Security In Wireless Cellular Networks

Ali I. Gardezi ali@aligardezi.com

Abstract:

Cellular Communication has become an important part of our daily life. Besides using cell phones for voice communication, we are now able to access the Internet, conduct monetary transactions, send text messages etc. using our cell phones, and new services continue to be added. Therefore, it is important to provide users with a secure channel for communication. This survey paper will give a brief introduction to the various generations of cellular networks. For those not familiar with the cellular network architecture, a brief description of the new 3G cellular network architecture will be provided. Limitations of cellular networks, their security issues and the different types of attacks will be discussed. Then the steps taken in the new 3G networks to combat the different security threats will be provided. Also, the security features of the Wireless Application Protocol (WAP) used to access the Internet will be discussed. The paper will go over some new security mechanisms that have been proposed by researchers.

Table Of Contents:

1. Introduction

Cellular Communication has become an important part of our daily life. Besides using cell phones for voice communication, we are now able to access the Internet, conduct monetary transactions, send text messages etc. using our cell phones, and new services continue to be added. However, the wireless medium has certain limitations over the wired medium such as open access, limited bandwidth and systems complexity. These limitations make it difficult although possible to provide security features such as authentication, integrity and confidentiality. The current generation of 3G networks have a packet switched core which is connected to external networks such as the Internet making it vulnerable to new types of attacks such as denial of service, viruses, worms etc. that have been used against the Internet.

Back to Table Of Contents

2. Generations Of Cellular Networks

Cellular Networks have been around since the 1980s and each year their subscribers increase at a very fast rate. First generation (1G) networks were the first cellular networks introduced in the 1980s. They were only capable of transmitting voice at speeds of about 9.6 kbps max. In the US the system was known Advanced Mobile Phone System (AMPS) and in Europe the Nordic Mobile Telephony (NMT). Both these technologies used analog modulation to transmit data as a continuously varying waveform.

1G systems had some limitations such as no support for encryption, poor sound quality and inefficient use of the spectrum due to their analog nature. Second generation (2G) cellular networks also known as personal communication services (PCS) introduced the concept of digital modulation meaning that voice was converted into digital code, and then into analog (radio) signals. Being digital, they overcame certain limitations of 1G systems. Various 2G technologies have been deployed around the world. Code Division Multiple Access (CDMA), North American Time Division Multiple Access (NA-TDMA) and digital AMPS (D-AMPS) have been deployed in the US whereas Global System for mobile communication (GSM) has been deployed in Europe and USA and Personal Digital Cellular (PDC) has been deployed in Japan.

Although 2G systems were a great improvement from 1G, they were only used for voice communication. 2.5G is a transition step between 2G and 3G (explained later). It is also known as data services over 2G. There have been several deployments of 2.5G across the world. In the USA, they are known as 1xEV-DO and 1xEV-DV. In Europe or places where GSM has been used, 2.5G technologies such as High Speed circuit switched data (HSCSD), General packet Radio Service (GPRS), Enhanced Data Rate for GSM Evolution (EDGE) have been deployed.

The Third generation (3G) standard is currently being pushed as the next global standard for cellular communications. It will provide services such as fast Internet surfing, advanced value added services and video telephony. Deployments of this technology have already begun and several countries like Austria, Denmark, South Korea and Japan have adopted the 3G network architecture. There are three main technologies that are being applied. In the US CDMA2000, in Europe Wideband CDMA (W-CDMA) and in China Time Division-Synchronous Code Division Multiple Access (TD-SCDMA).

Although 3G has not been fully deployed, people have already started talking about the fourth generation (4G) technology. This generation will be designed to have data rates of up to 20Mbps. It will have support for next generation Internet such as IPv6, QoS and Mo-IP, lower system cost and high capacity and capable of supporting communication in moving vehicles with speed up to 250 km/hr.

2.1 2G And 2.5G

GSM is the most widely adopted 2G technology in the world. Although it was initially employed in Europe, it has become a global technology with subscribers in about 197 countries. Its specifications were completed in 1990 and service began in 1992. This paper will not delve into the techniques of 2G/2.5G because it will soon be replaced by 3G. Interested readers are encouraged to look at [Imai05] for more details. However, some of the data services which are part of the 2.5G extension are

- Short Messaging Service (SMS): Transfer of messages between cell phones. Large messages are truncated and sent as multiple messages.
- High-Speed Circuit-Switched Data (HSCSD): This was the first attempt at providing data at high speeds data over GSM, with speeds of up to 115 kbps. This technique cannot support large bursts of data. HSCSD was not widely implemented and GPRS became a more popular technique.
- General Packet Radio Service (GPRS): This technique can support large bursty data transfers. In order to support this two new elements have to be added to existing networks. Service GPRS support node (SGSN) for security mobility and access control and Gateway GPRS support node (GGSN) in order to connect to external packet switched networks.
- Enhanced Data Rates for GSM Evolution (EDGE): The standard GSM uses GMSK modulation. Edge uses 8-PSK modulation. GPRS and EDGE combined provide data rates of up to 384 kbps.
- Cellular Digital Packet Data (CDPD): CDPD is a packet based data service. CDPD is able to detect idle voice channels and uses them to transfer data traffic without affecting voice communications.

