Providing Security challenges in 4G Systems

Dhiraj D.Shirbhate, Snehal G.Ingole

Abstract— Several research groups are working on designing new security architectures for 4G networks such as Hokey and Y-Comm. Since designing an efficient security module requires a clear identification of potential threats, this paper attempts to outline the security challenges in 4G networks. A good way to achieve this is by investigating the possibility of extending current security mechanisms to 4G networks. The results show that due to the fact that 4G is an open, heterogeneous and IP-based environment, it will suffer from new security threats as well as inherent ones. In order to address these threats without affecting 4G dynamics, we propose an integrated security module to protect data and security models to target security on different entities and hence protecting not only the data but, also resources, servers and users.

Index Terms— *4G systems, IEEE X.805, IPV6 protocol, Integrated Security Layers, Targeted Security Models.*

INTRODUCTION

Due to some security weaknesses in 2/2.5G networks and the need to support voice and data transmission, third generation (3G) networks have been recently deployed. Aside from supporting multimedia communication, 3G-based technologies, e.g., Universal Mobile Telecommunications System provide new services such as location dependent services, which along with the support of voice and high quality video traffic are the major innovations, compared to 2G technologies. Furthermore, 2G's main security weaknesses have been tackled in 3G systems; a more generic Authentication and Key Agreement (AKA) method has been developed. In addition, integrity and stronger encryption mechanisms have been introduced. However, due to the increasing demand for ubiquitous connectivity and service provision, there is growing momentum to move towards Beyond 3G or 4G communication systems. 4G networks represent an open environment where different wireless technologies and service providers share an IP-based core network to provide uninterrupted services to their subscribers with almost the same quality of service (QoS). In 4G systems, mobile devices are expected to switch between networks of different operators and technologies; this is referred to as vertical handover and it is required to maintain the Service Level Agreements (SLAs) needed by their applications. It is no longer the case that security for communication frameworks is considered as an add-on rather than a fundamental issue. Future communication systems consider security from the initial stages of the design process. This is reflected in the design of 4G architectures such as Y-Comm where security is considered as an integral part of the design. However, in order to develop an efficient security module, it is necessary to identify the threats and risks faced by communication systems. But since analyzing security requirements of communication systems is quite complex, the ITU introduced a systematic analysis tool called X.805 as a holistic approach to network security by discussing systems security requirements at different levels and pinpointing potential network vulnerabilities. In this paper, we examine whether it is possible to use 3G security mechanisms such as for 4G systems.

Firewall:

Firewall enforces a security policy on data from and to a corporate network. Established at the borders of core network. Application firewalls prevent direct access through the use of proxies for services.

3G User/Application Domain Security

User Domain Security

Ensures secure access to the Mobile Station. Based on a physical device called UMTS Integrated Circuit Card.

USIM

Represents and identifies a user and association to his Home Environment. Responsible for subscriber and network authentication. USIM authenticate user by secret (e.g. a PIN) Terminal authenticate USIM by a secret Application Domain Security Deals with secure messaging between the MS and the Serving Network or the Service Provider. Remote application should authenticate a user. Application-level security mechanisms are needed. Because the lower layers' functionality may not guarantee end-to-end security.

Wireless Application Protocol (WAP) WAP is a suite of standards for delivery and presentation of Internet services on wireless terminals. Taking into account the **limited bandwidth** and **processing capabilities** of mobile devices. To connect wireless domain to the Internet **WAP gateway** is needed.

Two releases –

V1.2.1 and v2.0

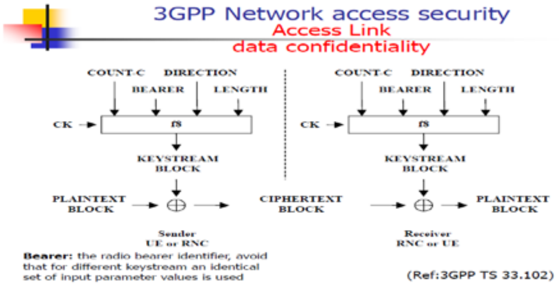
WAP 1.2.1

To secure data transmission in WAP Wireless Transport Layer Security (WTLS) based upon the TLS WAP device and WAP Gateway.

WTLS
WAP Gateway and Web server TLS Does not support end-to-end security

WAP 2.0

Re-design of the WAP architecture.
Introducing Internet protocol stack including the Transmission Control Protocol (TCP).
TCP-level gateway allows for two versions of TCP. One for wired and the other for wireless TLS channel can be established all the way from the mobile device to the server.


