it knows the code used to spread the original information.

However, if the spreading code is based solely on public information that a perpetrator can get a hold of, this advantage may disappear. Anyone who knows the code can monitor the air interface and decode the transmitted information with the right equipment.

In CDMA networks, privacy of information transmitted over the air interface is protected by combining the built-in privacy mechanism of the CDMA technology with the use of cryptographic algorithms and encryption.[9]

Voice privacy

Voice privacy in CDMA networks is protected using a secret private long code mask (PLCM). A PLCM is derived from an intermediate value named voice privacy mask (VPM) which is generated using the CAVE and secondary key information called shared secret data (SSD). The SSD itself is also generated using the CAVE algorithm and a secret primary key name A-key which is known only to the MS and the AuC in the network. An SSD is a 128-bit long integer value whose first haft (SSD_A) is used for authentication and the second half (SSD_B) is used for privacy protection.

The voice privacy feature of CMDA network can be activated or deactivated. If voice privacy is activated, a PC lifecycle management (PLCM) is used to change the characteristics of the spreading code used to spread a voice information before being transmitted over the air interface. Transmitted voice information is scrambled with a secret PCLM which is used to alter the characteristics of the spreading code. Unless the PCLM (which itself is a secret) and the method to alter the characteristics of the spreading code is known, it is extremely difficult to de-spread a signal transmitted over the CDMA air interface to obtain the original voice information.

Signaling privacy

To protect signaling privacy (e.g., to whom a person is calling), the symmetric encryption process is used to encrypt signaling messages. An encryption key named cellular message encryption algorithm (CMEA) is generated by both the MS and the network using a common SSD_B value as input to the CAVE algorithm. The signaling messages are then encrypted and decrypted by the MS and the network using this CMEA key and the CMEA encryption algorithm.

A TMSI is also used to further protect subscriber identity in CDMA networks in a similar manner as in GSM networks. A TMSI is assigned to the MS after a successful authentication and is used in subsequent transactions between the MS and the network to conceal the identity of a subscriber.

Authentication

The challenge-response process and cryptographic algorithms are used for authentication in CDMA networks. A secondary key SSD_A and a RAND number are fed into the CAVE algorithm to generate both response and expected response.[9]

The network sends the RAND number as the challenge to the MS to be authenticated. The MS feeds the received RAND number and the stored SSD_A value to the CAVE algorithm to generate an AUTHR (18-bits) and sends it to the network as the response. The network uses the same RAND number and the SSD_A value for the MS as input to the CAVE algorithm to compute an expected response. The network then compares the AUTHR received from the MS against the computed expected response to determine the authenticity of the subscriber.

There are two procedures available to the network for authentication purposes: global challenge and unique challenge. With global challenge, all MSs are challenged with the same RAND number which is broadcasted over a broadcast channel. In the unique challenge procedure, a specific RAND number is used for each MS that is requesting access.

For additional security, the network may also use a call history COUNT register. The COUNT register is a 6-bit counter that counts the times the MS has made calls and is maintained in both the MS and the network. To be authenticated, the value of the COUNT register in the MS must match with that of the COUNT register for the MS maintained in the network.

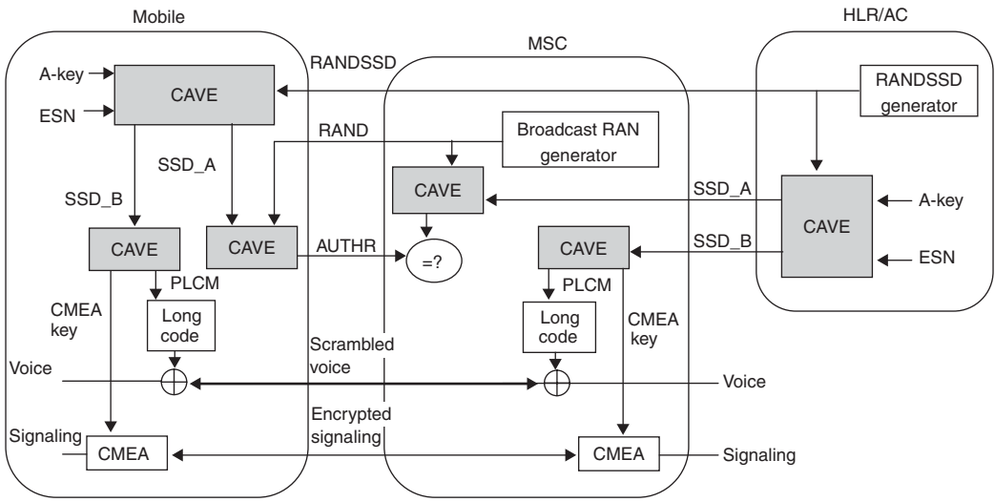

Fig. 7 Authentication and privacy in second generation code division multiple access networks.