CDMA is the primary 2G technology in the USA. CDMAOne, also known as IS-95a was the initial technique. This technique

allows users to use the entire spectrum and can support more users than TDMA and GSM. Speed between 4.8 and 14.4 kbps can be supported. The CDMATwo extension can provide data rates of up to 115.2 kbps. The 2.5G extension to this technology can be divided into two techniques. 1xEV-DV uses one radio frequency channel for data and voice, whereas 1xEV-DO uses separate channels for data and voice. These are fully compatible with both CDMAOne and its 3G replacement CDMA2000, to make the transition as easy as possible.

2.2 3G

3G is the next generation wireless cellular network whose aim is to provide a world wide standard and a common frequency band for mobile networking. The International Telecommunication Union (ITC) started the process in 1992, the result of this effort was a new network infrastructure called International mobile telecommunications 2000 (IMT- 2000), with the 2000 signifying that this new technology will be available in 2000, will have data rates of up to 2000 Kbps and will be in the 2000 MHz frequency range. The following is the list of objectives that IMT-2000 aims to receive [Balderas04],

1. To make a wide range of services, both voice and data available to users, irrespective of location.
2. To provide services over a wide coverage area.
3. To provide the best quality of service (QoS) possible.
4. To extend the number of services provided subject to constraints like radio transmission, spectrum efficiency and system economics.
5. To accommodate a great variety of mobile stations.
6. To admit the provision of service by more than one network in any area of coverage.
7. To provide an open architecture which will permit the easy introduction of technology advancements as well as different applications.
8. To provide a modular structure which will allow the system to start from small and simple configuration and grow as needed, both in size and complexity within practical limits.

The 3rd generation partnership project was formed in 1998 to produce specifications for UMTS, a 3G technology based on Universal Terrestrial Radio Access (UTRA) radio interface and the extended GSM/GPRS network. A second radio interface also exists called IMT Multicarrier (IMT-MC) which is being promoted by the 3GPP2 organization. This interface is backward compatible with IS-95 to make a seamless transition to 3G. This proposal is known as CDMA2000. The following graph from [Balderas04] shows the number of licenses of the third generation spectrum granted since 1999.

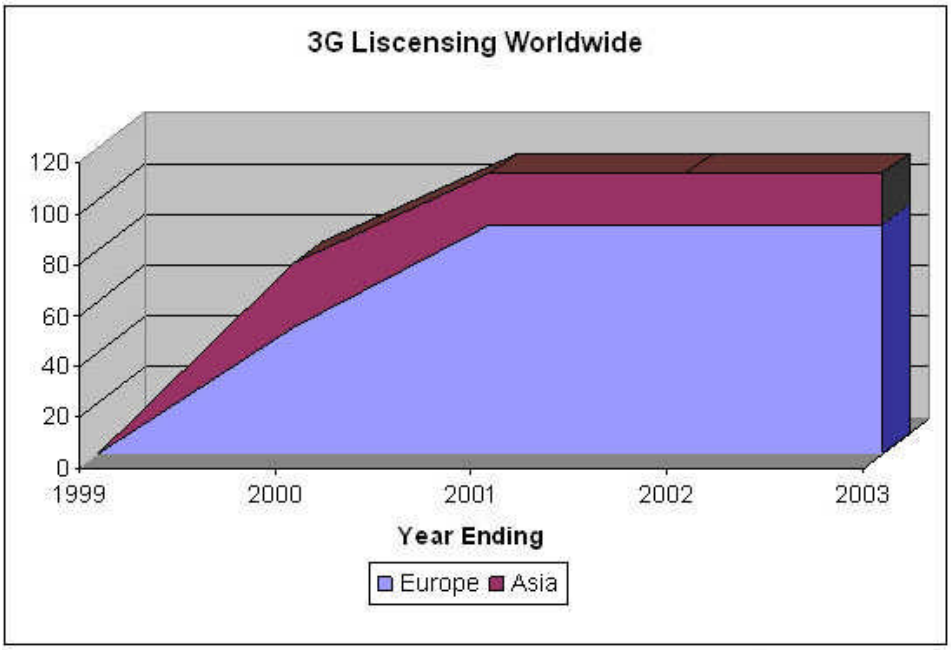

Fig 1. Number of Licenses of Third Generation Spectrum granted since 1999

2.3 3G - UMTS Architecture

To understand the threats to a network, one must understand the network infrastructure. UMTS is considered the most

important 3G proposal. It is being developed as an evolution of GSM and therefore based on the GPRS network which is a 2.5G technology and the UTRA radio interface.