3GPP Network access security
Access Link
data confidentiality

Bearer: the radio bearer identifier, avoid that for different keystream an identical set of input parameter values is used

(Ref:3GPP TS 33.102)

3GPP Network access Security

3G Weaknesses and Proposed Improvements 3G Architecture Weaknesses

Backup procedure for TMSI reallocation. IMSI confidentiality in wireline part

Firewall Issues

WAP Architecture (V1.2.1) Data Privacy Voice Call Transcoded Threat Backup Procedure for TMSI Reallocation.VLR cannot associate the TMSI with the IMSI because of TMSI corruption or database failure when the user roams, and the SN/ VLRn cannot contact the previous VLRo.

Voice Call Transcoded Threat

Voice calls may need to be transcoded when they cross network borders. Such as, bit rate change it is not possible to apply such transformation on an encrypted signal. Signal has to be decrypted before transcoding. Network-wide confidentiality lacks flexibility.

3G security weakness and Security Issues

Important Changes in Security Defeat the false base station attack. Key lengths were increased. Support security within and between networks Integrity mechanisms.

Types of Attacks

Eavesdropping Impersonation of a user Impersonation of the network Man-in-the-middle Compromising authentication vectors in the network

3G Security Feature

3G network enhances much vulnerability in 2G. Many 2G attacks are not suitable for 3G network.

Denial of service Attack

De-registration request spoofing the intruder spoofs a de-registration request (IMSI detach) to the network Location update request spoofing User spoofs a location update request in a different location area camping on a false BS/MS

Denial of Service Solution

Integrity protection of critical signaling messages Location update request spoofing and Deregistration request spoofing. In Camping on a false BS/MS Integrity can't prevent the false BS/MS ignoring certain service requests and/or paging requests.

Identity Catching Attack

Passive identity catching requires a modified MS. Expect network may sometimes request the user to send its identity in plaintext. Active identity catching Requires a modified BS Requests the target user to send its permanent user identity in plaintext.

Identity Catching Attack Solution

Identity confidentiality mechanism counteracts this attack Encryption key shared by a group of users to protect the user identity when new registrations or temporary identity database failure in the serving.

Eavesdropping on user data

Suppression of encryption between the target user and the true network Modified BS/MS When set up a connection, false BS/MS modifies the ciphering capabilities of the MS; network may then decide to establish an un-enciphered connection.

Eavesdropping on user data Solution

Message authentication and replay inhibition of the mobile's ciphering capabilities. Network can verify that encryption has not been suppressed by an attacker.

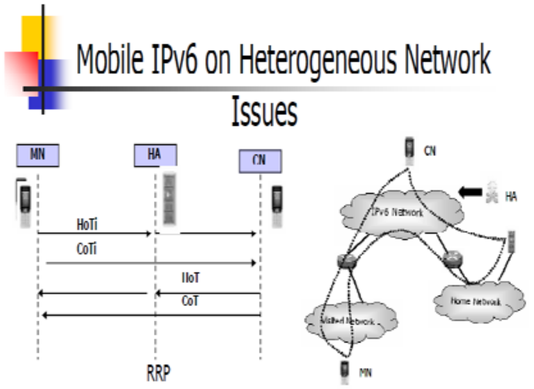
4G Security

4G Security Issues

QoS and Security

Seamless integrated Mobility, QoS and Security Delay across different networks for QoS Privacy
AAA for 4G Heterogeneous Network Mobility

Mobile IPv6 with inherent problems of IP Security and Handover



Mobile IPv6 on Heterogeneous Network Issues

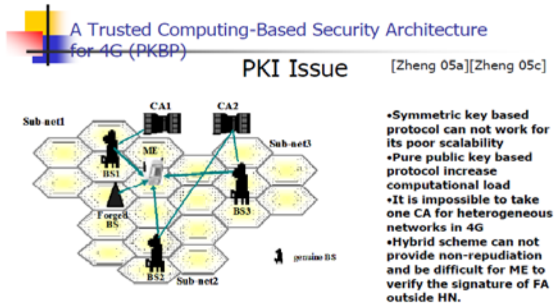
When handoff in heterogeneous network Acquire a new CoA (Care of Address) only, Security Association (SA) between HA and MN is not impacted (MIPv6 Routing Header Type2 and Home address option are transparent to IPSec SA) Kbm is encapsulated in BU RRP (Return Routability Procedure) mechanism is vulnerable to attacks along the path between the HA and the CN, where a malicious node, aware of a session between MN and CN, might simulate a handoff of the MN by sending fake HoTI and CoTI messages. > Impersonation attack/Man-in-the middle attack (Adversary can obtain Kbm and send fake BU to CN or MN) When MN roams away from its HN => Binding new address by sending Binding Update (BU) message to HA by RRP.

