Internet Engineering Task Force
Internet Draft

D. Kroeselberg
Siemens

Expires: Juli, 2001

January 2001

SIP security requirements from 3G wireless networks
<draft-kroeselberg-sip-3g-security-req-00.txt>

Status of this Memo

Abstract

At present based on a different protocol architecture, 3G wireless standards start to become more and more IP-based. The upcoming set of 3G wireless specifications defined by 3GPP will include SIP [RFC2543] as the session control protocol for IP-based voice and multimedia. An important requirement for introducing SIP is the definition of a security architecture protecting the session control signaling.

This Internet Draft collects requirements for a SIP security architecture that are related to the use of SIP in 3GPP wireless

networks. It is intended to stimulate the discussion about SIP security and is meant as a source of input for a requirements draft on SIP security.

Table of Contents

1. Definitions

Some of the following definitions related to mobile cellular networks are taken from [3G TR 21.905] and [3G TR 23.821].

3GPP: Third Generation Partnership Project

UMTS: Universal Mobile Telecommunications System

PLMN: Public land mobile network. A telecommunications network providing 3GPP mobile cellular services, in the context of this document.

Domain: Highest-level group of functional PLMN entities.

Network domain: The fixed part of a PLMN which is independent of the connection technology of the terminal (eg radio, wired).

Access domain: The part of a PLMN that is responsible for carrying communication between the UE and the network domain,

which especially includes the air interface.

CS domain: Comprises all network domain entities for provision of circuit-switched telecommunication services.

PS domain: Comprises all network domain entities for provision of packet switched, IP connectivity services.

IMS: IM subsystem. Comprises all network domain entities providing support for IP multimedia services on the signaling and control level, carried on top of the PS domain. This especially includes the network domain SIP entities.

UICC: UMTS IC Card. An IC card (or 'smartcard') of defined electromechanical specification which contains at least one USIM.

Mobile user: A user who is subscribed to a mobile network, and is represented by a USIM.

USIM: Universal Subscriber Identity Module. An application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security.

UE: User Equipment. A device allowing a user access to network services. For the purpose of 3GPP specifications the interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains. Currently one defined domain is the USIM which is part of the UE.

SIP NE: A network entity that belongs to the network domain of a PLMN, is part of the IM subsystem, and offers the functionality of a SIP server, location server or proxy.

Visited network: The PLMN that a UE is currently roaming to.

Home network: The PLMN that a UE is subscribed to. In the special case that a UE roams within the home network, the visited equals the home network.

RNC: Radio Network Controller, in charge of controlling the use and the integrity of the PLMN radio resources.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. Introduction

There are currently two bodies producing two different sets of specifications for third generation (3G) mobile systems. These bodies are known as 3GPP and 3GPP2. This draft concentrates on requirements resulting from 3GPP. The views expressed in this document are those of the author, not 3GPP as a whole.

The system specified by 3GPP is also known as UMTS. For UMTS whose core network evolves out of the second generation mobile system GSM, 3GPP has produced a first release of 3G specifications referred to as "Release 99".

The architecture of this 3G wireless network is based on a domain concept, grouping functional network entities. The Release 99 network domain splits into a CS domain that is responsible for all "classical" circuit-switched services and a PS domain that introduces IP connectivity to the network.

On top of the PS domain, a future Release (so-called Release 5, specifications are due to be completed by the end of 2001) of 3GPP specifications introduces an IM subsystem (IMS) that shall provide IP-based services with session control using the SIP protocol.

From a SIP point of view, the UE provides the functionality of a SIP user agent, and the IM subsystem roughly consists of SIP proxies, registrars and location servers that support global roaming.

Since there are several threats to SIP messages sent between the different mobile network entities, a framework offering complete security for these messages is required for Release 5. This draft gives a short overview of the current 3GPP security architecture. It

discusses several security issues raised by the introduction of SIP with the 3GPP Release 5 specifications and collects related security requirements.

3. Security architecture of 3GPP Release 99 specifications

The 3GPP security architecture protecting the first generation of 3G mobile networks offers mutual entity authentication and session key establishment between a roaming UE and the network side.

Across the most exposed part of mobile networks, the air interface, all data sent between a UE and the visited network is optionally encrypted at the link layer.
In addition to encryption, signaling data is mandatorily integrity protected across the air interface (more precisely, confidentiality and integrity protection extend further back to the RNC, covering parts of the fixed network as well). This is the signaling used to control the bearers in the circuit and the packet switching domains of UMTS and is different from session control signaling by an application layer protocol such as SIP.

The protocol used for authentication and key establishment is called the UMTS AKA (authentication and key agreement) protocol. It is based on long-term secret keys shared between the USIM and the authentication center in the home network.

Within a run of this protocol short-term session keys are derived. Subsequently all signaling messages sent between the UE and the visited network are protected by applying integrity protection and encryption transforms based on these session keys.In so far, this could be compared roughly to the approach taken in the IPSec framework [RFC2401]. A major difference between UMTS AKA and e.g. IKE [RFC2409] is that UMTS AKA has been designed especially for

roaming scenarios. According to 3GPP, IKE does not match the requirements for these scenarios.