As described above, privacy and authentication mechanisms used in CDMA networks rely on secondary key information SSD which is derived from the primary key A-key using the CAVE algorithm. To keep SSD information in the MS and the network in sync and to provide further security by changing the common secondary key information SSD, the network may initiate an SSD update procedure to change the SSD value on the MS. The network sends a RANDSSD number to the MS to start the SSD update procedure. The MS uses the received RANDSSD number, its equipment serial number (ESN), and the primary key A-key as inputs to the CAVE algorithm to generate a new SSD value. To prevent illegal SSD updates by a rogue base transceiver station (BTS), the MS authenticates the network before updating SSD with the new value. The MS sends a RANDBS number to the network as a challenge. The network uses this RANDBS to calculate an AUTHBS response to the challenge and sends it back to the MS. The MS verifies the received response to authenticate the network. It updates the SSD with the new SSD value only if it has successfully authenticated the network (Fig. 7).

PRIVACY AND AUTHENTICATION IN THIRD GENERATION NETWORKS

3G mobile networks are based upon specifications developed by either the third generation partner project (3GPP) or the third generation partner project 2 (3GPP2) standardization bodies.

3GPP Based 3G Networks

The 3GPP standards define the operation of 3G networks using the wideband CDMA (WCDMA) technology for radio access networks (RANs). For core networks, GSM based standards specifies circuit switching (CS) domain operations whereas general packet radio service (GPRS) based standards specifies packet switching (PS) domain operations. In newer releases of the specifications the Internet protocol (IP) multimedia subsystem (IMS) which is totally IP based is specified for the core network operations.

Privacy and authentication mechanisms in the 3GPP based networks are largely based on security mechanisms developed in GSM standards but with many enhancements to address the identified shortcomings, noticeably the lack of mutual authentication, of GSM networks.

3GPP2 Based 3G Networks

The 3GPP2 took an evolutionary approach toward 3G networks. The core network and the RAN respectively evolve from the IS-41 and the IS-95 specifications of the 2G CDMA networks. The 3GPP2 defines the specifications IS-2000 which specify the operations of CDMA2000 1xRTT (radio transmission technology) and 3xRTT networks in revisions 0, A and B. The 1xRTT specifications are then further evolved into two 3G specifications: the CDMA2000 1xEV-DO (evolution—data only) standards specified by IS-856/3GPP2 C.S0024) defines the enhancement for data applications only while the CDMA2000 1xEV-DV (EV—data and voice) standards (defined in IS-2000/3GPP2 C.S001-0005 revision C) specifies enhancement for both data and voice applications.

The privacy and authentication mechanisms used in these 3GPP2 networks are largely based on an enhanced version of the ones used in the IS-41 standards, but newer releases of the specifications are adopting the mechanisms used in 3GPP based 3G networks.

Privacy

3GPP networks

In the 3GPP networks, the privacy of information exchanged between a mobile subscriber and the network over the open air interface is also protected by using a symmetric encryption process.

User voice traffic and certain signaling messages in dedicated wireless channels are protected with symmetric encryption using the UMTS encryption algorithm (UEA) with the session encryption key CK, or cipher key, established during the authentication and key agreement (AKA) procedure described below. The algorithm also makes use of other information such as the sequence number COUNT-C, the 1-bit direction information DIRECTION, the length of the keystream LENGTH, and the radio bearer identification BEARER as inputs to the f8 ciphering algorithm to further protect the privacy of exchanged information.[10]

For user data traffic, the encryption procedures are setup by an IP based security protocol. As of Release 7 of the 3GPP specifications, the IP security (IPSec) protocol is used as the main protocol for privacy protection of data traffic in 3G networks. After a successful AKA procedure, the identity module of the mobile subscriber uses the agreed upon session key for encryption (CK) and the session key for integrity verification (IK, or integrity key) to set up IPSec tunnels with the network. Privacy (as well as integrity) of data exchanged between the mobile subscriber and the network are then protected by these IPSec tunnels using the session keys (CK and IK) and cryptographic algorithms specified by the IPSec standards.[11]

3GPP2 networks

In CDMA2000 1xRTT and 3xRTT networks (i.e., up to Release B of IS-2000 specifications), voice and signaling privacy protection process is similar to the one used in 2G CDMA networks. Symmetric encryption based on the CAVE algorithm is used to encrypt signaling traffic. Voice traffic is scrambled using the PLCM also derived from the CAVE algorithm. The encryption algorithm for signaling traffic encryption is enhanced with the new enhanced CMEA (ECMEA) algorithm. The enhanced subscriber privacy (ESP) requirements are also specified to protect the keys used for privacy protection.[12] Data traffic is protected by a symmetric encryption process that uses the ORYX ciphering algorithm.

In CDMA2000 1xEV-DO networks, the Diffie–Hellman algorithm is used for session encryption keys exchange instead of the CAVE algorithm. The encryption algorithm is also replaced with one that is based on the more secure AESs.

