3GPP TSG SA WG3 Security **S3z020019**

January 31 – February 1, 2002

Antwerp, Belgium

Agenda Item: 6.2

Source: Ericsson

Title: The need for confidentiality protection for the first/last hop

Document for: Discussion and decision

1. Scope and objectives

The scope of the document is to discuss the need for confidentiality protection for the first/last hop in R'5 timeframe. It is proposed in this contribution that for R'5 only integrity protection of SIP signalling shall be offered. And as a recommendation in order to protect the user information a 3G operator should apply encryption at link level for the PS-domain user plane for encrypting both the IMS user plane as well as control plane.

This still makes IMS independent from the PS-domain since the IMS control plane is integrity protected at SIP level and securing billing and charging functionality.

2 Background

According to [TS21.133]:

Unauthorised access to sensitive data (violation of confidentiality)

- **Eavesdropping:** An intruder intercepts messages without detection.
- **Masquerading:** An intruder hoaxes an authorised user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a legitimate system into believing that they are an authorised user to obtain system service or confidential information.
- **Traffic analysis:** An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place.
- **Browsing:** An intruder searches data storage for sensitive information.
- **Leakage:** An intruder obtains sensitive information by exploiting processes with legitimate access to the data.
- **Inference:** An intruder observes a reaction from a system by sending a query or signal to the system. For example, an intruder may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

The stage 2 requirements for the CS-domain and the PS-domain are defined in [TS33.102] and they are:

- User plane traffic will be ciphered using the cipher key agreed for the corresponding service domain
- Control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains

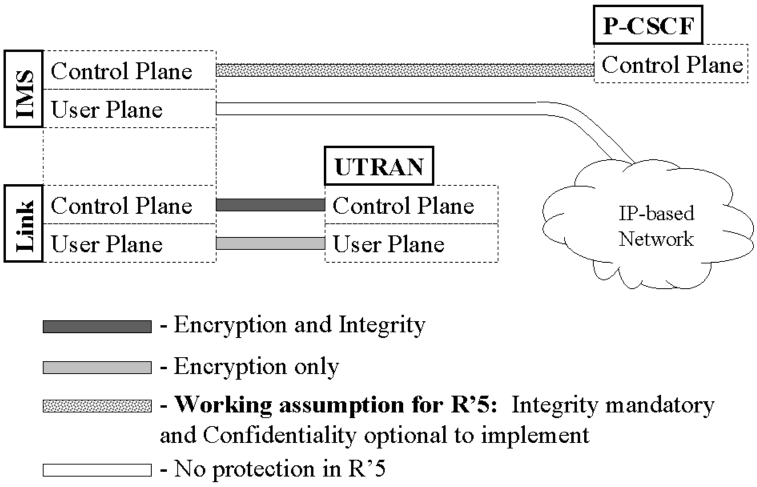
The domain of interest, which is protected by link layer, is the PS-Domain, which is the transport protocol for IMS control plane, as well as user plane. Of course both the IMS control plane as well as the user plane is transported by the user plane in the PS-domain and can potentially only be offered encryption but not integrity protection at link level.

Some of the relevant Stage 2 security requirements for the new domain called IMS as specified in [TS33.203] are:

- User plane is offered no protection and no TS has been defined in 3GPP to offer this kind of protection
- Control plane data will be integrity protected and optionally confidentiality protected

An overview of the current protection offered is given below where it can be seen that both the user plane and the control plane could in theory experience protection at Link level.

Overview of protection of control plane and user plane (R'99 and IMS)



3 Some technical analysis

It has already been agreed in SA3 not to offer end-to-end security including IMS type of services, cf. [S3-010406]. This means that there will be no standardised feature how to protect RTP and no corresponding key management scheme i.e. the user plane is unprotected in Release 5 framework. Furthermore it has also been concluded that IP address anonymity is not provided in the R'5 time frame. However this type of end-to-end services could be available in R'6 and beyond.