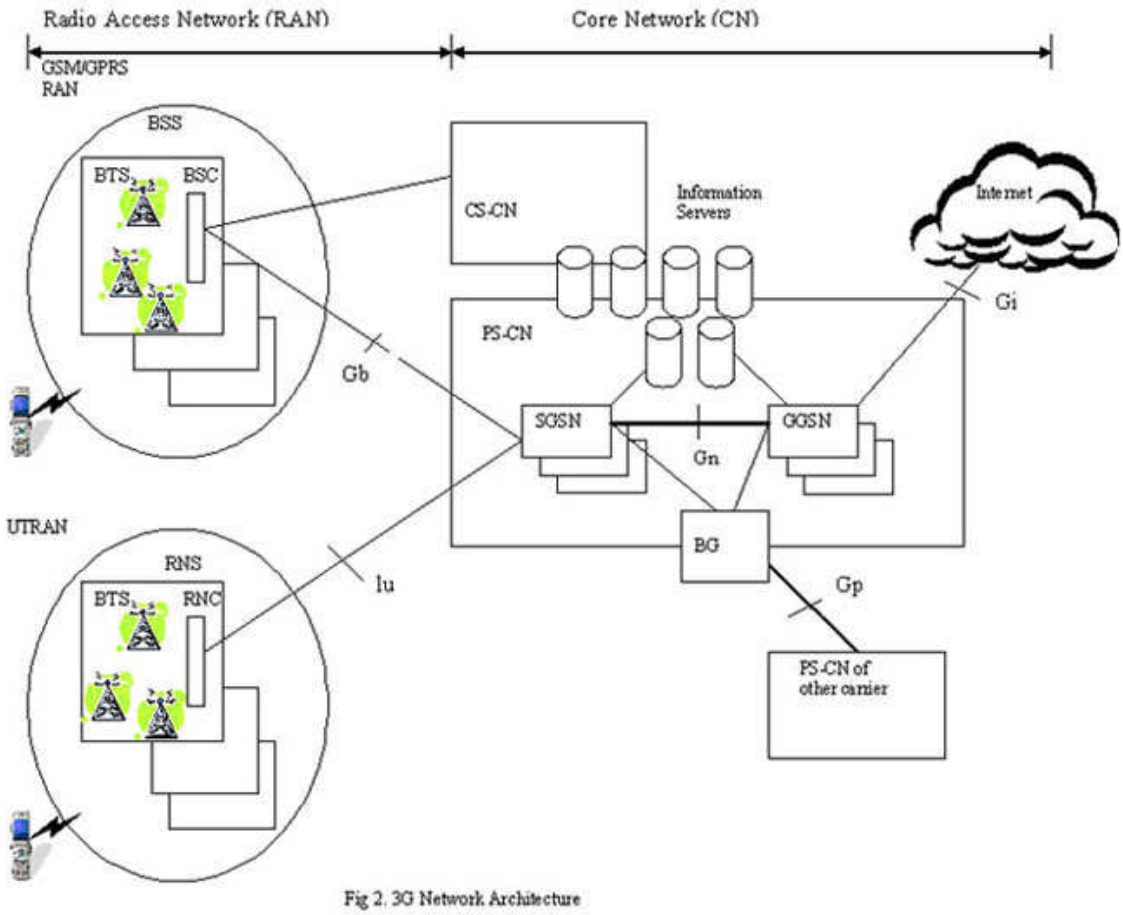

Fig 2. 3G Network Architecture

As can be seen in Figure 2 [Yang06], the 3G network has two main parts

1. The Radio Access Network (RAN)
2. The Core Network (CN)

The RAN consists of the existing GPRS/GSM RAN system which is connected to the Packet Switched Network (PS-CN) and also to the circuit switched network (CS-CN). The PS-CN will eventually connect to the UTRAN system as part of the full transition to 3G. The UTRAN consists of subsystems, with each subsystem consisting of one Radio Network Controller (RNC) which is connected to several Base Transceiver Stations (BTN). The GRPS RAN has a similar architecture.

The Core Network consists of the PS-CN and the CS-CN. The PS-CN consists of several information servers, the SGSN and the GGSN. Each SGSN connects one or more RSC and BSC with the PS-CN. Its functionality includes access control, mobility management, paging and route management [Yang06]. The GGSN is the logical gateway to the Internet. The BG interface can be used to connect to another PS-CN or to another carrier. The information servers provide several functions. The Home Location Register (HLR) maintains subscriber information and the Authentication Center (AuC) maintains authentication information. There are also IP based servers such as DNS, DHCP and RADIUS servers which interact with the SGSN/GGSN and provide control and management functions.

Back to Table Of Contents

---

3. Security Issues In Cellular Networks

The infrastructure for Cellular Networks is massive, complex with multiple entities coordinating together, such as the IP Internet coordinating with the core network. And therefore it presents a challenge for the network to provide security at every possible communication path.

3.1 Limitations Of Cellular Networks

Compared to Wired Networks, Wireless Cellular Networks have a lot of limitations.

