

# A SURVEY OF WIRELESS SECURITY

DILEEKA DIAS

Department of Electronic & Telecommunication Engineering, University of Moratuwa

**Abstract.** The paper discusses security issues specific to wireless networks, and the evolution of security mechanisms in these networks. Wireless networks are wide and varied in terms of their capabilities and application environments. The success of these networks are clearly linked to their security mechanisms. Security in two important wireless networks in today's context: wireless LANs and mobile networks are described in detail.

## 1. Introduction

Wireless networks have become an integral component of our telecommunications infrastructure today. Ranging from short range ad-hoc networks such as Bluetooth to wide-area, broadband networks such as IEEE802.16 (WiMax) or 3G mobile networks, the capabilities and applications of these networks are numerous. For example, a wireless LAN may be employed for local coverage, low mobility and high data rates while an overlaying cellular network is used for wide area coverage, high mobility, but low data rates.

The basic components of a wireless architecture remain the same throughout different systems, even though implementation and technology offers different capabilities and options. The architecture use to represent a generic framework shown in Figure 1.

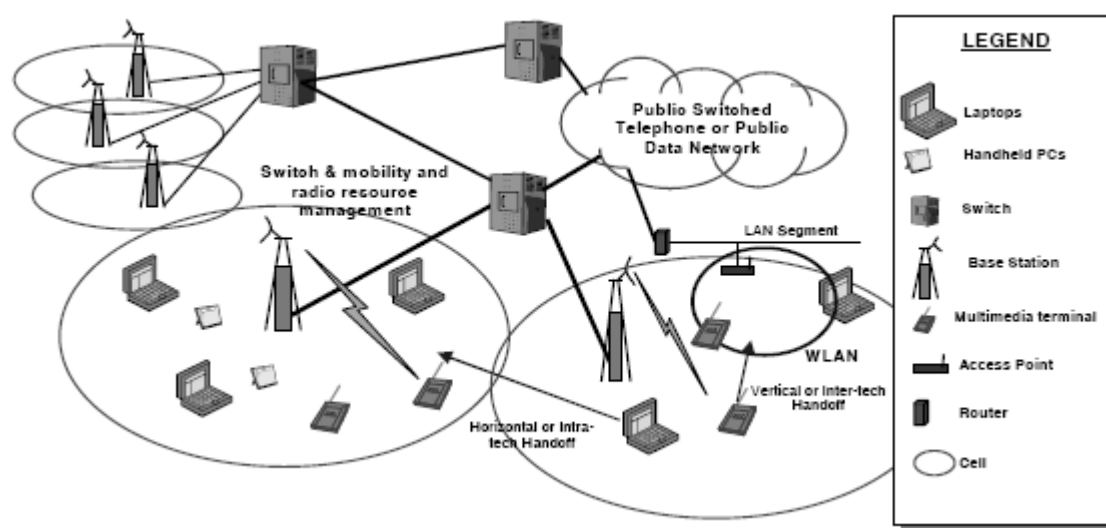


Figure 1. Generic Wireless Network Framework [Source: Kabara et. al, 2001 ]

It is a hybrid of technologies that are integrated to form an infrastructure with interconnecting fixed base stations (or access points) and a cellular architecture. A wired infrastructure consisting of switches, routers and mobility management units exists to support the operation of the wireless network (Kabara et. al, 2001).

As illustrated in Figure 1, the wireless network infrastructure consists of terrestrial cellular/PCS, high capacity links (wired or fixed point-point radio), programmable multi-band multimode radios, and high-speed WLANs connected either through an infrastructure or operating in an ad hoc fashion. The user terminals range from high power servers, to desktops, laptops, handheld computers, PDAs, cellular phones and smart sensor devices. As locations of mobile nodes (MNs) change the MNs will enter and leave macro and microcells, accessing the network at various points of attachment (base stations BSs and access points APs). The technology used to access the network and the patterns of connectivity and disconnections will vary widely and yet must happen seamlessly (Kabara, et. al, 2001).

The paper illustrates security issues specific to wireless networks in Section 2. Section 3 is devoted to the evolution and current status of security in wireless LANs. Section 4 describes security mechanism in key worldwide mobile network standards, GSM and UMTS.

