"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

APPLYING IPSEC IN RADIO NETWORKS FOR ENHANCED SECURITY

Cristian-Gabriel APOSTOL[1]
Vlad Mihai COTENESCU[2]
Ciprian RACUCIU[3]
[1]Eng. Electronics and Telecommunications Faculty, Doctoral School, Military Technical Academy
[2]Eng. Electronics and Telecommunications Faculty, Doctoral School, Military Technical Academy
[3]Prof. Ph.D. Electronics and Telecommunications Faculty, Doctoral School, Military Technical Academy

Abstract: *Mobile radio networks offer many advantages and provide a certain level of security. While the standards advance, information security and user privacy is regarded as a priority for all involved parties starting from telecom vendors, mobile operators, government and ending with mobile users. In this paper we will analyze the possibility of increasing the security level of cellular networks by combining their technology with the principle of IPSEC.*
Keywords: *Information Security, Radio Networks, IPSEC, transport, tunneling*

Introduction

In present days, network security is a major factor considered by public operators, government, military entities and usual users when implementing and using mobile networks. Radio standards define security services and mechanisms, analyzed and improved overtime by researchers.

Starting from the simple 2G GSM-AKA (Global System for Mobile communications – Authentication and Key agreement) and continuing to recent improvements in 4G LTE EPS-AKA (Long Term Evolution Evolved Packet System - Authentication and Key Agreement), security is in constant development in order to face new challenges like DoS attacks (Denial of Service), MITM (Man in The Middle), Base Station Cloning, IP address spoofing, flooding, and many more. Also there is a wide proliferation of increasingly intelligent handsets that have network connections equal or superior typical PCs. This suggests that the LTE network will be susceptible to aggressive network security attacks [1]

Most radio standards, including 2G, 3G, WiMAX (Worldwide Interoperability for Microwave Access) with the exception of 4G LTE which included in last years the Se-GW (Security Gateway), focus on securing besides authentication, integrity and encryption only on the radio link.

We want to specify that 2G does not perform mutual authentication between the mobile equipment and the network. This means that only the user is authenticated by the network, not also authenticating the network itself. This security flaw makes it possible for attackers to perform man in the middle attacks, by cloning the BTS. The same possibility exists in WiMAX if weak authentication mechanisms are being applied (EAP-MD5, EAP-POTP, EAP-PSK, EAP-PWD, EAP-FAST, EAP-SIM). This is why we recommended in reference [2] the use of EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layered Security) of the PKI (Public Key Infrastructure) and as a second phase of authentication using user credentials. The security level of WiMAX networks is increased in this manner, because we obtain strong authentication and also strong keys for encryption due to this improvement because they are based on the AK (Authorization Key), obtained through the authentication process.

Improvements of 4G LTE security, besides mutual authentication for UEs which is not totally secured, introduce an interesting principle for further studies: The introduction of a new network element named the Se-GW (Security Gateway) which allows the establishment of an IPSEC tunnel between the eNodeB (evolved NodeB) and the Core Network / Data Gateway.

The importance of this principle has deep security improvements for all standards from our perspective because the backhaul is secured between the base stations and the center of the network.

In the present state, 2G, 3G, WiMAX, LTE and many other standards limit the encryption only to the radio link, the wired part connecting the base stations transmit unencrypted traffic containing user calls and data exchanges which can easily be exploited by attackers.

IPSEC principles

The evolution of mobile networks towards the all IP based feature has improved network performance and also it has reduced deployment costs. On the other hand they have inherited the vulnerabilities of IP networks which leaves them open to new security threats.

IPSEC represents a security mechanism which is implemented at the IP layer and is composed by three protocols, as defined by the Internet Engineering Task Force:

- Authentication Header (AH)
- Encapsulation Security (ESP)
- Internet Key Exchange (IKE)

The protocol addresses the following key concepts in information security:

- Confidentiality: data is encrypted in order to prevent disclosure on the transmission path
- Integrity: The receiving entity checks the data in order to prove that is has not been tampered
- Authentication: The data source is authenticated
- Anti-replay protection: identification and rejection of packets sent by attackers

IPSEC relies on Security Associations (SAs) for successful deployment: IPSEC SAs and IKE SAs. The SAs define security policies which can be negotiated between communicating peers in order to protect service flows.[3] The security policies include:

- Security protocols
- Encapsulation modes
- Verification algorithms
- Encryption algorithms
- Encryption keys and expiration time of keys

For packet encapsulation, IPSEC defines two modes: transport mode and tunnel mode.

a) Transport Mode IPSEC

In transport mode an AH header is inserted after the IP header before the payload.

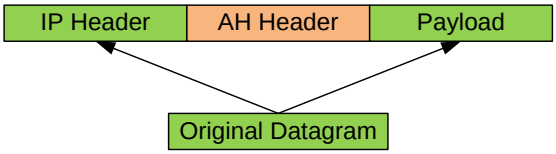

Figure 1: AH Encapsulation in IPSEC Transport mode

EPS header is inserted after the IP header At the rear of the packet we will find the ESP trailer and an ESP authenticator.

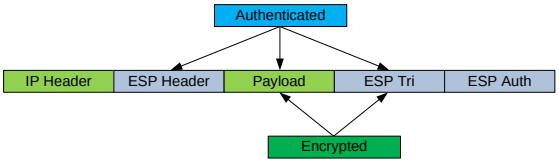

Figure 2: ESP Encapsulation in IPSEC Transport mode

In the IPSEC transport mode. The source IP is the BTS IP and the destination IP is the Se-GW.

b) Tunnel Mode IPSEC

In tunnel mode, the original IP header is encrypted resulting in a new IP header used for routing.

