Pranali Dhete, Dr. B.B. Meshram / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 3, pp.860-863

Preventive Measures For MITM in 3G-WLAN Integrated System

Pranali Dhete, Dr. B.B. Meshram
Computer Department, VJTI, Matunga,
Mumbai-400019,India

Abstract-
The 3G-WLAN integrated system provides communication with high bit rate and wide area coverage. On the other hand it is also susceptible to attack like non-repudiation, DoS, MITM etc. There can be many problems like data integrity, fraud in wireless communication. To avoid this various preventive measures can be taken so as to provide secure communication over the integrated network. In this paper, we list the various types o attacks that can be possible in 3G-WLAN integrated system. Later the attack MITM is discussed with its proposed solution.

Index terms – Attacks, 3G-WLAN, MITM

1. INTRODUCTION

The 3G-WLAN integrated system has becoming very popular and can provide better services to the world. While providing these services the main concern is secure communication between 3G and WLAN. There are various security measures are provides for individual 3G and WLAN technologies. To maintain secrecy and security during the telecommunication session through UMTS, the service network (SN) must authenticate the identity of the mobile station (MS) through MS's home environment(HE) before SN serves for the MS. The UMTS's Authentication and Key Agreement (AKA) protocol was proposed by the 3GPP (3rd Generation Partnership Project) for this purpose. [1]

While in case of WLAN various security measures are implemented for secure communication between one wireless device to another.

To achieve the security in 3G-WLAN integrated system, we have considered the possible attack on individual technology and tried to identify what all attacks are possible on this integrated system.

When communication takes place between 3G and WLAN, vertical handover occurs in which there is high possibility of attack. As the data is opened for attacker when it travels from one network to another , attacker can attack and try to identify the message or data that is being transmitted. To achieve secure communication various protocols and techniques have been used. The most common attack is MITM and in this paper counter measure for this attack is provided.

1. RELATED WORK

The author Muhammad sher and Thomas Magedanz have done the similar work of identifying the possible attacks on 3G-WLAN integrated system. They have identified the security attack scenarios which are as follows:

The attacks listed below are likely to happen in two main areas. WLAN and AP.

1) Possible attacks in WLAN

- The attack can be made directly on WLAN user equipment. In this attacker may implant malicious software and try to launch Distributed DoS attack.
- The attacker can use his own equipment for the attacks like man-in-the-middle which is possible during authentication ,or attacker can fake a network or commercial site.
- He can also fake configuration of control messages such as ARP or ICMP to redirect user's message.

2) Possible attacks on AP

- Attacker may use rough APs to flood the communication with SYN signals.

By considering these scenarios and the types of possible attacks, a secure mechanism should be applied to communication takes place between

heterogeneous network.

