3GPP TSG SA WG3 Security **S3-030372**

July, 2003

San Fransisco, USA

Agenda Item: Presence/IMS

Source: Ericsson

Title: Profiling of RFC3325

Document for: Discussion/Decision

1. Introduction

On the SA3 email reflector there have been some discussions on the increased openness of Rel 6 version of the IMS. This paper aims to discuss on the Trust Domain and the SPEC(T) concepts as defined by IETF or the use of p-asserted-identity and as incorporated in the TS24.229 in CN1. A CR to TS33.203 is attached to reflect how SPEC(T) is implemented in 3GPP. It is proposed that this is captured in an Informative Annex.

It should be noted that this input paper defines the trust domain T to be equal to 3GPP-IMS i.e.

T := 3GPP-IMS

2 Discussion

In RFC 3325 [1] a private extension mechanism that makes it possible for nodes in the network to assert identities of users is defined. Clearly the user needs to be authenticated by a node in the system before an identity could be asserted. If a node has authenticated a user it can then assert the identity. All nodes belonging to the same system and are all included in the same Trust Domain can therefore trust that the identity belongs to the claimed one. As soon as an asserted identity is received from or sent to the complement to the trust domain the identity can no longer be asserted.

An example of such a system is a closed network as exemplified in the RFC 3325, which emulates a circuit switched telephone network.

SA3 has earlier discussed the problems with a UE that bypasses a P-CSCF after successful registration. It was then concluded that cf. TS33.203 Annex J "….if neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the NDS/IP [5] mechanisms, then physical protection measures or IP traffic filtering should be applied. This is anyhow not in the scope of 3GPP specification.".

Furthermore this seems to be inline with the SA2 requirement from TS23.228 that an operator should based on the operator policy decide whether a S-CSCF may forward the SIP request/response to the open Internet, cf. Clause 5.4.2 in TS23.228. However no exact mechanism how this requirement could be implemented has been defined by 3GPP. One conclusion could be then that SA2 has had the view similar as SA3 on the bypassing P-CSCF problem that the exact mechanism is out of the scope of 3GPP. Clearly an operator has the choice to exclude all SIP traffic towards the Internet, which is one way of achieving this technically, but this choice might not be attractive for all operators considering the business implication of such an implementation.

2.1 SPEC(T)

The RFC 3325 requires that a SPEC(T) is defined from the template given below:

1. The manner in which users are authenticated
2. The mechanisms used to secure the communication among nodes within the Trust Domain
3. The mechanisms used to secure the communication between UAs and nodes within the Trust Domain

4. The manner used to determine which hosts are parts of the Trust Domain T
5. The default privacy handling when no Privacy header field is present
6. That nodes in the Trust Domain are compliant to SIP
7. That nodes in the Trust Domain are compliant to RFC 3325
8. Privacy handling for identity as described in Section 7 in RFC 3325

The RFC is only applicable for a defined Trust Domain T trusted by end users and end systems. It is worthwhile to mention that the RFC does not specify any security measure for protection of the asserted identity in terms of confidentiality, integrity and replay protection or any other mechanism. It is not possible to verify who has asserted the identity meaning that it is the responsibility of the Trust Domain. As indicated in the RFC there are sufficiently many type of networks where this is useful where this can be used although the limitations associated with it such as a closed network. A 3GPP network and the IMS network in many aspects are viewed as closed networks but this requires that the owners of the networks implement what is required in 3GPP standards as well as security measures not visible in the standards like Firewalls and Physical protection.

2.2 How does it work?

There are many cases covered in RFC3325 but at high level it works like as briefly described in this clause.

A node inserting p-asserted-identity performs an authentication of the user utilizing e.g. Digest.

Assume $N_i \in T$ and $N_j \in T$ and $N_k \notin T$ i.e. $N_k \in T'$ (i.e. the complement to T):

1. If N_i receives an asserted-id from N_j since both belong to T it can be accepted and no authentication of the subscriber is necessaryIf N_i receives an message from N_k, which is not trusted then if N_i wants to add an asserted identity to the message the N_i has to authenticate the user e.g. using DigestIf N_i receives a message from N_k, which is not trusted, and an asserted id is present then N_i must remove the header. This could be the case when an I-CSCF receives a message from the Internet, which could claim that the identity belongs to an IMS subscriber. Clearly 3GPP has not specified any means to authenticate a user form the Internet so this identity cannot be trusted.If N_i is about to forward an asserted identity to the N_k, which is not trusted. If the UE has required Privacy i.e. priv-value=id then N_i shall remove the asserted identity

2.3 What has been implemented in IMS?

Here we describe what has been implemented already in the TS33.203 and the Presence TR and indicates where there are some open issue left for study.