## 2. Wireless-specific Security Issues

While wireless networks bring the much needed flexibility to our lives, they also bring new security problems. These problems can be summarized as (Tarn and Chen, 2006. Kabara et. al., 2001):

- Wireless devices can form ad hoc networks that enable collection of communications between peer nodes
- The nature of wireless media may provide cover for malicious users for launching attacks to fixed networks. Wireless networks are unique in that the channel is not physically secure and has a lower data rate and higher error rate compared to a wired connection. Information availability is limited by failures in the network that may be a result of intentional attacks or accidental breakdown.
- Mobile devices can be at a higher risk of loss or theft, thereby contributing to the elevated possibility of intrusion and activities to compromise existing networks
- Mobile devices are limited in computational and battery power, all of which combine to constrain information security and availability mechanisms.

In addition, wireless networks, being the backbone of mobile commerce, users need to trust the technology as well as the parties involved in a transaction. Since mobile commerce is a new way of conducting business, its security requirements are inherently different from that of traditional networks.

The potential hindrances to better security in both wireless and wireline networks include unauthorized access to the network, packet sniffing, unauthorized activities, data alteration, unregistered transactions, eavesdropping, repudiation, and spoofing.

A robust wireless network security solution should facilitate a range of functions from the protection of network assets to the minimization of threats and vulnerabilities. This involves security protection at three levels: technology, operational, and infrastructure levels.

The requirements of wireless security can be broadly classified as follows:

- Encryption and Data Privacy – The aim of encryption is to provide a mechanism to provide data privacy and integrity. The data should not be decrypted by any unauthorized means. All transmitted packets should be originated from the senders. The security mechanism should enforce the integrity of data under any circumstances.
- Authentication and Access Control – Authentication should be mutual, enabling wireless device clients and access points to authenticate each other. A framework should be introduced in order to facilitate the transmission of authentication messages between clients, access points and authentication servers.

## 3. Security in IEEE802.11 Wireless LANs

### 3.1 Wired Equivalent Privacy (WEP)

IEEE 802.11 defines an optional Wired Equivalent Privacy (WEP) mechanism to implement the confidentiality and integrity of the traffic in the network. WEP is used at the station-to-station level and does not offer any end-to-end security. WEP uses the RC4 PRNG symmetric key, stream cipher algorithm based on a 40 bit secret key and a 24 bit initialization vector (IV). WEP includes an integrity check vector (ICV) to allow integrity check. One MPDU frame contains the clear text IV and ICV and the cipher text data block, so receiver is always able to decrypt the cipher text block and to check the integrity. The IV can always be new or reused for a limited time [Uskela, 1997]. The scheme is illustrated in Figure 2.