1. Open Wireless Access Medium: Since the communication is on the wireless channel, there is no physical barrier that can separate an attacker from the network.
2. Limited Bandwidth: Although wireless bandwidth is increasing continuously, because of channel contention everyone has to share the medium.
3. System Complexity: Wireless systems are more complex due to the need to support mobility and making use of the channel effectively. By adding more complexity to systems, potentially new security vulnerabilities can be introduced.
4. Limited Power: Wireless Systems consume a lot of power and therefore have a limited time battery life.
5. Limited Processing Power: The processors installed on the wireless devices are increasing in power, but still they are not powerful enough to carry out intensive processing.
6. Relatively Unreliable Network Connection: The wireless medium is an unreliable medium with a high rate of errors compared to a wired network.

3.2 Security Issues In Cellular Networks

There are several security issues that have to be taken into consideration when deploying a cellular infrastructure. The importance of which has increased with the advent of advanced networks like 3G.

1. Authentication: Cellular networks have a large number of subscribers, and each has to be authenticated to ensure the right people are using the network. Since the purpose of 3G is to enable people to communicate from anywhere in the world, the issue of cross region and cross provider authentication becomes an issue.
2. Integrity: With services such as SMS, chat and file transfer it is important that the data arrives without any modifications.
3. Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.
4. Access Control: The Cellular device may have files that need to have restricted access to them. The device might access a database where some sort of role based access control is necessary [Fernandez05-1].
5. Operating Systems In Mobile Devices: Cellular Phones have evolved from low processing power, ad-hoc supervisors to high power processors and full fledged operating systems. Some phones may use a Java Based system, others use Microsoft Windows CE and have the same capabilities as a desktop computer. Issues may arise in the OS which might open security holes that can be exploited.
6. Web Services: A Web Service is a component that provides functionality accessible through the web using the standard HTTP Protocol. This opens the cellular device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc. [Fernandez05-2]
7. Location Detection: The actual location of a cellular device needs to be kept hidden for reasons of privacy of the user. With the move to IP based networks, the issue arises that a user may be associated with an access point and therefore their location might be compromised.
8. Viruses And Malware: With increased functionality provided in cellular systems, problems prevalent in larger systems such as viruses and malware arise. The first virus that appeared on cellular devices was Liberty. An affected device can also be used to attack the cellular network infrastructure by becoming part of a large scale denial of service attack.
9. Downloaded Contents: Spyware or Adware might be downloaded causing security issues. Another problem is that of digital rights management. Users might download unauthorized copies of music, videos, wallpapers and games.
10. Device Security: If a device is lost or stolen, it needs to be protected from unauthorized use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.

3.3 Types Of Attacks

Due to the massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to.

1. Denial Of Service (DOS): This is probably the most potent attack that can bring down the entire network infrastructure.

This is caused by sending excessive data to the network, more than the network can handle, resulting in users being unable to access network resources.
2. Distributed Denial Of Service (DDOS): It might be difficult to launch a large scale DOS attack from a single host. A number of hosts can be used to launch an attack.
3. Channel Jamming: Channel jamming is a technique used by attackers to jam the wireless channel and therefore deny access to any legitimate users in the network.
4. Unauthorized Access: If a proper method of authentication is not deployed then an attacker can gain free access to a network and then can use it for services that he might not be authorized for.
5. Eavesdropping: If the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc.
6. Message Forgery: If the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing.
7. Message Replay: Even if communication channel is secure, an attacker can intercept an encrypted message and then replay it back at a later time and the user might not know that the packet received is not the right one.
8. Man In The Middle Attack: An attacker can sit in between a cell phone and an access station and intercept messages in between them and change them.
9. Session Hijacking: A malicious user can highjack an already established session, and can act as a legitimate base station.

Back to Table Of Contents

---

4. Security Mechanisms In 3G - UMTS

This survey paper will not delve into the security features of different 3G architectures. Since the underlying technology is the same, security features of one architecture are applicable to others as well. 3G - UMTS, the most popular of the architectures builds upon the security features of 2G systems so that some of the robust features of 2G systems are retained. The aim of the 3G security architecture is to improve on the security of 2G systems. Any holes present in the 2G systems are to be addressed and fixed. Also, since many new services have been added to 3G systems, the security architecture needs to provide security for these services.

4.1 3G Security Architecture

There are five different sets of features that are part of the architecture:

1. Network Access Security: This feature enables users to securely access services provided by the 3G network. This feature is responsible for providing identity confidentiality, authentication of users, confidentiality, integrity and mobile equipment authentication. User Identity confidentiality is obtained by using a temporary identity called the International Mobile User Identity. Authentication is achieved using a challenge response method using a secret key. Confidentiality is obtained by means of a secret Cipher Key (CK) which is exchanged as part of the Authentication and Key Agreement Process (AKA). Integrity is provided using an integrity algorithm and an integrity key (IK). Equipment identification is achieved using the International Mobile Equipment Identifier (IMEI).
2. Network Domain Security: This feature enables nodes in the provider domain to securely exchange signaling data, and prevent attacks on the wired network.
3. User Domain Security: This feature enables a user to securely connect to mobile stations.
4. Application Security: This feature enables applications in the user domain and the provider domain to securely exchange messages.
5. Visibility And Configurability Of Security: This feature allows users to enquire what security features are available.