In case of UMTS network as, UMTS-AKA protocol is used to overcome the communication overhead for delivering the AVs. This helps in the scenarios when message being sent from WLAN to 3G and vice-versa, the attacker gets little time to track the session and identify the session key.
The main problem occurs due to delay in the communication on the network, so to reduce this delay is of main concern in man-in-the-middle attack.
There are 2 phases authentication and key establishment. In phase 1, the SN receives AVs by delivery of the MS'sidentity IMSI/TMSI to the HE, where IMSI is the International Mobile Subscriber Identity and TMSI is the Temporary Mobile Subscriber Identity. Upon receipt of the message, HE sends an authentication data response back to SN, including an ordered array AV [1 ...n] of authentication vectors. Each authentication vector, also called a quintet, consists of five components: a random number RAND; an expected response XERS = f2k(RAND); a cipher key CK = f3k(RAND);an integrity key IK = f4k(RAND); and an authentication token AUTN = SQN ⊕ AK‖AMF‖MAC , where AK=f5k(RAND),MAC=f2k(SQN‖RAND‖AMF), and ‖ denotes concatenation, ⊕ is bit-wise exclusive-or operation. The anonymity key AK is used to conceal the sequence number as the latter may expose the location of the user. If no concealment is needed, is set to 0. In each authentication vector, an authentication and key management field AMF is included, which serves to define operator-specific options in the authentication process, e.g., the use of multiple authentication algorithms or a limitation of key lifetime. In addition ,HE increases SQN by 1 for each above quintet.
In Phase 2, there are n sets of AV for n times of AKA between the MS and the SN. Each time, SN selects the next unused authentication vector from the ordered array of authentication vectors in its database and send the RAND and AUTH to MS. Upon receipt of RAND and AUTn,MS computes the anonymity key AK = f5k(RAND) andretrieves the sequence number SQN =(SQN ⊕AK)⊕AK. Then MS computes f1k(SQN‖RAND‖AMF) and compares this with the included MAC in AUTN. If they are different, MS sends a user authentication reject message back to SN with an indication of the cause and abandons the procedure. Otherwise, MS verifies if the received sequence number SQN is in the correct range, i.e., SQN > XSQN.
If MS considers the sequence number to be not in the correct range, it sends a synchronization failure message back to SN.In this case, HE may need to resynchronize the counter SQN maintained for the mobile station. More information about resynchronization refers to [3]. If the sequence number SQN is considered to be in the correct range, the authentication of the network is successful. In this case, MS computes RES = f2k(RAND) and sends it back to SN. Next, MS sets XSQN equal to SQN if SQN > XSQN. Lastly MS computes the cipher key CK = f3k(RAND) and the integrity key IK = f4k(RAND). Upon receipt of the user authentication response, SN compares RES with the expected response XRES from the selected authentication vector. If RES is equal to XRES, the authentication of the user is successful and SN selects the cipher key CK and the integrity key IK from the selected authentication vector. If RES and XRES are different, SN sends an authentication failure report to HE and abandons the procedure.

When man-in-the-middle attack occurs the

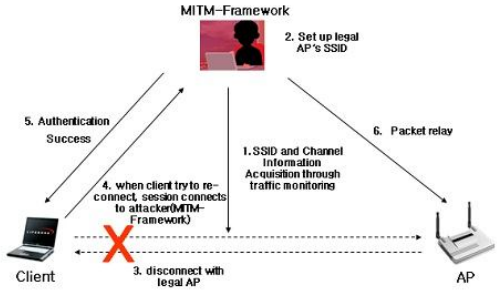

Fig 1. MITM framework flow

Thus MITM attack is possible on 3G-WLAn integrated system.

2. Proposed System

Secure mechanism to detect and avoid MITM attack.

The one possible solution to detect and avoid MITM attack is to use digital signature. Digital signature is the encrypted hash of the message that is send along with the message. In this first hash of message being sent is calculated using SHA or

MD5. Hash value is the sent with sender's private key called as signature. This ensures that the communication is taking place between two

authenticated user. But the message being sent with hash value also need to be encrypted. The flowchart of message