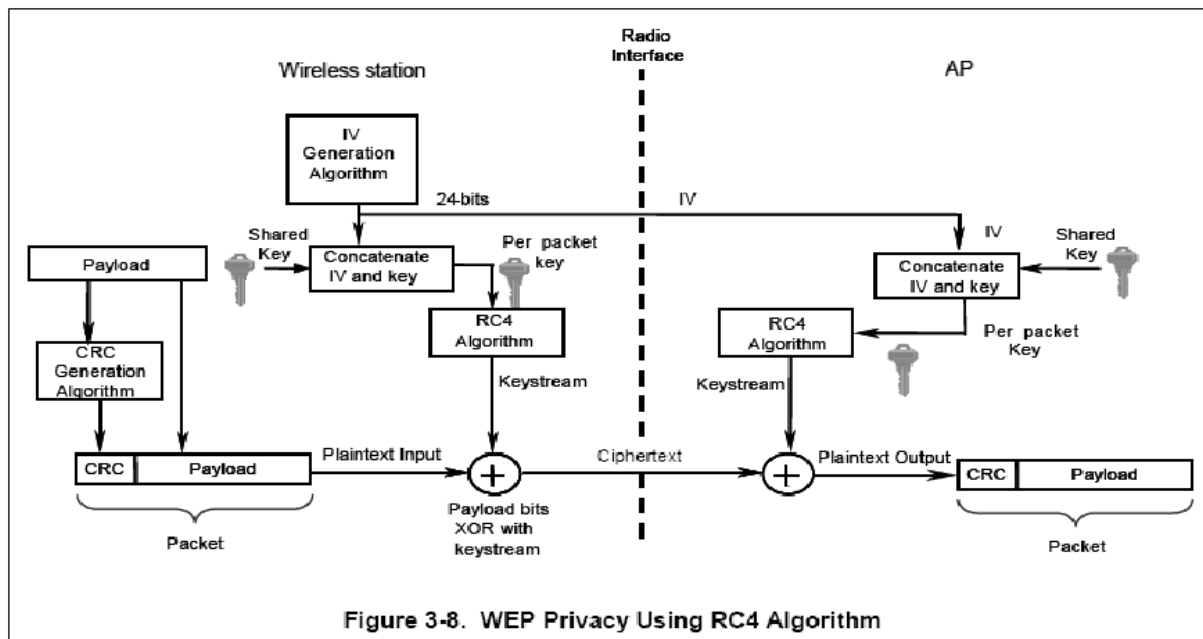


Figure 2. Wired Equivalent Privacy (WEP) [Source: karygiannis and Owens, 2002]

### 3.2 Vulnerabilities of WEP

Though WEP is able to use an RC4 cryptographic algorithm with a variable length key to protect traffic, the 802.11 standard supports WEP cryptographic keys of 40-bits. Different vendors have adopted variations of the cryptographic key such as extension of key length to 104 and 128, generating keys based on passwords or keystrokes from the user.

Several groups of computer security specialists have discovered security problems that let malicious users compromise the security of WLANs. These include passive attacks to decrypt traffic based on statistical analysis, active attacks to inject new traffic from unauthorized mobile stations (i.e., based on known plain text), active attacks to decrypt traffic (i.e., based on tricking the access point), and dictionary-building attacks. The dictionary building attack is possible after analyzing enough traffic on a busy network. More information on these are found in (Karygiannis and Owens, 2002) and the references therein.

### 3.3 Wi-Fi Protected Access (WPA)/802.11i

The IEEE and the Wi-Fi Alliance realized the need to look at WEP's deficiencies and create a new standard. The IEEE began to look at what was coined 802.11i. This, when implemented correctly, would create what are called Robust Security Networks (RSNs). 802.11i would create standards that scale much better than WEP and provide an international standard that can be followed to secure WLANs.

However, the Wi-Fi alliance realized that a quick alternative for WEP was urgently needed until the 802.11i standardization was complete. Therefore, they decided to create their own subset of 802.11i called WPA (Wi-Fi Protected Access). WPA was based on portions of the 802.11i standard that were already decided on. WPA was supported by a large number of manufacturers, and WEP was superseded by WiFi Protected Access (WPA) in 2003. The full IEEE802.11i standard (also known as WPA2) came into effect in 2004. WPA and 802.11i specified new standards for authentication, encryption, and message integrity.

The IEEE 802.11i specification introduces the concept of a Robust Security Network (RSN). An RSN is defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA). IEEE 802.11i defines an RSN as a wireless network that allows the creation of RSN Associations (RSNA) only. The RSNA is a security relationship established by the IEEE 802.11i 4-Way Handshake. This validates that the parties to the protocol instance both possess a pairwise master key (PMK), synchronizes the installation of temporal keys, and confirms the selection of cipher suites. The PMK is the cornerstone for a number of security features absent from WEP. Complete robust security is considered to be possible only when all devices in the network use RSNAs (Frankel et. al., 2007). Figure 3 shows the Pre-RSN and RSN security architecture.