We can assume the following definition of the Trust Domain T for IMS (i.e. by definition T := 3GPP-IMS):

a) Nodes belonging to the same administrative domain and consequently, belonging to the 3GPP-IMS Trust Domain T (e.g., nodes under the control of the same operator);

b) Nodes belonging to other administrative domains and belonging to the 3GPP-IMS Trust Domain T (e.g., nodes belonging to other 3GPP networks); and

c) Nodes belonging to other administrative domains and not belonging to the 3GPP-IMS Trust Domain T (e.g, nodes that do not belong to any 3GPP network).

It is clear that we have that P-CSCF$\in$T, I-CSCF$\in$T and S-CSCF$\in$T. It is also clear that all other nodes in the architecture as specified in TS23.228 are trusted. However a node outside the 3GPP domains such as SIP server cannot be trusted.

The following aims to discuss the SPEC(T) from a 3GPP and IMS perspective:

1. How users are authenticated

The Authentication of subscribers takes place in the S-CSCF using IMS AKA as specified in TS33.203. Based on this authentication a Security Association can be created between the UE and the P-CSCF based on IK and CK

derived form IMS AKA. The P-CSCF will be able to verify the claimed identity and also able to assert identities based on the integrity protection using IK and applying either HMAC-MD5 or HMAC-SHA1 of the SIP message.

2. The protection mechanisms among nodes within the Trust Domain

The security protection that has been defined for IMS in 3GPP relies upon underlying hop-by-hop security and the use of IPsec and TS33.210. It is mandatory to apply confidentiality protection and integrity protection between security gateways i.e. SEGs for SIP signalling between a VN and a HN. However it is optional for implementation to use the Zb interface inside the VN or the HN. According to TS33.203 it is also stated that if neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the mechanisms defined in TS33.210, then physical protection measures or IP traffic filtering should be applied, which is outside the scope of 3GPP specifications.

3. The mechanism to secure communication between the UAs and nodes within the Trust Domain

The UE and the P-CSCF is utilizing IPsec for integrity protection as specified in TS33.203 and optionally the confidentiality protection as defined in TS33.102 between the UE and the RNC.

Since the AS's that reside within the HN are trusted it is up to the owner of the HN to apply IPsec as defined in TS33.210. All other SIP servers/proxies residing outside a 3GPP network is not considered in the 3GPP standards in terms of what security mechanisms should be applied.

4. The manner to determine which hosts belong to the Trust Domain

SIP nodes that receive or send traffic to other SIP nodes may take different actions (e.g., removal of P-Asserted-Identity header field) before forwarding the SIP message to the next node as described above.

Prior to forwarding a SIP message, a SIP node belonging the 3GPP-IMS Trust Domain must determine whether the next hop is part of the 3GPP-IMS Trust Domain or not. Similarly, when a SIP node in the 3GPP-IMS Trust Domain receives a SIP message, it must determine whether the previous node belongs to the 3GPP-IMS Trust Domain T or not.

The trust model in 3GPP has implicitly assumed what nodes belong to T however nothing has been stated in the specifications on how to determine that a node belongs to the complement to T i.e. T'. This could be accomplished in several ways at high level and here is an example list. The list is not exhaustive and does not exclude that the solutions can be combined:

I. The use of certificates and TLS

II. The operator implements the Zb interface and IPsec

III. Dedicated I-CSCF's for the Internet access

IV. 'Trusted' and 'untrusted' interfaces in I-CSCF

V. Physical protection measures or IP traffic filtering is applied. This is anyhow not in the scope of 3GPP specification.

VI. The 3GPP network is from a standardization point of view assumed to be a closed network i.e. there is no need for 3GPP to extend the existing standards further to verify that a message came from or is being sent to a trusted or untrusted node i.e. NDS/IP applies

In the following text some more details are given on some of the technical solutions however it does not aim to be an exhaustive review and many other possibilities are assumed to exist.

When a SIP node is receiving or sending a SIP message from/to another SIP node, it needs to determine whether it is a trusted node or not in the general IETF sense.

The manner to determine if the previous or next host is part of a the Trust Domain T is considered separated from incoming than outgoing traffic.

Incoming traffic:

These are SIP messages received by a SIP node. The SIP node must determine whether the previous node was part of T or not.

