www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1263-1267

Wireless Cellular Communications Security Issues and Types of Attacks with WAP

K.V.N.R.Sai Krishna
Dept. of Computer Science
S.V.R.M.College Nagaram,
Guntur (Dt), A.P, INDIA
E-mail: saikrishna@svrmc.edu.in

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 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.*

Keywords: Wireless Application Protocol (WAP), 3G Network, HTTP Protocol, Denial Of Service (DOS), Cipher Key (CK), Key Agreement Process (AKA), International Mobile Equipment Identifier (IMEI), Wireless Datagram Protocol (WDP)

I. 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

II. SECURITY ISSUES IN CELLULAR COMMUNICATIONS

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.

III. LIMITATIONS OF CELLULAR COMMUNICATIONS

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.

IV. SECURITY ISSUES IN CELLULAR COMMUNICATIONS

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 .

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.

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.

V. 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.

VI. 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.

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. Figure1 [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.

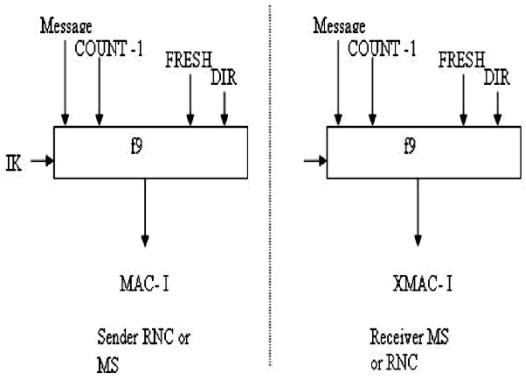

Fig 1. Signaling Data Integrity Mechanism

The confidentiality algorithm is known as f8 and it operates on the signaling data as well as the user data. Figure 2 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.

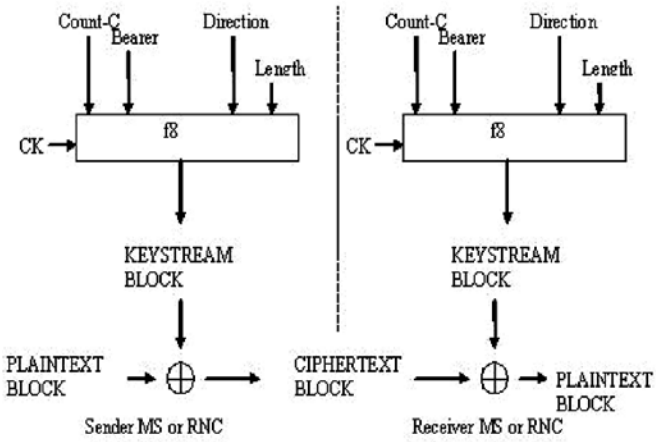

Fig 2. Air Interface Confidentiality Mechanism

For more information on the inputs to the f8 and f9 algorithms,. 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.

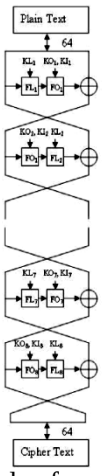

Fig 3. KASUMI Block Cipher

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 3, 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.

VII WIRELESS APPLICATION PROTOCOL

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 4 and Figure show the protocol stack for WAP1 and WAP2 respectively.

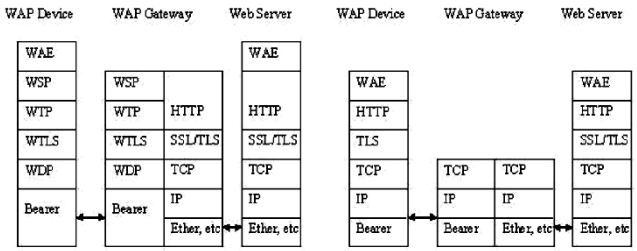

Fig 4. WAP1 Protocol Stack

Fig 5 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.

VIII FORTHCOMING

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.

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 .

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.

IX Conclussion

Cellular Communications 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.

X References

[1] Fernandez, E., et. al.,"An overview of the security of wireless networks," Handbook of Wireless LANs, CRC Press.

[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.

[3] Imai, H., et. al.,"Wireless communications security," Boston: Artech House, 2006

[4] Xenakis, C., et. al.,"Security In Third Generation Mobile Networks," Computer Communications 27 (2004) pg.638 to 650.

[5] 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.

[6] Gehrmann, C.,"Manual authentication for wireless devices," RSA Cryptobytes, 2004,.

[7] Carneiro, G.,"Cross-Layer Design In 4G Wireless Terminals," IEEE Wireless Communications,2004