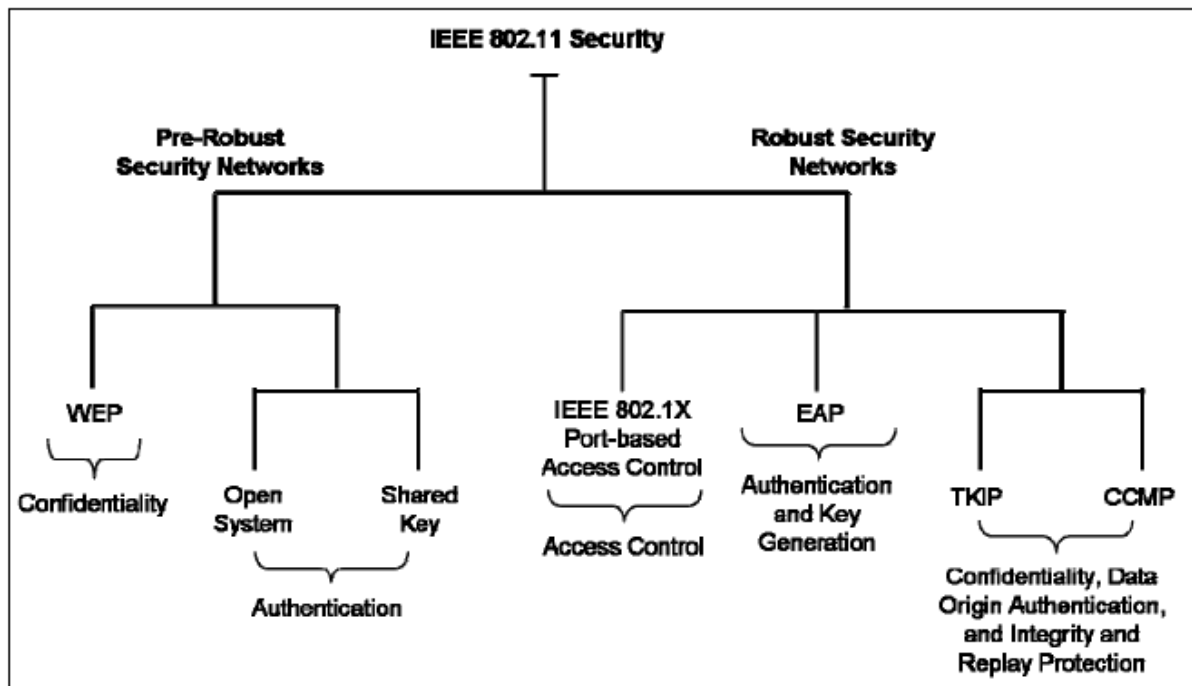


Figure 3: Pre-RSN and RSN Security [Source: Frankel et. al., 2007]

At a high level, RSN includes IEEE 802.1X port-based access control, key management techniques, the Temporal Key Integrity Protocol (TKIP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) data confidentiality and integrity protocols. These protocols allow for the creation of several diverse types of security networks because of the numerous configuration options.

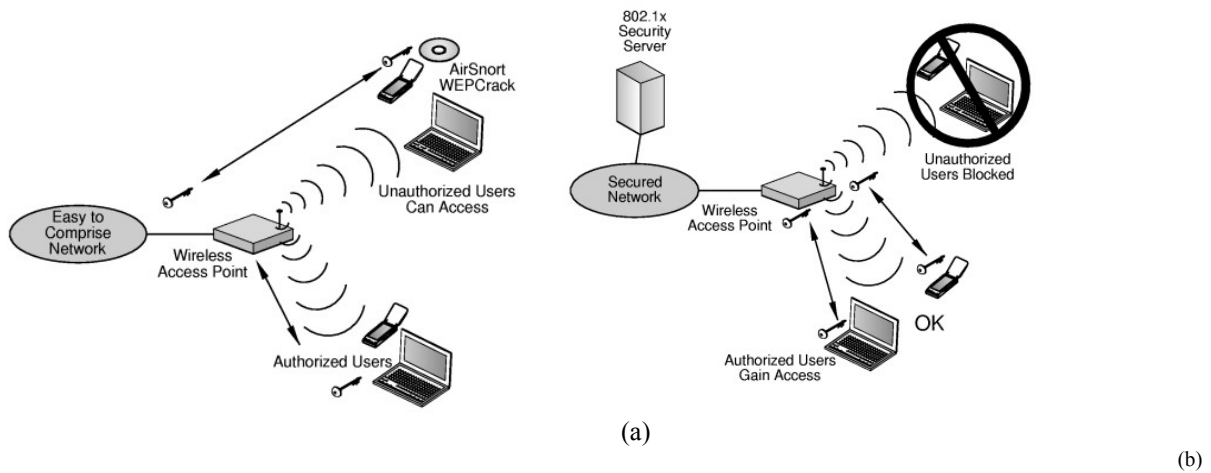
RSN security is at the link level only, providing protection for traffic between a wireless station and its associated access point, or between one wireless station and another. It does not provide end-to-end application-level security, such as between a station and an e-mail or Web server (Frankel et. al., 2007). The components of RSN security are described below.

### 3.3.1 IEEE802.1x

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X user authentication as shown in Figure 4(b), requires a user to provide credentials to the security server before getting access to the network. The credentials can be in the form of user name and password, certificate, token, or biometric. The security server authenticates the user's credentials and verifies that he/she is authorized to access the network.