The UMTS Authentication and Key Agreement (UMTS AKA) mechanism is responsible for providing authentication and key agreement using the challenge/response mechanism. Challenge/Response is a mechanism where one entity in the network proves to another entity that it knows the password without revealing it. There are several instances when this protocol is invoked. When the user first registers with the network, when the network receives a service request, when a location update is sent, on an attach/detach request and on connection reestablishment. The current recommendation by 3GPP for AKA algorithms is MILENAGE. MILENAGE is based on the popular shared secret key algorithm called AES or Rijndael. Readers interested in the AES algorithm are encouraged to look at [Imai06]. AKA provides mutual authentication for the user and the network. Also, the user and the network agree upon a cipher key (CK) and an integrity key (IK) which are used until their

time expires.

Control Signaling Communication between the mobile station and the network is sensitive and therefore its integrity must be protected. This is done using the UMTS Integrity Algorithm (UIA) which is implemented both in the mobile station and the RNC. This is known as the f9 algorithm. Figure 3 [Imai06] shows how this algorithm is applied. First, the f9 algorithm in the user equipment calculates a 32 bit MAC-I for data integrity using the signaling message as an input parameter. This, along with the original signal message is sent to the RNC, where the XMAC-I is calculated and then compared to the MAC-I. If both are same, then we know that the integrity of the message has not been compromised.

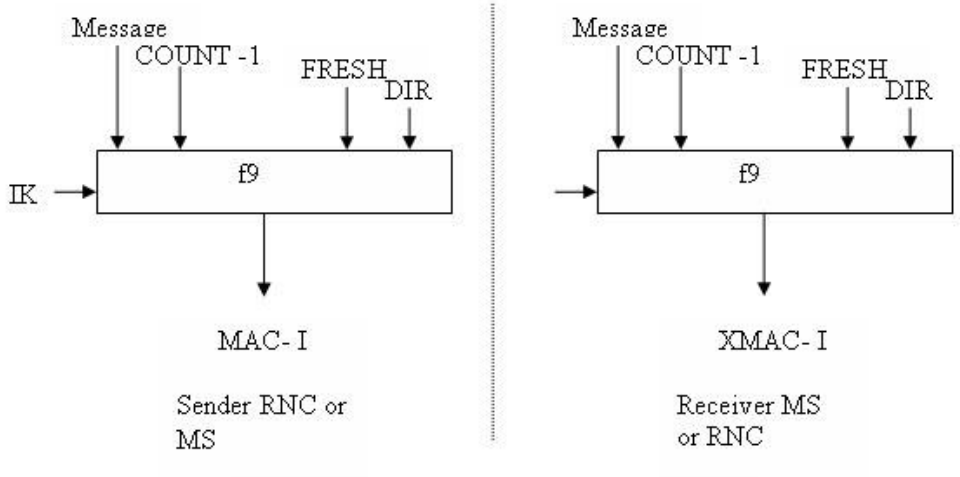

Fig 3. Signaling Data Integrity Mechanism

The confidentiality algorithm is known as f8 and it operates on the signaling data as well as the user data. Figure 4 [Imai06] shows how this algorithm is applied. The user's device uses a Cipher Key CK and some other information and calculates an output bit stream. Then this output stream is xored bit by bit with the data stream to generate a cipher stream. This stream is then transmitted to the RNC, where the RNC uses the same CK and input as the user's device and the f8 algorithm to calculate the output stream. This is then xored with the cipher stream to get the original data stream.

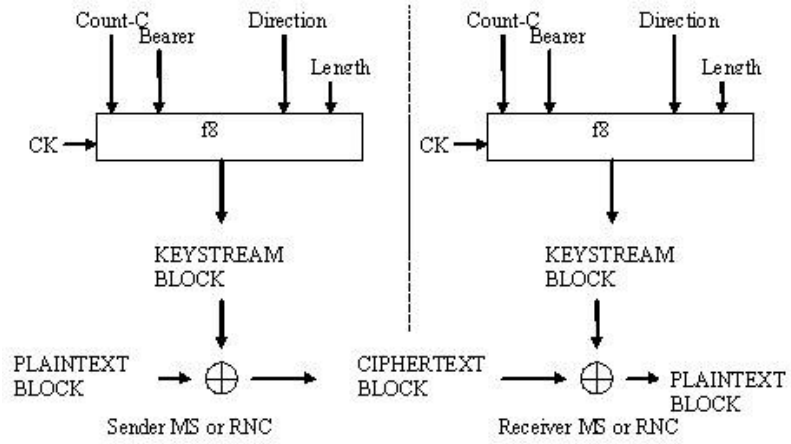

Fig 4. Air Interface Confidentiality Mechanism

For more information on the inputs to the f8 and f9 algorithms, please refer to [Xenakis04]. A block cipher known as the KASUMI cipher is central to both the f9 and the f8 algorithm. This cipher is based on the feistel structure using 64 bit data blocks and a 128 bit key.