Authentication involves three parties: the roaming UE, the visited network and the home network. The authenticating entities are the USIM and an Authentication Center in the user's home network as they share the long-term secret key. However, the home network delegates control of authentication to the visited network, mainly for performance reasons. Here, mutual trust is required between the

visited and the home network, handled within a so-called "roaming agreement".

The UE and the Authentication Center also establish the session keys between them. The Authentication Center subsequently transfers the session keys to the visited network which terminates confidentiality and integrity to the UE. By using the session keys, the visited network proves to the UE that it is authorized by the home network to serve the UE.

Delegation of authentication control and transfer of session keys to the visited network is realized by the transfer of authentication vectors from the authentication center to the visited network. These authentication vectors contain challenge-response pairs and session keys. Usually several authentication vectors for a specific USIM are transferred to the visited network within a single request to the home network, which significantly reduces the network load between visited and home network for subsequent authentications and minimizes the delay the mobile user experiences.

The UMTS AKA protocol is specified in [3G TS 33.102].

4. Scope of SIP security in 3GPP

This section shows why security mechanisms for SIP are important in 3G networks and what they shall be used for.

SIP security is meant for IM subsystem session control (i.e., SIP messages) only. The protection of media streams, whether this is end-to-end or hop-by-hop, is not in the scope of the current 3GPP discussion on SIP security.
Therefore, this draft compiles requirements for the protection of SIP messages only and does not deal with media stream security, e.g. the exchange of keys for media stream encryption within SIP.

Human user authentication is not in the scope of this document as well. A mobile user is represented by a USIM within a PLMN and a secure method to authenticate a human user against the secure token containing the USIM is assumed as given.

Within this context, each PLMN and each IM subsystem represents a single domain of trust. Different PLMN operators can set up a

roaming agreement to establish an inter-domain trust relationship between their networks.

The bearer level signaling of a PLMN is separated from the media (e.g. voice) data, and the already in place integrity protection over the air interface is only provided for the bearer level signaling channels, not for media data.
In contrast to bearer level signaling, SIP messages as new application level signaling introduced for the IM subsystem are handled by the air interface as media data, and are not integrity protected. Therefore the goal is to define a new mechanism for protecting SIP messages between the UE and the SIP NE terminating security at the network side.

There are different parts of mobile networks where different means of protection are required. Two important parts of the IM subsystem must be considered for securing SIP. These are the interface between the UE and the SIP NE that terminates security at the network side (access domain part), including the air interface, on the one hand and IP-based traffic between SIP NEs in the IM subsystem, within the same or between different networks on the other (network domain part).

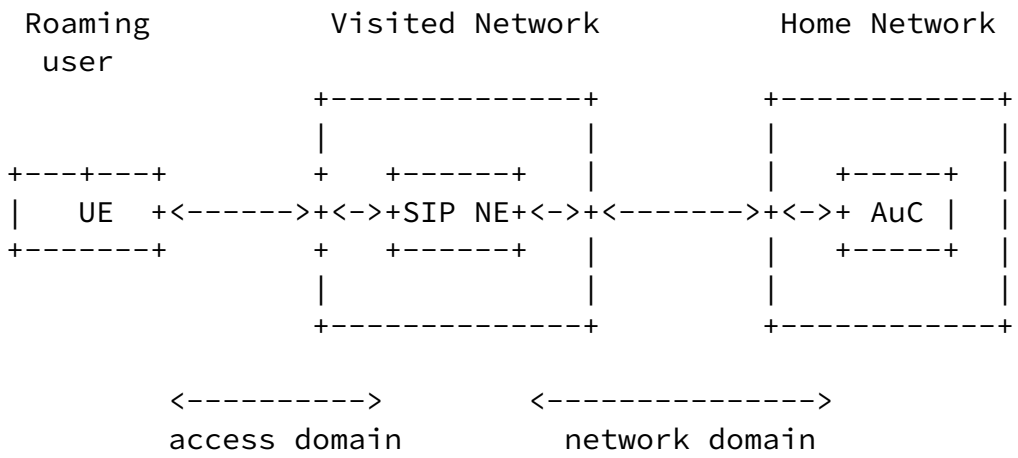

Figure 1: IM subsystem parts to be secured

For securing both access and network domain parts of the IM subsystem, it is important that each single SIP message is integrity protected and, optionally, confidentiality protected.
This shall be achieved for the access domain part by running the UMTS AKA protocol during SIP registration and protecting all subsequent SIP messages sent between UE and visited network by applying integrity protection and encryption mechanisms, based on session keys which are derived during AKA and are individual per user. Theses session keys are different from the session keys used for bearer level security as described in section 3.

