Security Analysis of 3G—WLAN Fusion

Dongya Chen [1,2]
1. Department of Physics and Information Engineering
Jining University
Qufu 273155,PR China
2. School of Information Science and Engineering,
Shandong University
Jinan 250100,PR China
e-mail: chendya@126.com; corresponding author: chendya@126.com

***Abstract*—With development of wireless Internet, the interworking of the third generation(3G) and wireless Local Area Network(WLAN) has become a focus research. Fusion of 3G—WLAN has complementary advantages. The background and scheme of 3G and WLAN Fusion are discussed. The security of Fusion was analysed. Presents two security Fusion schemes has given. The first is called a loose coupling, The second is called close coupling. Two schemes are complement each other, realize the 3G and WLAN user unified management and 3G signing based on user WAPI security mechanism of WLAN access, and protect the user privacy.**

Keywords- Fusion;Safety;Loose coupling; Close coupling; Verification

I. INTRODUCTION

Safety is the third generation and wireless Local Area Network（3G –WLAN）converged network is one of the major challenges faced by, and the integration of network need to deal with WLAN and 3G security threats at the same time. Because 3G and WLAN network system structure and security threats have difference. The security solution is putting in very big difference. Universal Mobile Telecommunications System（UMTS）is the key to the authentication and the third generation mobile communication network and Authentication and Key Agreement(AKA). And WLAN have IEEE802. 11i and Wireless LAN Authentication and Privacy Infrastructure (WAPI) the two different safety systems. Single security solution can't provide a complete safety guarantee. How to access network integrates different heterogeneous security system structure is the important problem to solve.

The existing scheme is mainly directed against the IEEE 802.11i and 3G security system security fusion not in WAPI and 3G security system security integration solutions. One obvious solution is in the User Experience(UE) to 3G network signing register, to issue the certificate of WAPI, and to establish certificate and International Mobile Subscriber Identification Number(IMSI) mapping relations. Due to the limitation of WAPI mechanism, the scheme exists the following questions:

(1) The scheme can't realize the user identity privacy protection. On the one hand, users don't want to expose his identity; On the other hand, users don't hope the agreement before the execution to be a third party to link.

(2) UE need to be stored more operator's certificate to support the roaming. The reason is the existing WAPI standard does not support roaming the authentication, the user must have the corresponding certificate to access external regional operators WLAN.

(3)Multiple certificate leads to certificate management complex [1].

WAPI and 3G security system safety issues on fusion research. We propose a new USIM based on the certificate distribution agreement, and it has the anonymity and not tracking sex to protect the user identity privacy, at the same time solving the roaming UE and Authentication Service Unit trust relationship problems. Combined with certificate distribution agreement and WAPI - XG1, we give two kinds of safety fusion scheme. The two schemes of the difference is the certificate distribution and WAPI - XG1 between the degree of coupling. The first is called a loose coupling which certificate distribution and WAPI relative independence. UE uses 3G interface card and certificate distribution mechanism application certificate, then uses WLAN interface card in WAPI mechanism Access Access Network. The second is called close coupling which certificate distribution stacks to access WAPI authentication mechanism. Two schemes are complement each other and realize the 3G safety system and WAPI user unified management and 3G signing based on user WAPI security mechanism of WLAN access.

II. 3G-WLAN FUSION NETWORK SYSTEM STRUCTURE

AN defines the network elements: WLAN AN and UTRAN AN.WLAN AN for UE to provide wireless IP connection, so that UE request can get 3G authentication and authorization of network server. UTRAN AN is UMTS most important access for UE to provide seamless connection service. 3GPP I - WLAN makes 3G users can access in WAPI mechanism roaming, by AN and 3G VPLMN and 3G HPLMN of three parts.

In the 3G VPLMN, SGSN and GGSN is the core of the UMTS network element. 3GPP AAA Proxy completes AAA agent and filter function. WLAN Access Gateway completes data forwarding functions, for UE providing 3G PS domain service and Internet Access services. Packet Data Gateway

Published by Atlantis Press, Paris, France.

will be exist at the of network, also can be located in ownership network. Through the PDG we can access 3G PS field service, and setting up tunnel is the user Data transmission of the important levels. VASU is domain ASU, in order to support the expansion of WAPI network elements, which mainly completes user certificate management and user identity authentication. VASU is the logical entity that can with other network elements coexist in a physical entity, also can exist independently.

3G HPLMN has two kinds of network element: 3GPP AAA Server and HSS. AAA Server completes AAA function as well as the PDG,WAG and WLAN AN providing authorization, strategy implementation and routing information. HSS storage users access to Internet service need of the authentication information and service subscription information, is essentially an information database. HASU ownership domain ASU, in order to support the expansion of WAPI network elements, mainly completes user certificate management and user identity authentication.

III. Safety Fusion Scheme

This paper proposes certificate distribution plan based on USIM, and UE through the proposal to the HSS apply for temporary certificate. Combined with certificate distribution plan, we put forward two kinds of specific safety fusion scheme. The two schemes have difference between certificate distribution and the degree of coupling between WAPI. The first kind is loose coupling. Certificate distribution and WAPI have relative independence. UE use 3G interface card using certificate distribution mechanism application certificate, then use WLAN interface card in WAPI mechanism access WLAN AN, applicable to 3G - WLAN dual mode UE; The second kind is close coupling. Certificate distribution stacks to WAPI mechanism, suitable for WLAN single-mode UE. Two schemes are complement each other to achieve the safe fusion .[2]