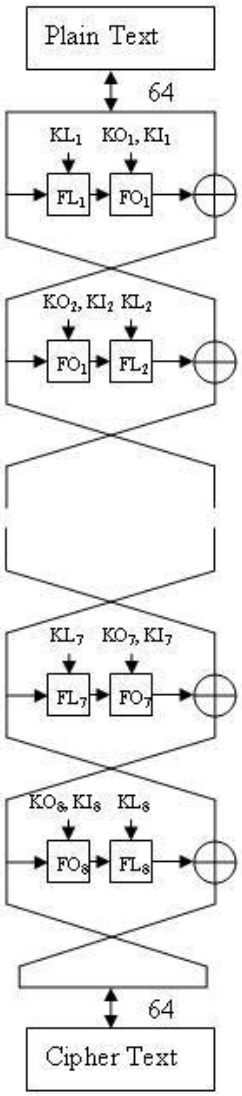

Fig 5. KASUMI Block Cipher

It has eight rounds of processing, with the plain text (can be any form of data) as input to the first round and the cipher text the result after the last round. An encryption key is used to generate round keys (KLi,KOi,KIi) for each round i. Each round calculates a separate function since the round keys are different. The same algorithm is used for encryption and decryption. The KASUMI cipher is based on the MISTY1 cipher which was chosen by 3GPP due to its proven security against many advanced cipher breaking techniques. It has been optimized for hardware implementation which is important concerning the hardware constraints of cellular devices, such as limited power and limited memory. As shown in the Figure 5 [Balderas04], the function f consists of subfunctions FLi and FOi. FL is a simple function consisting of shifts and logical operations. The FO function is much more complicated and is itself based on the fiestel structure and consists of three rounds. Anyone interested in the details of the KASUMI algorithm are encouraged to look at [Balderas04].

4.2 Wireless Application Protocol (WAP)

Since one of the most important services provided by 3G systems is access to the Internet, it is important to understand the security mechanisms of the protocol used to access the Internet. WAP is an open specification which enables mobile users to access the Internet. This protocol is independent of the underlying network e.g. WCDMA, CMDA 2000 etc and also independent of the underlying operating system e.g. Windows CE, PALM OS etc. The first generation is known as WAP1 which was released in 1998. WAP1 assumes that the mobile devices are low on power and other resources. And therefore the devices can be simple while sharing the security responsibilities with the gateway devices. The second generation is known as WAP2 and was released in 2002. WAP2 assumes that the mobile devices are powerful and can therefore directly communicate with the servers. Figure 6 and Figure 7 [Imai06] show the protocol stack for WAP1 and WAP2 respectively.

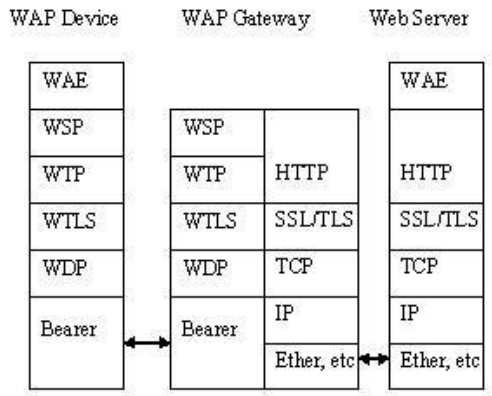

Fig 6. WAP1 Protocol Stack

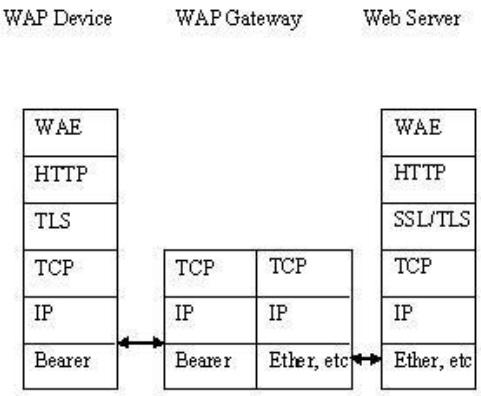

Fig 7. WAP2 Protocol Stack

A brief description of each layer is as follows,

1. Wireless Application Environment (WAE): This provides an environment for running web applications or other WAP applications.
2. Wireless Session Protocol (WSP): This is similar to the HTTP protocol and provides data transmissions with small sizes so that WAP1 clients can process the data with less complexity.
3. Wireless Transaction Protocol (WTP): This is responsible for providing reliability.
4. Wireless Transport Layer Security (WTLS): This is responsible for providing security features such as authentication, confidentiality, integrity etc. between a WAP1 client and the WAP gateway.
5. Wireless Datagram Protocol (WDP): This provides the underlying transport service.
6. Hypertext Transfer Protocol (HTTP): A standard protocol used to transmit web pages.
7. Transport Layer Security (TLS): This layer provides security features such as authentication, confidentiality, integrity etc. In WAP1, this is between the WAP1 gateway and the server. In WAP2 this is between the WAP2 client and the server.
8. Transport Control Protocol (TCP): Standard transport protocol used to provide reliability over IP.
9. Internet Protocol (IP): Protocol used to route data in a network.
10. Bearer Protocol: This is the lowest level protocol and can be any wireless technique such as GSM, CDMA etc.