In this working scenario the AH is prefixed to the IP header of the initial packet, and a new IP header is assigned before the AH header.

Figure 3: AH Encapsulation in IPSEC Tunnel mode

Tunnel mode also supports ESP header in which this segment is prefixed to the IP header of the initial packet, and a new IP header is prefixed to the ESP header.

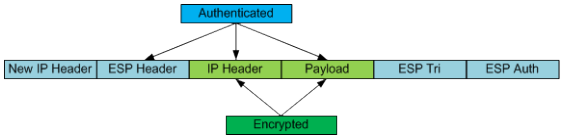

Figure 4: ESP Encapsulation in IPSEC Tunnel mode

There are some variable fields in the IP packet such as Checksum, Type of Service and Time to Live for which AH does not provide integrity protection because these fields are variable and can be modified during transmission by valid network requirements.

Security algorithms in IPSEC

a) Encryption algorithms

The logical reason for encryption is to prevent eavesdropping during packet transmission. Symmetric algorithms are used, this means that the same key is used for encryption and also for decryption.

The compatible IPSEC algorithms are:

- DES (Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- AES with key lengths of 128, 192 or 256 (Advanced Encryption standard)

AES provides a higher level of security and also faster performance. The next from a security point of view is 3DES, but regarding performance it takes longer to encrypt. DES is not recommended our days because it provides weak security compared to the attackers capabilities and todays performances in processing power.

b) Integrity algorithms

Both AH and ESP encapsulation modes can verify the integrity of IP packets, based on hash functions which have for input variable messages and generate fixed length outputs.

The result of the hash function is also known as a hash digest. When receiving a message the SeGW on one side or the BTS on the other side, calculate the digest and compares it with the one carried in the packet. If they are the same, it is assumed that the data has not been tampered, and if they don't coincide the packets are discarded.

The algorithms which can be used by IPSEC are:

- MD5 (Message Digest Algorithm 5)[4]
- Secure Hash Algorithm 1 (SHA-1)[5]
- Secure Hash Algorithm 256 (SHA-256)
- AES-XCBC (cipher-block-chaining)-MAC-96 (Message Authentication Code) [6]

Among these algorithms, MD5 has a low security level and is not recommended for use for more than 4 years. [6]

Improvement of Radio Network Security with IPSEC

In 2G the IPSEC tunnels established between the BTS and the SeGW inserted before the BSC can protect all traffic (user plane and control plane) over the Abis interface.

Figure 5: Standard connection between 2G/3G/4G (WiMAX/LTE) Network elements

In tunnel mode, a SeGW must be deployed on a network to separate the security and non-security domains. The Se-GW must support encapsulation in tunnel mode, integrity check and encryption.

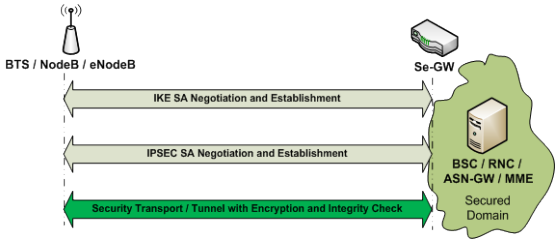

Figure 5: Proposed Improvement with the IPSEC Procedure in Cellular / Wireless Arhitecture

In EPS tunnel mode the New IP header is the BTS IP and the peer IP is the Security Gateway. If the transceiver does not encrypt packets and the receiver does not decrypt them, then the tunnel mode is used for secure communication.

Conclusions and perspectives

Before IPSEC is introduced, the base stations transmit data in plaintext.This is a big security issue for 2G,3G, WiMAX and LTE because backhaul traffic can be eavesdropped.

Packets transmitted over an insecure link are very vulnerable to interception and malicious modification.

IPSEC provides transparent security services between the IP communicating entities, thereby protecting the emerging radio networks from cyber-attacks.

The tunnel mode provides higher security than the transport mode because the original entire initial packet is encrypted and integrity protection mechanisms are performed.

The advantage of transport mode is that it provides better transmission performance because a new IP header is added in case of tunnel mode, so the used bandwidth is increased.

When choosing between the tunnel and transport IPSEC encapsulation modes, the telecommunication engineers must put in balance the security requirement versus the network performance requirement, because both modes have certain strong points.

Bibliography

[1] D. Herceg, "LTE Transport Security", MIPRO Proceedings of the 34th International Convention, 23-27 May 2011, pp. 1464 – 1467, Opatija, Croatia

[2] C-G. Apostol, C. Racuciu, "Improving Mobile WiMAX EAP–TTLS Authentication with Minimum Downtime and Securing its Management Channel", Paripex Indian Journal of Research, Vol. III, Issue: VI, June, 2014

[3] SingleRAN, IPSEC Feature Parameter Description, Issue 2, 15.09.2015, Huawei Technologies CO., LTD.

[4] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", Internet Engineering Task Force - Request For Comments (IETF RFC) 2404

[5] C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", Internet Engineering Task Force - Request For Comments (IETF RFC) 2403, November 1998.

[6] S. Frankel, H.Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", Internet Engineering Task Force - Request For Comments (IETF RFC) 3566, September 2003

Acknowledgement

This paper has been supported by the HORIZON 2020 project of the International Economy Institute, represented by the Electronics Doctoral School of the Military Technical Academy in Bucharest, Romania