If the user is both authenticated and authorized to access the network, and the access point is verified as being part of the network, then the security server communicates directly with the access point to authorize the user's access to the network. The security server also creates a unique pair of encryption keys for this user session, which are sent to both the access point and the client to securely and uniquely encrypt the wireless communication between the two. The security server also verifies that the access point is a valid part of the network. This is done to protect the user from connecting to an unauthorized access point that may have been set up to fraudulently capture network data.

802.1X security overcomes two significant limitations that physical layer security alone presents. It provides unique encryption keys for each user each time they sign onto the network, and eliminates the key management issues associated with maintaining common encryption keys across all access points and users. The security server allows network access to be managed on a user basis. Combining 802.1X user authentication with physical layer security provides robust, strong security.



**Figure 4:** Comparison of WEP and IEEE802.11i (a) the WEP standard: authorized users can gain access with easy-to-find software. Also, all authorized users must use the same encryption key.(b) IEEE802.1x Authentication: a security server verifies that the access point is part of the network and requires users to provide unique credentials to verify their identity. [Source: Hewlett Packard, 2003]

### 3.3.2 Extensible Authentication Protocol (EAP)

802.1x defines port-based network access control that uses the Extensible Authentication Protocol (EAP) and a RADIUS server. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods. 802.1x doesn't define the actual authentication protocol but specifies EAP that in turn supports a number of authentication protocols. EAP is extensible so that new authentication protocols can be supported as they are developed. EAP encapsulation over LANs (EAPOL)— it is the key protocol in IEEE 802.1x for key exchange. Two main EAPOL-key exchanges are defined in IEEE 802.11i. The first is referred to as the 4-way handshake and the second is the group key handshake.

### 3.3.3 Temporal Key Integrity Protocol (TKIP)

This is a data-confidentiality protocol that was designed to improve the security of products that implemented WEP. TKIP uses a message integrity code called Michael, which enables devices to authenticate that the packets are coming from the claimed source. Also TKIP uses a mixing function to defeat weak-key attacks, which enabled attackers to decrypt traffic.

### 3.3.4 Counter-Mode/CBC-MAC Protocol (CCMP)

This is a data-confidentiality protocol that handles packet authentication as well as encryption. For confidentiality, CCMP uses AES in counter mode. For authentication and integrity, CCMP uses Cipher Block Chaining Message Authentication Code (CBC-MAC). In IEEE 802.11i, CCMP uses a 128-bit key. CCMP protects some fields that aren't encrypted. The additional parts of the IEEE 802.11 frame that get protected are known as additional authentication data (AAD). AAD includes the packets source and destination and protects against attackers re-playing packets to different destinations.

Figure 5 shows the IEEE802.11 protocol stack and how the security mechanisms described above fit in.

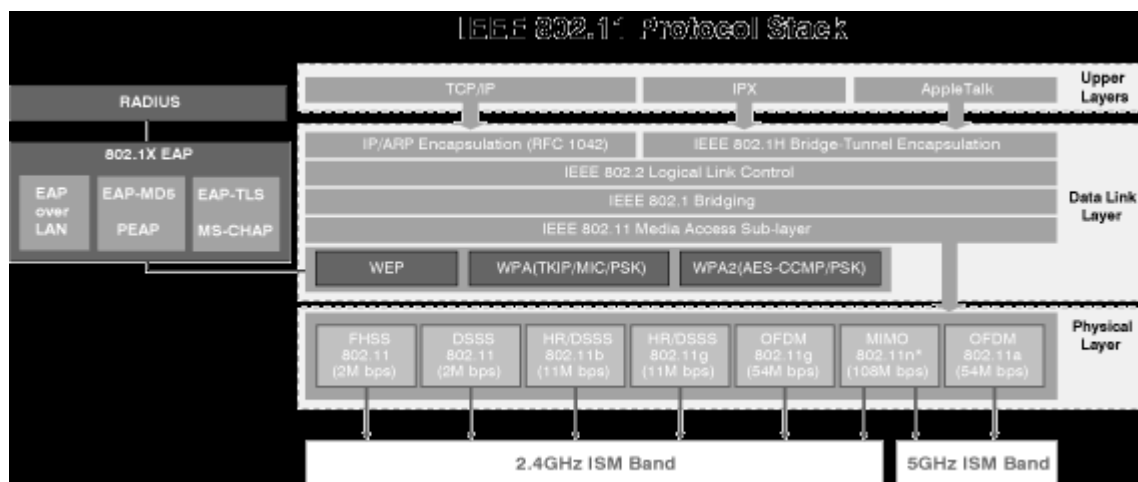


Figure 5: The IEEE 802.11 Protocol Stack [Source: Javvin Technologies Inc.]

