3GPP TSG SA WG3 (Security) –S3 #36 **S3-040930**
23-26 November 2004
Shenzhen, China

Agenda Item: **6.1.1 – IMS**

Source: **Nortel Networks**

Title: **TLS Compatibility in IMS**

Document for: **Discussion and Decision**

1. Introduction

It was proposed in tdoc S3-040732 at the SA3#35, that the naming restrictions be placed on the IMS network elements (such as CSCFs) and the IMPIs in order to support possible, future use of TLS to meet some of the security requirements for IMS. In this paper, we raise the issue of whether the naming restriction is the right approach to mitigate some of the man-in-the-middle security threats in the deployment models wherein certificates are used for authentication between the UE and the P-CSCF for establishing the TLS connection. We also outline two possible alternative approaches to support TLS without requiring such restrictions on naming.

2. Validating SIP Registrations

When TLS is used, tdoc S3-040531 to SA3#34 identified three possible deployment models: 1) Shared Key UE authentication and Certificate based P-CSCF authentication 2) Certificate based mutual authentication 3) Shared key based mutual authentication.

When server certificates are used to authenticate a SIP Registrar, RFC 3261 discusses a possible implementation option (and in our understanding not a mandatory requirement), in which the User Agent checks that the domain identified by the server certificate corresponds to the domain to which the UA is trying to register. Only if the validation succeeds, then the UA proceeds with the registration procedure by issuing a REGISTER request with Request-URI corresponding to the domain name identified in the server certificate. Similarly, the Registrar challenges the request with 401 (Proxy Authentication Required) with "realm" parameter in the Proxy-Authenticate Header corresponding to the domain previously given/identified by the server certificate.

This solution works in the IETF SIP model, as there is no concept of roaming. On the other hand, 3GPP facilitates roaming support. Requiring the same mechanisms as discussed in the SIP RFC for IMS by restricting the naming schemes used by the IMS elements only validates that the entities (e.g., P-CSCF) is part of the IMS trust domain (e.g., ims.com). It does not consider/validate whether there is a roaming/interworking relationship between the home and the visited domain SIP Registrars. We feel that validating whether a relationship exists between the home and visited network is important before accepting registrations in IMS. Otherwise, certain security threats are not mitigated: For example, a rogue registrar who may be part of the IMS trust domain but does not have any roaming/interworking relationship with the home network may be able to forge registrations with User Agents.

Furthermore, this solution does not seem practical to support roaming of 3GPP subscribers in non-IMS networks, when this capability is desired by operators as it is not realistic to expect that non-IMS networks would follow 3GPP naming restrictions.

3. Alternate approaches

We can think of at least two approaches, which do not place any restrictions on the naming scheme used by IMS elements. Furthermore, these approaches can be used to ascertain the presence of a valid trust relationship between the P-CSCF and the home network. Both the approaches rely on the fact that the roaming relationship between operators is known beforehand and do not change very often.

In the first approach, the server certificates issued for IMS network elements are signed by the home network CA (or it's authorized CA). This implies that, for example, a P-CSCF must have access to a certificates signed by each 3GPP operator with which there is a presence of roaming relationship. When a TLS connection is set-up using REGISTER message, the P-CSCF obtains the domain name contained in the request, and uses it to select the appropriate certificate signed by the owner of the domain and uses it for the TLS connection server authentication. If the server authentication and the signature verification of the certificate succeed at the UA, then, the UA can be sure that there is a presence of roaming relationship with the P-CSCF. Similarly when client certificates are used by UE and/or the UE wants to act as a server, the client certificates are self-signed.

Another approach would be to send the initial REGISTER request directly to the home network, including the proposed P-CSCF name to the home network. The home network verifies that the proposed P-CSCF name is valid (for example, by checking a table for the presence of roaming relationship) and if there is a relationship, then the register response from the home network includes the validated P-CSCF (for example, by securing the domain name of P-CSCF using a credential known only to the home network and the user agent but is unknown to the P-CSCF). Note that only initial register requests need to be sent to the home network and any subsequent register messages can be sent via the P-CSCF.

4. Conclusion

We have shown that restricting the name of an IMS element only proves that it is part of the broader IMS trust domain. It does not provide any solution for validating for the presence or absence of roaming relationship between the two inter-operating domains. Furthermore, the naming restriction may be unduly burdensome to the operators as they loose their flexibility with respect to selecting domain name of their choice for the IMPIs and the IMS network elements.

Furthermore, we have outlined two alternative approaches that do not require any such naming restrictions to for supporting TLS in the future for IMS for the deployment models in question (i.e., when certificates are used for TLS connection server and/or client authentication).

5. Proposal

It is proposed that SA3 agrees that no change requests are needed to Rel-5 and Rel-6 versions of TS 33.203 at this stage in order to support TLS for IMS. A solution can be studied in detail when TLS is introduced for IMS security.