Cipher Suite in WTLS: This suite provides a key-establishment protocol, a bulk encryption algorithm and a MAC algorithm. In SSL/TLS these are used together, in WTLS each can be used independently.

Key Exchange Suite: This protocol is responsible for establishing a secret key between a client and the server. An example of is the RSA key suite, which consists of the following steps: the WAP gateway sends a certificate consisting of the gateway's RSA public key and signed by the certification authority's private key. The client checks the validity of the certificate authority's signature. If invalid, the communication is aborted. If valid, the user generates a secret value, encrypts it with the gateway's public key. Both sides can then calculate their common keys using the secret value.

Bulk Encryption And MAC Suite: Bulk encryption is used for data confidentiality and the MAC is used for integrity. The common key that we calculated in the key exchange suite can be used for both purposes. For bulk encryption, algorithms such as DES, 3DES, IDEA and RC5 are used. For integrity WTLS uses the HMAC algorithm which uses either SHA-1 or MD5 twice.

WAP-Profiled TLS: WAP2 uses the WAP profiled TLS which consists of a cipher Suite, authentication suite, tunneling capability and session identification and session resume. Cipher suite consists of key establishment (e.g. RSA), encryption (e.g. DES) and integrity (SHA-1 for MAC calculation). A session identifier is chosen by the server to identify a particular session with the client. Server and Client authentication is done using certificates similar to WTLS. Tunneling is a mechanism set up between the client and the server, so that they can communicate even if the underlying network layers are different.

WAP Identity module: WIM (WAP Identity Module) is a method of identification in WAP. This enables the device to separate its identification from WAP. So a device can be updated without any changes made to the telephone number or billing information. WIM provides operations such as key generation, random numbers, signing, decryption, key exchange, storing certificates etc.

Back to Table Of Contents

---

5. Future

Security is an ever growing field. What is secure today may not be secure tomorrow. There will always be malicious users trying to exploit and find new holes in a network. Therefore, we need to look into the future so that we are able to face these security issues before they cause damage.

5.1. Additional Security Mechanisms

While there are several security mechanisms available in Wireless Cellular Networks, continued research is going on to provide new and even more secure mechanisms for cellular security.

A New Authentication Scheme with Anonymity For Wireless Networks: When a mobile user is roaming, it is necessary to provide anonymity to the users so that malicious parties are unable to associate the user with a particular session. The most basic method to provide anonymity is to have a temporary identity (TID) instead of the real id of the user. There are several issues to consider when designing a security protocol for cellular networks. One, they have low computational power which means that algorithms that require high processing power are not suitable. Second, the error rate of messages increase on wireless networks as compared to cellular networks. Therefore, any mechanism that is designed should minimize message sizes and the number of messages in order to reduce the error rate. The author(s) of [Zhu04] specifies an authentication scheme which use public key cryptosystems, hash functions and smart cards and makes use of a temporary key and a temporary certificate. They also show the performance of their algorithms with other algorithms, which clearly show that the proposed method is practical and efficient compared to other algorithms.

Manual Authentication For Wireless Devices: This is a technique used by devices to authenticate one another by manually transferring data between the devices. This means that the users will enter some information using some form of input (e.g. keypad). Underneath they employ MAC algorithms for authentication. Although the scheme that is proposed is secure, it usability depends upon how many numbers (or alphabets) the users have to input [Gehrmann04].

Elliptic Curve Cryptography For Wireless Security: Elliptic Curve Cryptography (ECC) is a mechanism which uses points on an elliptic curve to encrypt/decrypt data. It has an advantage over the popular RSA algorithm in that it is much faster. 163 - bit ECC provides the same security as a 1024 bit RSA algorithm, and can be anywhere from 5 to 15 times faster depending on the platform. For example, in order to secure a 128 bit AES shared key and 521 - bit ECC provides the same level of security as an 15,360 bit RSA while being about 400 times faster [Lauter04].

Channel Surfing And Spatial Retreats: Defense against Wireless Denial Of Service DOS attacks are one of the most dangerous attacks because they can bring down an entire network. An adversary can either trying to fill the buffer in a network device, or can by pass the MAC layer and try to jam the channel. Channel Surfing is a technique where the transmission frequency is changed to one where there is no interference. Spatial Retreats is a technique where the wireless users move to a location where there is no interference [Xu04].