## 4. Security in Mobile Networks

### 4.1 Security in GSM

Security has been a major driver for the success of GSM. Specifications have been developed to prevent terminal equipment theft, to allow encryption and authentication, to control payment for copyright material downloading and to respond to many other security threats (Brookson and Zumerle, 2006). The general description of the security functions can be found in (3GPP TS 43.020).

The major characteristics of security in GSM are described below:

- **Anonymity** – Anonymity implies preventing the tracking of the location of the user or identifying calls made to or from the user by eavesdropping on the radio path. Anonymity in GSM and UMTS is provided by using temporary identifiers. When a user first switches on his radio set, the real identity is used and a temporary identifier is then issued. From then on, the temporary identifier is used, until the network requests the real identity again.
- **Authentication and Signalling Protection** – Authentication is used to identify the user (or holder of a Smart Card) to the network operator and is based on encryption. The first thing the network must do is identify and authenticate the customer. To do this the network sends a 128-bit challenge to the customer phone. The SIM in the phone then uses the A3 algorithm and the Individual Subscriber Authentication Key (Ki, Unique to every different SIM) to compute a Signed RESponse(SRES) and sends it back to the base station. If the SRES matches the pre-computed value in the base station the next step takes place.

Here the SIM uses a different algorithm, A8, Ki and the original challenge to compute a Session Key (Kc) and sends this to the base station. This session key is now used along with the A5 algorithm to encrypt the data for over the air transmission. The process can be represented graphically as shown in Figure 6.

The A3 and A8 algorithms are implemented on the SIM. The A5 algorithm is a stream cipher residing in the mobile equipment and allows for data encryption and decryption over the air interface. It is implemented very efficiently in hardware and the design was never made public.

- **IMEI (Equipment Security)** – ETSI has created a set of standards system to prevent handset theft based on a handset identity number called the International Mobile Equipment Identity (IMEI). This is a unique number attributed during handset manufacturing, registered by the Mobile Network Operator (MNO) and implemented into the mobile terminal. It resides in the Equipment Identity Register (EIR). This number is completely independent of the SIM. Using the IMEI, mobile equipment declared as stolen can be blacklisted by the operators.

IMEI blacklisting is currently in operation, though not yet on a worldwide basis. To use stolen handsets, the IMEI value can also be changed to an authorised one. To reduce handset theft, some countries have passed laws that make IMEI alteration illegal. In parallel, handset manufacturers are working on increasing the IMEI's security.

The IMEI offers other benefits too: for example, certain handsets can be tracked by the network for evaluation or other purposes. IMEI is also useful to identify the makers of hoax emergency calls.

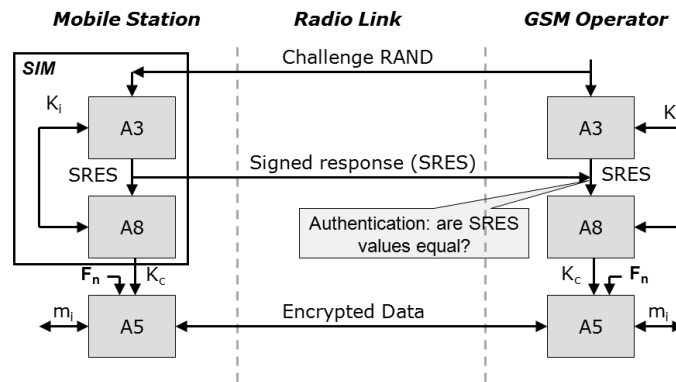


Figure 6: GSM Authentication

- **FIGS** – Fraud Information Gathering System (FIGS) (GSM 01.31) is a method of monitoring a subscriber's activities to limit the accumulation of large unpaid bills run up whilst roaming. FIGS allows the network that roaming subscribers are entering to collect information about their activities. The network then sends this information back to the home network of the subscriber, which can then clear certain types of calls and prevent fraudulent use of the system.
- **Priority** – GSM specifications include a public safety service called Priority. This allows users of the appropriate category (typically the emergency services, government agents and the military) to obtain high priority access to network services in crisis conditions, when there is a danger of overloading a potentially impaired network.

