3GPP TSG SA WG3 Security — S3#14 **S3-000447**

2-4 August, 2000

Oslo, Norway

Source: Siemens AG

Title: Overview of security mechanisms for access security for IP-based services

Document for: Discussion

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

This contribution contains a first overview over candidate security mechanisms. This overview is only for information.

There are two different approaches for the provision of security in the IM domain: it can be based on security mechanisms specifically defined for 3GPP or on security mechanisms mentioned in SIP [RFC 2543].

A general decision to be made is, if security mechanisms for the IM domain should be based on public key cryptography or on symmetric key cryptography. This requires a careful analysis which has to consider the restrictions imposed by a UMTS environment as well as the implications of having to provide a global public key infrastructure. Some of the mechanisms defined by the IETF use public key cryptography. Those defined so far by 3GPP for UMTS do not.

Security mechanisms specifically defined for 3GPP:

One possibility could be to re-use the 3GPP AKA (authentication and key agreement) of the bearer level (as specified in [TS 33.102]) for authentication and key agreement in the IM domain. For integrity and confidentiality protection 3GPP specific mechanisms may be re-used as well.

Security mechanisms specified by the IETF for SIP:

For the protection of SIP several alternatives are mentioned in [RFC 2543]. The mechanisms are taken from other RFCs. [RFC 2543] only describes in which way these mechanisms are applied to SIP. Below the alternatives mentioned in the SIP standard are listed together with some of their characteristics. A first analysis is given whether the mechanisms meet the requirements assembled in our related contribution [RASIP]:

- HTTP security mechanism "Basic Authentication" [RFC 2617]

  - Provides authentication of a client to a server based on passwords, where the password is transmitted in the clear.

  Authentication by a simple password transmitted without protection, does not fulfill any of the security requirements given in [RASIP].

- HTTP security mechanism "Digest Authentication" [RFC 2617]

  - Provides authentication of a client to a server based on passwords. The password is not transmitted in the clear, instead a digest (hash value) of the password and other parameters including a challenge parameter (issued by the server) to protect from replay attacks, is sent.

  - Authentication of a server to a client is also possible. [RFC 2617, 3.2.2]

  - As mentioned in [RFC2543, 13.2] Digest Authentication does not offer message integrity.

  Digest Authentication was designed as a replacement for Basic Authentication. RFC 2617 itself discusses several weaknesses of this mechanism (sections 3.1.4; 4, but see also [SIP2000]).It is therefore questionable whether it meets the system requirements in [RASIP].

  .

- Pretty good privacy (PGP) [RFC 2440] provides

  - Mutual authentication between client and server based on public key cryptography

  - Message integrity based on digital signatures

  - Message confidentiality, where data encryption is based on symmetric key cryptography and session key transport is protected by public key encryption.

  The provided mechanisms offer a sufficient level of security and fulfill the security requirements given in [RASIP], except the three-party AKA protocol. But PGP makes extensive use of public key mechanisms for authentication and key agreement. In particular, the use of digital signatures for message integrity seems inefficient. Transport layer security (TLS) [RFC 2246]

  - Mandates public key cryptography for authentication and key management

  - The record layer provides message integrity as well as confidentiality based on symmetric key cryptography, but TLS is monolithic, i.e. key management is not separable from the record layer.

  - TLS is only defined for TCP, not for UDP, and some servers used in SIP must support UDP

Although a strong security protocol, TLS is not suitable for providing access security for IP-based services, since it only supports TCP at the transport layer which is not sufficient. TLS also relies on public key mechanisms. TLS does not allow to separate key management from the record layer which provides integrity and confidentiality for the transmitted data. IPSec [RFC 2402], [RFC 2406] provides

- Mutual authentication between the communicating entities based on symmetric key cryptography
- Message integrity based on symmetric key cryptography
- Confidentiality protection of messages based on symmetric key cryptography
- A protection mechanism against replay attacks, when used with automated keying (e.g. IKE)
- Optional key management (IKE [RFC2409]) based on public key schemes

IPsec meets the security requirements of [RASIP], except for the three-party AKA protocol. The IPsec base protocols AH and ESP do not use public key mechanisms and seem to meet all system requirements.

Note that, according to a decision in 3GPP, IPv6 addresses shall be used in the IM domain. Note that if IPv6 was implemented with full functionality then all nodes involved in the IM domain would have to support IPSec AH and ESP.

IETF has not defined AKA for roaming SIP users: For authentication and key management IKE [RFC 2409] is an alternative to be considered. But note that neither IKE nor any of the alternatives listed above defined by the IETF for SIP specifies a three party authentication and key management for roaming users which is needed in UMTS. An appropriate mechanism would additionally have to be specified.

References

[RASIP] 3GPP TSG SA WG3 Security: “Requirements on access security for IP-based services“, Siemens contibution for S3 #14

[RFC 2402] IETF RFC 2402: *IP authentication header;* Nov. 1998.

[RFC 2406] IETF RFC 2406: *IP encapsulating security payload;* Nov. 1998.

[RFC 2409] IETF RFC 2409: The internet key exchange (IKE); Nov. 1998.

[RFC 2440] IETF RFC 2440: *Open PGP message format;* Nov. 1998.

[RFC 2617] IETF RFC 2617: *HTTP authentication: Basic and digest access authentication;* June 1999.

[RFC 2543] IETF RFC 2543: *SIP: Session Initiation Protocol*; March 1999.

[SIP2000] J. Rosenberg: *SIP security*, presentation at SIP2000 conference

[TS 33.102] 3G TS 33.102: *Security Architecture;* version 3.5.0, July 2000.