3GPP TSG SA WG3 – S3 #17 **S3-010028**

February 27 – March 2, 2001

Gothenberg, Sweden

Source: Motorola Inc.

Title: Trust Models for IM Domain Security

Document for: Discussion/Decision

Agenda item: tbd

Abstract

This contribution presents an overview about the trust models for IM Domain Security. IM domain security requires a trust model to allow different network nodes to validate a given message with the least overhead. The trust models discussed so far in SA3 are based on a symmetric key approach. In order to incorporate the symmetric key distribution infrastructure, SA3 has had difficulty reaching agreement on the trust models. Furthermore, IM domain service needs interoperability with different service realms. Symmetric key approach cannot provide end-to-end SIP message protection. This contribution proposes that SA3 consider a public key approach for IM domain security to provide a more robust and accessible trust model.

1. Introduction

Control signalling for the IP Multimedia (IM) Domain is to be accomplished by SIP. SIP is described in IETF RFC 2543, and is intended to provide end-to-end control of IM sessions. In order to provide security for SIP messages, the IETF further recommends the use of security techniques that work in harmony with the end-to-end nature of SIP.

SA3 has recognized the need for security of SIP as it is extended to the wireless domain. The approach taken by SA3 has been to first consider the User Equipment (UE) to Access Network link. This has led to considerable deliberations regarding the IM Domain Security trust model. At SA3 meeting #16 last November, two main opinions were presented and discussed. Both of the opinions are based on a symmetric key approach. The main divergence is regarding

- which network entity should perform authentication and key agreement with the UE for SIP registration of a (roaming) user; and
- which network entity should terminate the access integrity/confidentiality protection of SIP messages with the UE.

(See contributions S3-000689 and S3-000699).

By the discussions, it is obvious that SA3 faces a tough decision to commit to any of the opinions, since each opinion has been supported by numerous rationales.

We believe that the current impasse is brought about by the inherent restriction of symmetric key methods for the SIP application. Symmetric key has been shown to be an effective way to secure the wireless access link and to "register" the UE with the access network upon roaming. If we carry the argument one step further, we note that in a wireless UE-to-UE scenario, symmetric key may continue to be effective, but in a "hop-by-hop" fashion. This is because the access links might still be secured by a symmetric key, while the inter-network link can only be secured by another method such as IPsec, given that a roaming agreement

enables a key agreement within the core network.

However, the effectiveness of symmetric key cannot be sustained when the wireless UE interacts with a randomly-chosen internet user, and this results in a discontinuity in the trust model.

In Section 2, we present the problems with a symmetric key approach in greater detail. In Section 3, we will explore the potential use of a Public Key Infrastructure to solve the IM domain security problem. In Section 4 we cite some facts about the ability of handsets and SIMs to perform public key calculations.

2. Problems with Symmetric Key Approach

2.1 Problems in User Authentication for SIP Registration

With the symmetric key approach, the user authentication has to be done in a given entity. For a roaming multimedia service subscriber, it is necessary either for the home network to deliver authentication data to an entity or to provide a real time response to the serving network for each authentication.

If the authentication data is delivered to an entity, then it is necessary to assume some level of trust to the entity, for example, assume the entity will use the authentication data properly. In contribution S3-000689, it is proposed that the authentication data should be delivered to P-CSCF. However, according to contribution S3-000699, P-CSCF in the serving network should not be trusted to authenticate the user.

S3-000699 proposes to authenticate users in the HSS. However, S3-000689 presented numerous concerns regarding the use of HSS to handle real time authentication. One of the concerns is that "if the AKA was handled in the HSS, the HSS would have to send out requests and wait for responses, for a potentially large number of users simultaneously. This could reduce HSS performance."

These difficulties to determine where to authenticate the user emphasize the fact that by a symmetric key approach, some entity that exists within a confined domain must be trusted in order to authenticate the users.

2.2 Problems with SIP Message Confidentiality/Integrity Protection

If the confidentiality and integrity protection for SIP messages are provided by symmetric key method, then it has to be determined that between which two end points, a given security protection is applied.

Especially, with symmetric key method, end-to-end protection is impossible. In IETF RFC 2543 (see reference [1]), it is pointed that

> Since SIP requests are often sent to parties with which no prior communication relationship has existed, we do not specify authentication based on shared secrets.

Furthermore, UMTS IM domain should have interoperability with different service realms. For example, as discussed in Section 1, a wireless device might wish to call an Internet phone or wired device. No matter which symmetric key method we use, it can only protect SIP messages from the UE to a network entity in the UMTS IM domain. See Figure 1 for an illustration.