#### 4.2 Security in UMTS

UMTS is built on top of the existing GSM infrastructure and integrates both packet and circuit data transmission. The UMTS security specifications developed in 3GPP build on the mechanisms used in the GSM specifications, inheriting the proven GSM security features. This maximizes the compatibility between GSM and UMTS i.e. GSM subscribers roaming in a UMTS network are supported by GSM security features. UMTS also provides a solution to the weaknesses of GSM security and adds security features for new 3G radio access networks and services. New services introduced in UMTS also require new security features to protect them. The 3rd Generation Partnership Project (3GPP), a collaboration between groups of telecommunications associations, define globally applicable 3G mobile system specifications, including UMTS.

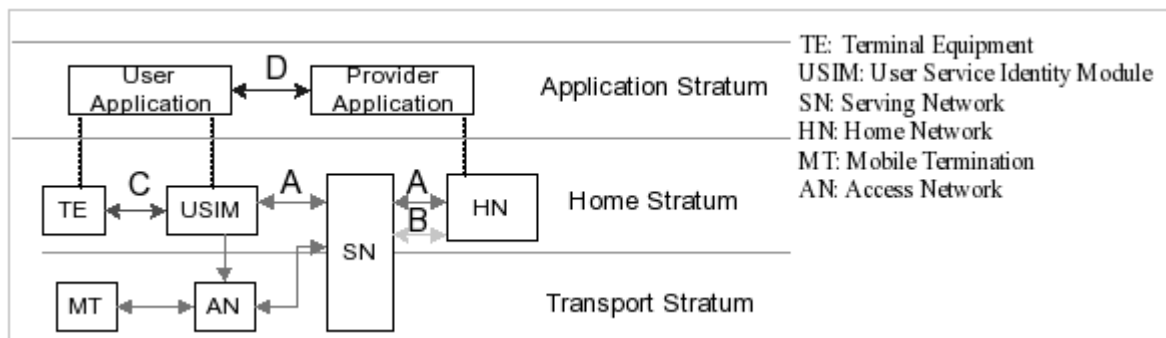
As in GSM, a smart card is used in UMTS (USIM) to store all the identification and security-related data that the subscriber needs to make or receive a call. Some of the issues that have had an impact on the design of the UMTS access security architecture are listed below (Boman et. al, 2002):

- The GSM cipher algorithms (used to provide confidentiality) were not published along with the bulk of the GSM standards. Instead, the GSM Association controls the distribution of the algorithm specifications. 3GPP adopted a more open approach to the design of the UMTS algorithms and to publish the algorithm specifications together with the rest of the UMTS standards.
- The GSM and UMTS authentication algorithms do not need to be standardised and operators are free to design or select their own. In GSM an example algorithm was not included in the standards. This resulted in some operators using algorithms vulnerable to cryptographic attack. To help avoid inadequate algorithms being used in UMTS, an example algorithm called MILENAGE10 has been included in the standards for use by operators who do not wish to design their own.
- The strength of the cipher algorithm depends in part on the length of the cipher key. In GSM the cipher key is transported as a 64 bit structure. UMTS required a new ciphering mechanism and increased the cipher key length to 128 bits, which should provide a good level of security for many years to come.

- GSM was not explicitly designed to protect against active attacks on the radio path, because they would require an attacker to masquerade as a GSM network (so-called ‘false base station attacks’). A much more thorough threat analysis was performed during the UMTS design phase. This has led to the development of new security features, which are explicitly designed to counteract false base station attacks.
- For GSM circuit-switched services, user traffic and sensitive signalling information are protected on the GSM radio path between the mobile and the base station using a ciphering algorithm. While this protects communications on the most vulnerable radio path, UMTS extends ciphering further back into the network. This allows more links within the radio access network to be protected, including potentially vulnerable microwave links that may be used to connect base stations to the fixed part of the network.