A. Loose coupling safety fusion scheme

Loose coupling includes two stages: certificate distribution stage and WAPI - XG1 security access stage. In the certificate distribution stage, UE to HSS/HASU request interim certificate, HSS/HASU issues interim certificate to UE, and will send UE VASU certificate for UE establishment and VASU relationship of trust. Certificate distribution process is completed, and UE in WAPI - XG1 mechanism will access WLAN AN. Process as follows [3] :

(1)When UE detects to WLAN signal and hopes that through WLAN access UE random selection SKUE private key is calculated and the corresponding public key PKUE, and will put PKUE and SKUE as interim certificate of public key and secret key. UE to HSS/HASU certificate request to send away CertReq:

{N, PKUE, Epkhasu (IDvasu, IMSI, TMSI, s, COUNTue, MACkuh (IDvasu, IMSI, TMSI, s, PKUE, COUNTue, IDhasu)}

The IDvasu is VASU's identity identification, and it is the HSS/HASU identity identification. IMSI is UE international mobile signing user id; TMSI is UE random selection of temporary identity. S is session identifier; COUNTUE is counter and its purpose is to prevent replay attacks; N is random number challenge, MACkuh is the use of UE main key KUH calculation message authentication code.

(2) After receiving the certificate request message, CertReq HSS/HASU first decryption get IMSI; According to the IMSI, from signing the user database accesss UE main key KUH, and uses KUH verification MACkuh (IDvasu, IMSI, TMSI, s, PKUE, COUNTue, IDhasu) effectiveness. If verification is successful, the HSS/HASU structure UE of the interim certificate Certue:

{PKhasu, TMSI, PKue, T, Sighasu (TMSI, PKue, T)}

The T is the period of validity of the interim certificate. According to the identification of network IDVASU, we search the corresponding certificate Certvasu. HSS send certificate CertRep response message.

(3) Receiving certificate response after the news, the first UE verifies the effectiveness of the interim certificate and signature. If verification is successful, the VASU will join UE trust ASU list. UE success and VASU built a relationship of trust solved WAPI-XG1 roaming trust relationship problems.

(4)Using Certue UE in WAPI mechanism access Internet, UE realized mechanism of the roaming access based on WAPI [4].

B. Close coupling safety fusion scheme

The scheme and the above scheme's difference is that certificate distribution process is superposition to WAPI authentication process. The certificate will be request message CertReq stack to access the authentication request message and certificate the authentication request message, replace UE certificate field. VASU to receive CertReq later, CertReq will be transmitted to HSS. HSS send CertRep to ASU response [5].

(1) AP to send UE authentication activation messages;

(2)Sending UE access the authentication request message to AP, and WAPI - XG1 difference is that will replace CertUE field for CertReq;

(3) AP receiving to access the authentication request news, from CertReq field for PKUE and validation SigUE, it sends certificate the authentication request message to VASU after through verification and its difference between WAPI - XG1 is that will replace CertUE field for CertReq;

(4) First VASU request the certificate the authentication message to resolve the certificate request message CertReq, and after that CertReq will be transmitted to HSS/HASU,

(5) HSS/HASU send certificate response message CertRep to VASU;

(6) To receive CertRep, VASU according to belonging to network identification IDHASU, searches the corresponding certificate CertHASU, and uses CertHASU CertUE validation.After verification, it sends certificate authentication response message to AP. WAPI - XG1 difference is that the certificate will be the authentication response message CertUE field replacement for CertRep;

(7) AP sends access the authentication response message to UE, and WAPI - XG1 difference is that it will replace CertUE field for CertRep;

(8) After CertRep verification and validation through, VASU will be joined UE trust ASU list. UE accesses successful of domain WLAN AN, and VASU built a relationship of trust so as to solve the WAPI - XG1 roaming trust relationship problems.

IV. SUMMARY

This paper studies the 3G and WAPI based on WLAN security problem. It puts forward a new USIM based on the certificate distribution agreement, combined with certificate distribution agreement and WAPI - XG1, and gives two kinds of safety fusion scheme. The first is called a loose coupling, certificate distribution and WAPI relative independence, UE uses 3G interface card using certificate distribution mechanism application certificate, then uses WLAN interface card in the API mechanism access WLAN AN. The second is called close coupling.The certificate distribution stacks to access WAPI authentication mechanism. Two schemes are complement each other, and realize the 3G and WLAN user unified management and 3G signing based on user WAPI security mechanism of WLAN access protecting the user privacy. The next step will through the simulation and test bed, means to the analysis of the contrast between two safety fusion scheme performance, including the calculation of cost and communication costs index.

AKNOWLEDGMENT

This work is Supported by Scientific Research Foundation of Jining University 2009 under Grant # 2009KJLX01.

REFERENCES

[1] Koien GM,Haslestad T.Security Aspects of 3G-WLAN Interworking[J].IEEE Communications Magazine,2003;41(11)

[2] ETSI TR 101 957 Vl.l.l.Broadhand Radio Access Networks(BRSN);HIPERLAN Type 2;Equirements and Architectures for Interworking between HIPERLAN/2 and 3nd generation Cellular systems.2001

[3] Axiotis DI,AI-Gizawi T,Peppas K et al.Services in Interworking 3G and WLAN Environments[J].IEEE Wireless Communications, 2004;11(5):14~20

[4] Buddhikot M,Chandranmenon G,Han S et al.Integration of 802.11 and Third-Generation Wireless Data.Networks [C]. IN:Proc of the INFOCOM 2003,IEEE,2003;503~512

[5] Mahapatra A,Uma R.Authentication in an Integrated 802.1X based WLAN and CDMA2000-1X network[C]. In:Proc of the APCC 2003.

Published by Atlantis Press, Paris, France.