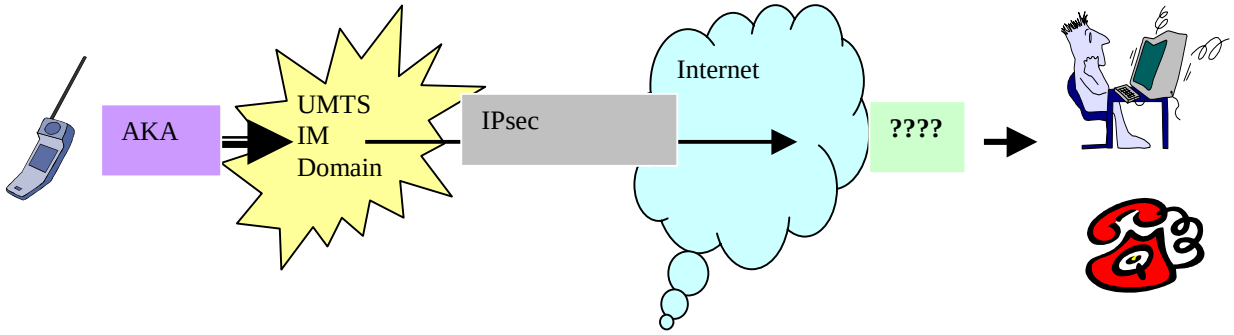

Figure 1. Interoperability with different service realms

An even worse situation would occur if a UMTS IM user were to be invited by an Internet SIP user to join a multimedia session. In this case the network element would have no means to check the validity of the INVITE message. Nor would the UE be able to validate the "other end."

3. PKI Is an Ideal Trust Model for IM Domain Security

IM Domain security demands a minimal overhead to provide robust security protection. It cannot be described simply by a "three party protocol" since the entities involved are more than three parties. This is essentially different from either the CS or the PS domain situation. As we have seen in Section 2, symmetric key method has intrinsic limitations to serve IM domain security.

Only with a public key method, can we minimize the overhead and make a robust trust model for IM domain security.

3.1 User Authentication with PKI

As we discussed in section 2.1, the entity entitled to authenticate the user has to be trusted if the symmetric key method is used. With a certificate-based public key method, the entity does not need the same level of trust as it does by symmetric key method.

A home network can fully control the authentication since it can issue and revoke user certificates. However, the home network does not need to be involved in real time for each user authentication. The user also can be authenticated at multiple entities depending on the transaction. Different entities can obtain access to the user's public key and its certificate.

3.2 Enable End-to-End Protection for SIP Message

With a public key method, the SIP messages can be protected end-to-end. This is consistent with IETF SIP security protection. See IETF RFC 2543

> All implementations SHOULD support PGP-based encryption and MAY implement other schemes.

With public key digital signature and PKI, each entity can verify the validation of a given SIP message without assuming specific overhead. Furthermore, if a message is forwarded via a proxy server, a digital signature extension can be added to the message to authenticate the proxy server. See Figure 2 for an illustration.

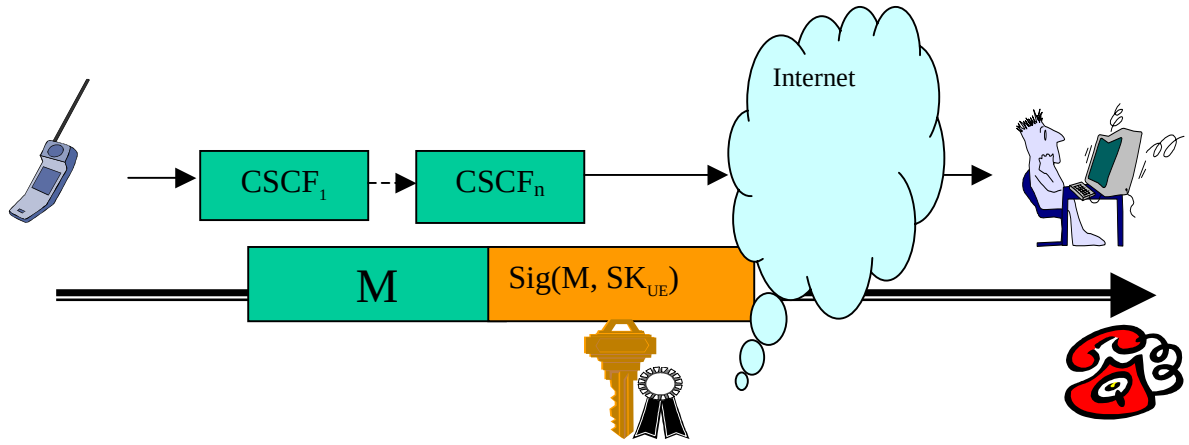

Figure 2. End-to-End Authentication

For SIP messages, end-to-end protection, provided by PKI, should be independent of IP layer protection by IPsec, which may be applied based on roaming agreement and/or network domain security requirements.

4. Public Key Calculations in User Devices

At past meetings of SA3, concern has been expressed over the ability of SIM card and handset platforms to execute public key calculations in a timely manner. However, as many of us may have been aware that public key cryptography has been intensively used to accomplish authentication and key establishment in WAP forum. Please see the technical specifications at

http://www.wapforum.org/what/technical.htm

5. Conclusion

Symmetric key method has intrinsic limitations in handling IM domain security. We should consider a public key method for IM domain security.

Reference

[1] IETF RFC 2543 “SIP: Session Initiation Protocol”, March 1999.