Authentication

3GPP based networks

The authentication method used in 3GPP based 3G networks is mostly an enhanced version of the one in GSM networks. This enhancement addresses one of the biggest security deficiencies in 2G networks: the network is not authenticated by the mobile subscriber during the authentication process. Using enhanced authentication method, mutual authentication between a mobile subscriber and the network is achieved. The 3GPP has specified this enhanced authentication method as part of the AKA protocol to protect communications in 3G networks.[10]

In this method, the home subscriber server (HSS) in a 3G network generates authentication vectors (AVs) which is an enhanced version of the authentication triplets used in GSM networks. The AV (a quintuplet) contains a random challenge RAND, a network authentication token AUTN, the expected response XRES, a session key for integrity check IK, and a session key for encryption CK. To calculate the AUTN, the HSS uses a cryptographic algorithm, with a sequence number SQN that is kept in synch between the HSS and the identity module of the mobile subscriber and the long term secret that it shares with the identity module as inputs. As in GSM networks, the network uses one AV for each authentication procedure.

The authentication process starts when the network sends the random challenge RAND and the network authentication token AUTN to the identity module of the mobile user. The identity module authenticates the network by verifying the received AUTN with the one calculated from the shared long term secret and the sequence number SQN stored in the identity module. If the calculated AUTN and the received AUTN matches, the network is authenticated. In this case, the identity module produces an AUTHR RES using the shared long term secret and a cryptographic algorithm and sends it back to the network.

The network verifies the received response to authenticate the mobile subscriber. If the received AUTHR RES matches with the expected response XRES in the AV, the mobile subscriber is authenticated. The session key for integrity check IK and the session key for encryption CK are then used to establish IPSec tunnels between the mobile user equipment and the network for privacy and integrity protection of communications between the mobile user and the network.[11]

3GPP2 based 3G networks

The AKA procedures for CDMA1xRTT and CDMA3xRTT (i.e., in 3GPP2 specifications revision B and earlier) is based on the CAVE algorithm used in 2G CMDA networks described above.

For enhanced authentication in 3G networks, 3GPP2 defines the requirements for enhanced subscriber authentication (ESA).[12] As the AKA procedures defined by 3GPP specifications met most of these requirements, the 3GPP2 Revision C (CDMA2000 1xEV-DV) specifications adopt the 3GPP AKA described above as the basis for 3GPP2 AKA.

Challenges and Open Research Issues

Wireless networks have difficult security challenges because of two aspects: the openness of radio channels and the mobility of users. There is much security infrastructure in place for authentication and privacy based on well known techniques in symmetric and asymmetric cryptography. Obviously, these security mechanisms are working successfully for the most part today.

One of the major difficulties in all wireless systems is key management. Keys should not be static because keys can be discovered by attackers given enough time. Thus, there is a need to exchange and manage secret keys. While it can be done, exchanging keys over unsecured networks involves risks and complexity.

Some security techniques depend on public keys and a public key infrastructure (PKI) for certificates. It could be said that PKI has been deployed slower than some expectations, and its success is an open question.

SUMMARY

This chapter has covered cryptographic techniques to enable privacy and authentication in the prevalent wireless networks, namely IEEE 802.11 wireless LANs, 802.16 wireless metropolitan area network (MANs), 2G GSM and CDMA cellular networks, and 3G networks. Privacy is typically protected by symmetric encryption. Authentication is a more difficult problem and involves more elaborate procedures in wireless systems.

LINKS

1. IEEE 802 standards, http://standards.ieee.org/getieee802/
2. WiMax forum, http://wimaxforum.org/
3. 3GPP, http://www.3gpp.org/
4. 3GPP2, http://www.3gpp2.org/
5. GSM association, http://www.gsmworld.com/
6. CDMA Development Group, http://www.cdg.org/

REFERENCES

1. Garrett, P. *Making, Breaking Codes: An Introduction to Cryptology*; Prentice Hall: Upper Saddle River, NJ, 2001.
2. NBS (U.S. National Bureau of Standards) Data encryption standard. FIPS Publ. **1977**, 46.
3. NIST (National Institute of Standards and Technology) Specification for the Advanced Encryption Standard AES. FIPS Publ. **2001**, 197.
4. Diffie, W.; Hellman, M. New directions in cryptography. IEEE Trans. Inf. Theory. **1976**, *IT-22*, 644–654.
5. Rivest, R.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM. **1978**, *21* (2), 120–126.
6. IEEE Std. 802.16E-2005, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, Dec 2005.
7. Johnston, D.; Walker, J. Overview of IEEE 802.16 security. IEEE Secur. Priv. **2004**, *2* (3), 40–48.
8. Mouly, M.; Pautet, M.-B. *The GSM System for Mobile Communications*; Cell & Sys: Palaiseau, France, 1992.
9. TIA IS-41D, Cellular Radio Telecommunications Intersystem Operations, Dec 1997.
10. 3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture, version 6.10.0, Oct 2006.
11. 3GPP TS 33.203, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services, version 6.6.0, Oct 2006.
12. 3GPP2 S.R0032, Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP), version 1, Dec 2000.