The security mechanism for SIP integrity and confidentiality protection for the access domain part is still open. When discussing the layer at which integrity and confidentiality protection shall be

applied it should be taken into account that the SIP NE which terminates access security at the network side is not necessarily the first SIP hop from the UE perspective. Hence, there may be a requirement for end-to-end security mechanisms at the SIP layer that are able to pass intermediate SIP hops. Security mechanisms at lower network layers, e.g. IPsec, do not provide end-to-end security in this case.

For the provision of SIP security the USIM will have a pre-shared secret key in common with the home network, where it is subscribed to for IM subsystem services. For the network domain part, IP packets carrying SIP messages between SIP NEs are envisaged to be secured by using IPSec.

5. Requirements for securing SIP

As a general requirement, any security architecture MUST allow different mechanisms for access domain security (i.e., UE - SIP NE) on the one hand and network domain security (i.e., SIP NE - SIP NE) on the other. This stems from different system requirements and different roles of SIP entities being part of one or the other network part.

5.1 Access domain security requirements

- Mutual authentication and key agreement between a mobile user (represented by the USIM) and the network side MUST be supported. The long-term shared secret used for authentication and key agreement MUST only be known to the USIM and the home network.

- Integrity protection between the mobile user and the SIP NE terminating integrity on the network side MUST be supported.

- Confidentiality between the mobile user and the SIP NE terminating confidentiality on the network side MUST be supported.

- A secure mechanism for delegating integrity or confidentiality to

a specific SIP NE MUST be supported. In addition, a secure mechanism for delegating control of entity authentication and key agreement MAY be supported.
This stems from the fact that control of integrity, confidentiality and authentication need not necessarily be carried out in the home network, or by the same entity. A secure transport for the agreed session keys to the SIP NE that terminates SIP integrity and confidentiality with the user MUST be provided.

- Any SIP security mechanism SHOULD be independent of the underlying access technology that provides IP connectivity and mobility.

- User identity confidentiality SHOULD be supported. It should be

possible to hide a mobile user's identity or other data from which this identity can be derived or which allows to trace the user or derive his location, while transmitted in the access domain (the problem here is that the user identity needs to be sent before a session key for confidentiality protection can be established).

5.2 Network domain security requirements

- Between SIP NEs of different IM subsystems mutual authentication and key agreement MUST be supported. Authentication based on pre-shared secret keys (instead of mandating a public-key based method) MUST be supported within this mechanism.
Integrity protection and confidentiality between SIP NEs of different IM subsystems MUST be supported.

- Hop-by-hop integrity and confidentiality SHOULD be supported between SIP NEs within the same IM subsystem.

- User identity confidentiality in the network domain SHOULD be supported (this will be provided by confidentiality when the complete SIP messages are protected e.g. by IPsec.)

5.3 System requirements on security

- Any cryptographic mechanism that has to be executed by the mobile device, especially authentication and key agreement which happens in the USIM, MUST not mandate the use of public key cryptography, i.e., MUST allow for symmetric key cryptography only.

- The limits of processing power, storage capacity of a USIM and the bandwidth on the USIM-UE interface have to be taken into account in the selection of mechanisms.

- The air interface has limited bandwidth and is error prone. Security mechanisms for the air interface MUST be able to deal with delays caused by high failure rates or low bandwidth.

- Any security solution SHOULD be scalable to accommodate a very large user base (up to one billion).

- Any security solution SHOULD be scalable to support a large number of different PLMNs (different domains of trust).

- Any security solution MUST support global roaming, i.e., a mobile user MUST be able to get access to a visited network without previous contact between the mobile user and the visited network (which is currently handled by the UMTS AKA protocol described in section 3 for non-IMS access).

- Any protocol for authentication and key agreement should be efficient. It should minimize the number of roundtrips for

authenticating a mobile user through a visited network, to reduce network load.

- A secure storage of long-term keys used for IM subsystem security MUST be provided, on the mobile user side and on the home network side.

- A secure storage and execution of security algorithms MUST be provided. Algorithms which require access to the long-term keys shall run in the same entities in which these keys are stored.

6. Security Considerations

The focus of this document is security, and security considerations permeate the document.

7. References

[3G TR 21.905] 3GPP TSG SA, TR 21.905: "Vocabulary for 3GPP Specifications (Release 1999)";V3.2.0, 10/2000.

[3G TR 23.821] 3GPP TSG SA2, TR 23.281: "Architecture principles for Release 2000"

[3G TS 33.102] 3GPP TSG SA WG 3 Security, TS 33.102: Security Architecture (Release 1999); v3.5.0, 07/2000.

[3G TR 33.8xx] 3GPP TSG SA WG3 Security, TR 33.8xx: Access security for IP-based services (Release 2000); v0.3.0, 11/2000.

[RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

[RFC2401] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2409] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2543] Handley, M., H. Schulzrinne, E. Schooler, and J. Rosenberg. "SIP: Session Initiation Protocol", RFC 2543, March 1999.

Author's Address

Dirk Kroeselberg
Siemens CT IC 3
Otto-Hahn-Ring 6
81739 Munich, Germany

Email: dirk.kroeselberg@mchp.siemens.de