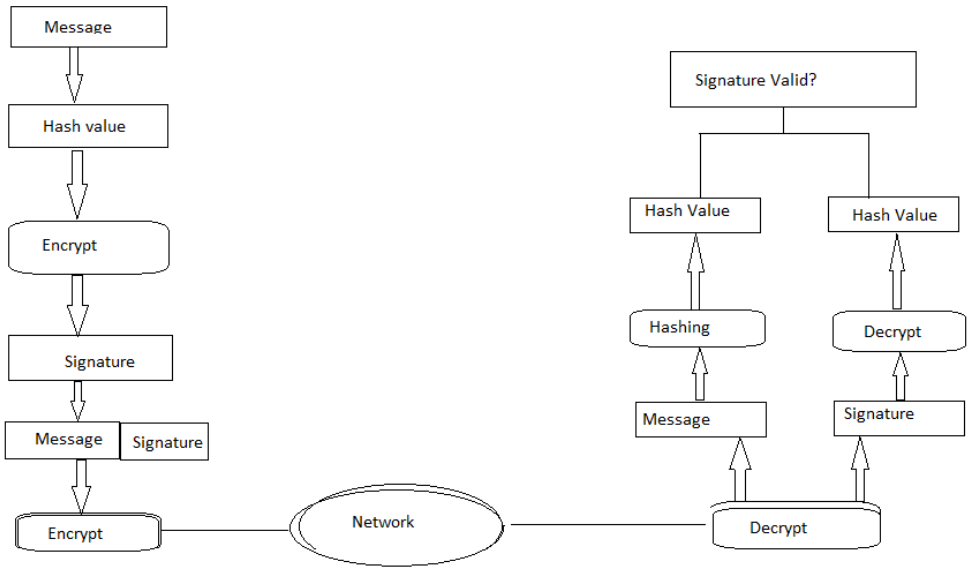

Fig 2. Flowchart of message and hash encryption

encryption with hash value is as shown in fig 2. The hash value of data is calculated.
Data or message contain following elements:

- EAP ID
- Password

This Hash value is calculated by function MD5. Then it is encrypted by Cipher key

CK = f3k(RAND)

This turns as signature. This signature along with the message is sent over the network. Before that message is encrypted with Integrity key.

IK = f4k(RAND)

When receiver receives the response it will decrypt the message and signature.
Recalculate hash value of message and check with the received hash value.

If man-in-the-middle attack occurs and though attacker gets session-id it will be hard for him to generate same hash of message as the function used for hashing will be unknown to attacker. So when attacker tries to establish the connection with other user in the communication and sends message, the other user will check the hash value as he has the legitimate copy of the function to calculate the hash value. Thus the man-in-the-middle can be detected and prevented by using digital signature.

3. CONCLUSION

We identified the various possible attacks on 3G-WLAN integrated system and the attack scenarios where attack can be possible. We found that man-in-the-middle attack is the most common attack on the integrated system. We used all these details to study and propose new system to detect and prevent man-in-the-middle attack. The attack can be detected using digital signature concept which uses hash value of the message to ensure authentication, confidentiality and integrity of the message. The advantage of hash function is that it is faster, give small output with high computational power.
Thus man-in-the-middle attack can be avoided.

REFERENCES

[1] “Security Analysis of a Cocktail Protocol with the Authentication and Key Agreement on the

UMTS”, Shuhua Wu, Yuefei Zhu, and Qiong Pu, 2010
[2] “Fraud In Roaming Scenarios: An Overview”, Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, And Jesus Diaz-Verdejo, December 2009.
[3] “A Service-Agent-Based Roaming Architecture for WLAN/Cellular Integrated Networks”, Minghui

Shi, Humphrey Rutagemwa, Xuemin Shen, Jon W. Mark, and Aladdin Saleh, September 2007.
[4] “Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol”, Muxiang Zhang and Yuguang Fang, March 2005.
[5] “An Introduction To Access Security In Umts”, Geir M. Køien, Telenor R&D And Agder University College, February 2004
[6] “Security Aspects of 3G-WLAN Interworking” , Geir M. Køien and Thomas Haslestad, Telenor R&D, Norway, November 2003
[7] “Improving Mobile Core Network Security with Honeynets” , 2007
[8] “A Fast Handover Authentication Mechanism Based on Ticket for IEEE 802.16m” , Anmin Fu, Yuqing Zhang, Zhenchao Zhu, and Xuefeng Liu, December 2010.
[9] “Interworking Techniques And Architectures For Wlan/3g Integration Toward 46 Mobile Data Networks”, Apostolis K. Salkintzis, Motorola, June 2004
[10]“HandoverManagement Architectures In Itergrated WLAN/Cellular Network”, George Lampropoulos, Nikos Passas, And Lazaros Merakos, Alexandros Kaloxylos, 2005