5.2. A Look At Security In 4G

4G is the next generation after 3G. Although still 3G has not been fully implemented in the real world, people have started talking about the features of 4G. Some of the 4G services talked about are incorporating quality of service (QoS) and Mobility. There is also a concept of always best connected which means that the terminal will always select the best possible access available. 4G will also make use of the IPV6 address scheme. This might make it possible for each cell device to have its own IP address. Currently, the problem of security is solved by using multiple layers of encryption of the protocol stack. There are disadvantages in this scheme such as wasted power, wasted energy and a larger transmission delay. In 4G there will be a concept of interlayer security where only one layer will be configured to do encryption on data. [Carneiro04]

Back to Table Of Contents

Summary

Cellular Networks are open to attacks such as DOS, channel jamming, message forgery etc. Therefore, it is necessary that security features are provided that prevent such attacks. The 3G security architecture provides features such as authentication, confidentiality, integrity etc. Also, the WAP protocol makes use of network security layers such as TLS/WTLS/SSL to provide a secure path for HTTP communication. Although 3G provides good security features, there are always new security issues that come up and researchers are actively pursuing new and improved solutions for these issues. People have also started looking ahead at how new features of the 4G network infrastructure will affect security and what measures can be taken to add new security features and also improve upon those that have been employed in 3G.

Back to Table Of Contents

References

The following are the list of references organized in order of relevance.

- [Imai06] Imai, H., et. al., "Wireless communications security," Boston: Artech House, 2006
- [Yang06] Yang, H., et. al., "Securing A Wireless World," Proceedings Of The IEEE v. 94 no. 2 Feb. 2006 http://www.cs.ucla.edu/~hyang/paper/ProcIEEE05.ps
- [Xenakis04] Xenakis, C., et. al., "Security In Third Generation Mobile Networks," Computer Communications 27 (2004) pg.638 to 650 http://www.cs.uakron.edu/~dang/CS655/Spring05/3G.pdf
- [Balderas04]Balderas-Contreras, T., et. al., "Security Architecture in UMTS Third Generation Cellular Networks," Coordinación de Ciencias Computacionales INAOE, Reporte Técnico No. CCC-04-002 27 de febrero de 2004 http://ccc.inaoep.mx/Reportes/CCC-04-002.pdf
- [Fernandez05-1] Fernandez, E., et. al., "An overview of the security of wireless networks," Handbook of Wireless LANs, CRC Press (2004) http://polaris.cse.fau.edu/~ed/WirelessSecSurv4.pdf
- [Fernandez05-2] Fernandez, E., et. al., "Some security issues of wireless systems," Advanced Distributed Systems: 5th International School and Symposium, ISSADS 2005, Guadalajara, Mexico, January 24-28, 2005, Revised Selected Papers http://www.cse.fau.edu/%7Eed/Fernandez_ISSADS2005Final.pdf
- [Lauter04] Lauter, K., "The Advantages Of Elliptic Curve Cryptography For Wireless Security," Wireless Communications, IEEE Feb 2004 Volume: 11, Issue: 1 On page(s): 62- 67 http://research.microsoft.com/~klauter/IEEEfinal.pdf
- [Xu04] Xu, W., et. al.,"Channel Surfing and Spatial Retreats: Defenses against Wireless Denial Of Service," Proceedings of the 2004 ACM workshop on Wireless security, 2004 http://www.winlab.rutgers.edu/~trappe/Papers/WiDoS_Wise04.pdf
- [Carneiro04] Carneiro, G., "Cross-Layer Design In 4G Wireless Terminals," IEEE Wireless Communications, 2004 http://paginas.fe.up.pt/~mricardo/doc/journals/crossLayerDesign.pdf
- [Gehrmann04] Gehrmann, C., "Manual authentication for wireless devices," RSA Cryptobytes, 2004 http://www.isg.rhul.ac.uk/~cjm/mafwd4.pdf
- [Zhu04] Zhu, J., "A new authentication scheme with anonymity for wireless environments," Consumer Electronics, IEEE Transactions on Publication Feb 2004 Volume: 50, Issue: 1 page(s): 231- 235 http://www.csl.mtu.edu/cs6461/www/Reading/Zhu04.pdf

Back to Table Of Contents

List Of Acronyms

- 1G - First Generation Cellular Networks
- 2G - Second Generation Cellular Networks

- 3G - Third Generation Cellular Networks
- 3GPP - 3rd Generation Partnership Project
- 4G - Fourth Generation
- AMPS - Advanced Mobile Phone System
- CDMA - Code Division Multiple Access
- CDPD - Cellular Digital Packet Data
- D-AMPS - Digital AMPS
- EDGE - Enhanced Data Rate for GSM Evolution
- GGSN - Gateway GPRS support node
- GPRS - General packet Radio Service
- GSM - Global System for mobile communication
- HSCSD - High Speed circuit switched Data
- IMT - International Mobile Telecommunications
- ITU - International Telecommunication Union
- NA-TDMA - North American Time Division Multiple Access
- NMT - Nordic Mobile Telephony
- PCS - Personal communication services
- PDC - Personal Digital Cellular
- SGSN - Service GPRS Support Node
- TD-SCDMA - Time Division-Synchronous Code Division Multiple Access
- UMTS - Universal Mobile Telecommunication System
- W-CDMA - Wideband CDMA

Back to Table Of Contents

Last Modified: April 23, 2006

Note: This paper is available online at http://cse.wustl.edu/~jain/cse574-06/ftp/CellularSecurity/index.html