An Approach of Secure Mobile IPv6

1. At set-up, Kbm distribute to MN and CN within the body of the SIP 200 OK and ACK message
=> Instead of RRP.
2. Kbm can be generated by AAA Server.
3. The distribution of keys is secured by IPSec and ESP between SIP user (MN and CN) and P-CSCF.
As the SA is not impacted, a solution is:

•Every handoff => update BU,

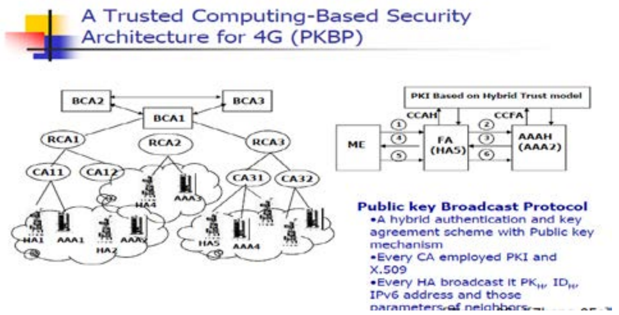
•On each path, IPSec or ESP is employed to protect the distribution of key.



A Trusted Computing-Based Security Architecture for 4G (PKBP)

PKI Issue [Zheng 05a][Zheng 05c]

•Symmetric key based protocol can not work for its poor scalability
•Pure public key based protocol increase computational load
•It is impossible to take one CA for heterogeneous networks in 4G
•Hybrid scheme can not provide non-repudiation and be difficult for ME to verify the signature of FA outside HN.



A Trusted Computing-Based Security Architecture for 4G (PKBP)

Public key Broadcast Protocol
•A hybrid authentication and key agreement scheme with Public key mechanism
•Every CA employed PKI and X.509
•Every HA broadcast it PK_H, ID_H, IPv6 address and those parameters of neighbors

•It is very difficult for ME to verify the validity of BS's publickey certificate since ME and BS usually belongs to different CA.
• It is hard to achieve mutual authentication between ME and FA, and ME is vulnerable to be cheated by forged BS/FA.
A Trusted Computing-Based Security
Architecture for 4G (PKBP)
The PKBP Scheme achieved :
1. Authentication on heterogeneous networks
2. Against the man-in-the-middle attack
3. Mutual authentication
4. Anonymity and Non-repudiation
5. Security of key agreement

CONCLUSION

In this paper we have demonstrated that the security requirements for 4G systems are much greater than those of 3G. A lot of this is due to the fact that in 4G systems we require a more open architecture with its inherent security vulnerabilities compared to the closed network of 3G systems. These requirements clearly indicate that we need an integrated security module to protect data across different networks and in addition, we need targeted security models to protect various entities: users, servers and network infrastructure.3GP provided more security mechanisms than 1G and 2G as- Mutual authentication, stronger confidentiality and integrity, …,etc. 3G and 4G still exists some problems as - privacy, DoS, IMSI: plaintext,….etc. Convergence of heterogeneous networks, for example, 4G, is an important trend, and exists a lots of issues as - Seamless connection, high mobility, QoS, secure service,…,etc. All-IP is an important and necessary environment for communication networks

ACKNOWLEDGEMENT

I express my sincere gratitude to **Resp. Dr A. D. Gawande sir**, Head of the Department, Computer Science & Engineering & Resp.Prof V.T. **Gaikwad sir** for providing their valuable guidance and necessary facilities needed for the successful completion of this seminar throughout. I am also obliged to our principal, Resp. **Dr. S. A. Ladhake** who has been a constant source of inspiration throughout.

Lastly, but not least, I thank all my friends and well-wishers who were a constant source of inspiration.

REFERENCES

[1] [3GPPTS202] 3GPP TS 35.202 V3.1.1 Technical Specification.

[2] [3GPPTS205] 3GPP TS 35.205 V6.0.0 Technical Specification.

[3] [3GPPTS201] 3GPP TS 35.201 V6.1.0 Technical Specification.

[4] [3GPPTS121] 3GPP TS 23.121 V3.6.0 Technical Specification.

[5][Zheng05a] Yu Zheng, Dake He; Lixing Xu and Xiaohu Tang, "Security scheme for 4G wireless systems," Proceedings. 2005 International Conference on Communications Circuits and Systems, Vol. 1, Page(s):397 – 401, May 2005 .

[6][Joseph06] Joseph, V.C.and Talukder, A.K.;" Verifiable AKA for beyond 3G wireless packet services," 2006 IFIP International Conference on Wireless and Optical Communications Networks, pp. 11-13 April 2006.

[7] [Zhang05] Muxiang Zhang and Yuguang Fang; "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Transactions on Wireless Communications, Vol. 4, No. 2, PP. 734-742, March 2005.

[8] [Barba93] Barba, A., Recacha, F. and Melus, J.L., "Security architecture in the third generation networks," Proceedings of IEEE Singapore International Conference on Networks,1993. International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Volume 1, PP. 421 - 425 , Sept. 1993 .