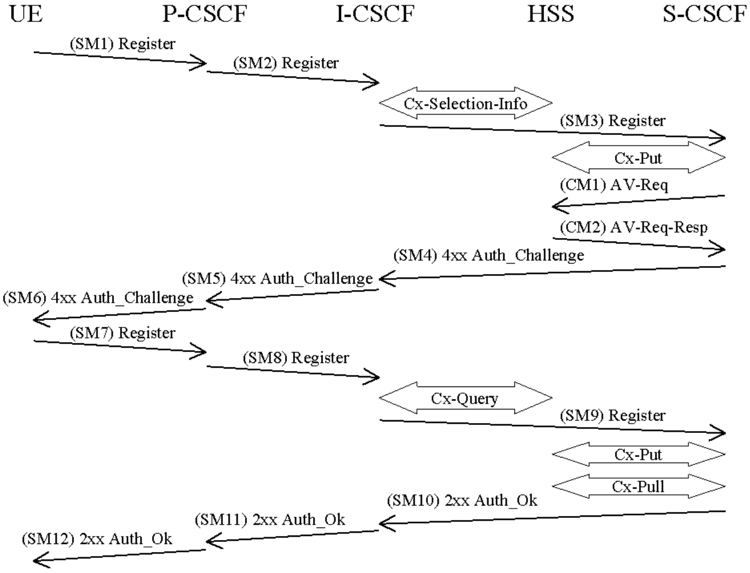
It is envisioned that end-to-end type of services would add value for a user, which could be offered by a 3G mobile operator as a service. Clearly if the user plane is not protected there is no clear security argument why to encrypt the control plane only. It could even give the wrong impression of the offered security level for the user. It therefore seems advantageous that the operator for R'5 turns on the confidentiality protection at Link level since then all potential threats mentioned above in Section 2 could be removed. This protection is then offered both to the IMS user plane as well as the control plane. The level of the offered confidentiality is then the same for the IMS control plane and the user plane.

Still IMS can be viewed as being independent since all events related to charging are appropriately secured e.g. by integrity protection and replay protection. It does not rely on the potential encryption of the user plane at the link layer. Hence a 3G operator and a 3G subscriber can be certain that the charging and billing is secured and this is an important feature of the IMS system.

There has been some extensive work within the IETF community to extend HTTP digest such that the solution is compliant with the 3GPP requirements. It looks promising that IETF will be able to deliver such a solution according to the IMS time plan. This working model should also apply for the work needed finding an appropriate model on how to encrypt SIP at SIP level in IMS.

According to [TS33.203] at Registration of an IM-subscriber the Security association shall be activated in SM7 in the figure below. The UE has in SM6 received a challenge and the RES is sent to the node, which will check the RES, i.e.

the S-CSCF. It is a requirement in [TS33.203] that the RES sent by the UE shall be checked by the S-CSCF both in the successful case as well as the unsuccessful case.



This means that SM7 should not be encrypted since it is required that the RES shall be sent to the S-CSCF. In theory the P-CSCF could identify if the RES is correct or not but it has been agreed that in order to reduce the S-CSCF trust in the P-CSCF the RES shall be sent to the S-CSCF. It seems that one potential solution is to start encryption in SM12 but it is not clear what implications that will have on the current requirements in [TS33.203]. This seems to some extent have an impact on at least when to start encrypting SIP for IMS with the current IPSec proposal. It is foreseen that some further analysis and clarifications in relation to this is needed e.g. on the use of the security associations. Hence the current requirements in [TS33.203] should be modified accordingly.

4 Conclusions

It is envisioned that for R’6 and beyond there will be a work item defined for protecting the user plane for IMS related services. However since no protection is offered to the user plane in R’5 it is concluded that the extra protection for encrypting the signalling plane is low since an attacker easily can approach the user plane rather than the control plane. Hence the extra effort to encrypt the signalling plane does not really pay off.

It is proposed that the signalling plane is offered encryption in parallel to the work for protecting the user plane. Since IETF is currently developing HTTP Digest to work with 3GPP requirements for integrity protection it is believed that this working procedure will also work fine for protecting SIP with encryption as well. If needed based on e.g. specific 3GPP specific requirements it is assumed that it will be possible to extend SIP with encryption by using S/MIME. It should be noted that the current SIP bis includes S/MIME tunnelling.

Since IPSec has been viewed as a ready technology making it easy to offer encryption as well as integrity protection it has been kept in an Annex in [TS33.203]. However according to the analysis above further work is needed for defining the exact requirements on how IPSec shall be utilised for encrypting SIP.If the threats as defined in [TS21.133] regarding encryption are utilised by an intruder it is proposed that the operator offers encryption for both signalling plane and user plane in a similar fashions as for the CS-domain and the PS-domain i.e. link layer encryption. Furthermore IP-address anonymity is not offered but this protection could be included in R’6 and beyond. Hence there are a number of attacks available and encrypting the signalling plane only will not close the gap sufficiently

It is proposed that SA3 agree on the roadmap above and as a working assumption accepts that SIP signalling is only integrity protected for R’5. However the security mode set-up mechanism shall take encryption into account but for R’5 only the NULL encryption algorithm is allowed.

References

[TS33.203] 3G TS 33.203: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA3; Access Security for IP-based services".

[TS33.102] 3G TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA3; 3G Security; Security Architecture ".

[TS21.133] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA3; 3G Security; Security Threats and Requirements (3G TS 21.133 version 3.1.0)"

[S3z010102] 3GPP TSG SA WG3 Security, S3z010102: " On integrity protecting SIP-signalling in IMS ". Source: Nortel,Nokia and Ericsson, September 2001

[S3-010406] 3GPP TSG SA WG3 Security, S3-010406 “Draft Report of SA WG3 Meeting #19, version 1.0.0” Source: SA3 Secretary, October 2001