UMTS consists of five security feature groups as illustrated in Figure 7:

- **Network Access Security** (A in diagram below) provides users with secure access to UMTS services and protect against attacks on the radio access link.
- **Network Domain Security** (B in diagram below) protects against attacks on the wireline network and allows nodes in the provider domain to exchange signaling data securely.
- **User Domain Security** (C in diagram below) provides secure access to mobile stations.
- **Application Domain Security** (D in diagram below) allows the secure exchange of messages between applications in the user and in the provider domain.
- **Visibility and configurability** of security allows the user to observe whether a security feature is currently in operation and if certain services depend on this security feature



**Figure 7:** Security feature groups in UMTS

UMTS also provides different security features for maintaining identity confidentiality.

- **User identity confidentiality** is maintained by ensuring the permanent user identity (IMSI) of a user using the service cannot be eavesdropped on the radio link.
- **User location confidentiality** means that one cannot determine whether the presence of a user by eavesdropping on the radio access link.
- **User untraceability** ensures that it cannot be determined if different services are available to the same user by eavesdropping on the radio access link.

UMTS boasts many security advantages over GSM including a data integrity mechanism, enhanced authentication and encryption, identity confidentiality, a potential for secure roaming and greater facilities for upgrading. However UMTS also has security problems. For example everything that could happen to a fixed host attached to the internet could also happen to a UMTS terminal. Also if encryption is disabled hijacking calls is possible. And if the user is drawn to a false base station, he/she is beyond reach of the paging signals of the serving network. Finally when the user is registering for the first time in the serving network the permanent user identity (IMSI) is sent in cleartext (Brookson et. al, 2006)

## Summary

The paper illustrates the evolution of security mechanisms in wireless networks, specifically wireless LANs and cellular networks. A wide variety of wireless networks and related standards exist, each having its own capabilities and application environments. The success of all these networks depend on the security mechanisms they implement, since wireless networks are more susceptible to security threats than wired networks. The success of GSM for example, may be attributed to the security features it implements. However, 3G networks, UMTS for example, while building on GSM security, incorporates more advanced features in line with the advanced services it is intended to offer. Wireless LANs using the IEEE802.11 family of standards have suffered from poor security mechanisms in its initial version. However, many improvements, in the forms of both proprietary as well as advanced IEEE standards have been since developed to overcome these deficiencies.

## References

- Tarn, J. M., Chen, K., (2006). Mobile Technology as a Learning Object and an Exploration Tool in an IS Curriculum: An Innovative Instruction of Wireless Network Security. IEEE Transactions On Education, Vol. 49, No. 2, May 2006.
- Kabara, K., Krishnamrthy, P., Tipper, D. (2001). Information Assurance in Wireless Networks. Department of Information Science and Telecommunications University of Pittsburgh, 2001.
- Uskela S., Security in Wireless Local Area Networks. Department of Electrical and Communication Engineering, Helsinki University of Technology, 1997 ([http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/wireless\\_lan.html](http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/wireless_lan.html))
- Karygiannis, T., Owens, L., Wireless Network Security 802.11, Bluetooth and Handheld Devices. National Institute of Standards and Technology, Special Publication 800-48, 2002.
- Perez, E. IEEE802.11i (How we got here and where we are headed). SANS Institute, 2004.
- Frankel, S., Eydt, B., Owens, L., Scarfone, K., Establishing Wireless Robust Networks: IEEE802.11i, National Institute of Standards and Technology, Special Publication 800-97, 2007.
- Hewlett Packard, Three Levels of Wireless Security, 2003. (<http://docs.hp.com/en/T1428-90017/ch01s04.html>)
- Javvin Technologies Inc. IEEE802.11i Wireless Security Standards (<http://www.javvin.com/protocol80211i.html>)
- Brookson, C., Zumerle, D., ETSI White Paper No. 1: Security for ICT - the Work of ETSI., European Telecommunications Standards Institute, 2006.
- 3GPP TS 43.020. TS 143 020 3GPP SA 3 Digital cellular telecommunications system (Phase 2+); Security-related network functions, European Telecommunications Standards Institute.
- GSM 01.31. 101 105 SMG 10 Digital cellular telecommunications system (Phase 2+) (GSM); Fraud Information Gathering System (FIGS) service requirements, European Telecommunications Standards Institute.
- Boman, K. Horn, G. Howard, P. Niemi, V. UMTS security, Electronics & Communication Engineering Journal, Volume: 14, Issue: 5 , Oct 2002.