This can be achieved in many ways e.g. through:

1) A node can do a reverse DNS query (Note: one could perhaps argue DNS security could apply here but that is FFS) to find out if the source IP address belongs to a node of the same administrative domain or not. If the node belongs to the same administrative domain it belongs to T. Otherwise, it is uncertain whether the node is trusted or not i.e. it may or may not belong to T since it may or may not belong to 3GPP IMS. Hence this is not a complete solution.

2) A SIP node can implement TLS an operator apply suitable PKI. If a message is received over TLS, the SIP node possesses a certificate of the remote node. The management of the PKI in this case is out of scope for 3GPP. This solution does not work when the message is received without TLS as the sender of the message does the decision whether to use TLS or not.

3) The solution is based on differentiating trusted and not trusted traffic. This could be done at the Security Gateway or at an I-CSCF. It would require two logical SIP nodes, one processes trusted traffic and the other processes untrusted traffic. The Security Gateway is provisioned with rules that routes traffic received over the Zb interface to the logical trusted node, and traffic received outside the Zb interface to the node, which is not trusted. Differentiation of the trusted/untrusted traffic may be done in several ways, such us forwarding to a specific IP address or port numbers.

Outgoing traffic:

Prior to forwarding a SIP message, a SIP node belonging to the 3GPP-IMS Trust Domain needs to determine whether the next node is a trusted or untrusted node. While 3GPP does not mandate a specific mechanism, operators must make sure that the SIP nodes support at least one of the mechanisms:

1) A node can do a reverse DNS query to find out if the destination IP address belongs to a node of the same administrative domain or not. If the node belongs to the same administrative domain it belongs to T. Hence this is not a complete solution.

2) A SIP node can implement TLS and set up a TLS session towards a remote node. The exact structure of the PKI system is out of the scope of 3GPP. This solution only works the SIP node forwards SIP requests, but not for the SIP responses since it can choose the transport protocol when forwarding a SIP request but not when forwarding a SIP response since that choice is made by the originator of the request. This is an issue since TLS only works with TCP and hence cannot provide with a full solution for UDP.

5. The default privacy handling when no Privacy header field is present

The elements in the Trust Domain must support the 'id' privacy service therefore absence of a Privacy header can be assumed to indicate that the user is not requesting any privacy. However the exact details of this is under consideration in the TR for Presence Security and there are some FFS's that need to be progressed to fully cover this part of the SPEC(T).

6. That nodes in the Trust Domain are compliant to SIP

It can be assumed by SA3 that all the IMS nodes in 3GPP are compliant with SIP RFC 3261 as specified in TS23.228 and TS24.229. The security parts are specified in TS33.203, which is SIP compliant.

7. That nodes in the Trust Domain are compliant to RFC 3325

All nodes in IMS are compliant with RFC3325 (however the work is still being progressed in SA3 for Release 6).

8. Privacy handling for identity as described in Section 7 in RFC 3325

The nodes in IMS act appropriately upon the Privacy "none" and "id" tags. This requires keeping the P-Asserted-Identity header or removing it according to the procedures described in RFC 3325 [23]. However the exact details of this is under consideration in the TR for Presence Security and there are some FFS's that need to be progressed to fully cover this part of the SPEC(T).

It can be seen that from the definition of the SPEC(T) above there are some open issues still in the TR for Presence in SA3 that need to be further progressed. Furthermore some of the issues in the SPEC(T) is not under the responsibility of SA3 only since it includes also SA2 i.e. there some architectural issues that need to be resolved.

3 Conclusions

Ericsson proposes that SA3 initiates an LS to SA2 asking SA2 on the need for creating standards in more detail in order to specify how a S-CSCF can decide if it is communicating with an node within IMS or with the external Internet and clarify what solutions they foresee in relation with Clause 5.4.1 in TS23.228 from a network implementation point of view. SA2 should consider the need to do standardisation as indicated in bullet VI in clause 2.

In order to progress the work on including material on this topic Ericsson asks SA3 to approve the attached CR to TS33.203. This CR contains material that covers these aspects however not in every detail as described in part 4 in this document. However depending on the outcome of the discussions in SA3 as well as answers from SA2 Ericsson will progress this in TS33.203 such that if necessary more details are defined. It should be noted that there ~~are two~~the attached CRs assumes that some other Ericssons CR to SA3#29 on Privacy is approved. ~~attached. One that assumes that another CR on anonymity is endorsed which makes references to new clauses in TS33.203 and another, which do not make these references.~~ In the case that the CR is postponed it is proposed to view this CR as a pseudo CR to the Presence TR and that SA3 endorses to put the relevant text into the TR.

4 References

[1] IETF RFC 3325 (2002): " Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".