3GPP TSG SA WG3 Security **S3-030391**

15th – 18th July, 2003

San Francisco, CA, USA

Agenda Item: 7.18 (Presence)

Source: Nokia, Ericsson

Title: Comparison of different approaches in the Presence/Ut interface

Document for: Discussion/Decision

1. Introduction

At SA3#28, three solutions related to the HTTP security in Presence/Ut interface were discussed. SA3 provided feedback for each solution, and further analysis was requested.

This document compares the two approaches, namely the one by Nokia and Ericsson based on HTTP authentication proxy, and the other by Siemens based on IMS registration. It is suggested that SA3 decides which of the two approaches is preferred for further study.

2. Comparison

In general, the solutions promoted by Ericsson and Nokia [S3-030245, S3-030256] are similar in many ways. Both of the solutions are trying to introduce a general security infrastructure for HTTP access that is independent from IMS security. The goal is to create a simple, extendable and future-proof system, and avoid complexity from protocol and architectural point of view. The solutions are also similar in the sense that they require similar enhancements to the system, e.g. new Cx-like interfaces.

The solution proposed by Siemens in [S3-030223, S3-030224], on the other hand, uses a quite different approach. It tries to optimize the existing system components, and at the same time, it allows complexity and interdependencies between network nodes. The solution may seem as a simple way to progress; however, it includes inherent limitations as a trade-off.

2.1 Server authentication

Server authentication is mandatory in all proposals. Without server authentication, the MitM can spoof the IMS-derived secret from a client authentication over Ut interface, and then starts another TLS session with any targeted server.

SA3#28 commented on Nokia's and Ericsson's solutions that the network side is authenticated twice. Even though this may seem to be specific to AKA based solutions, this may also be an issue in the Siemens proposal because both TLS and HTTP Digest includes server side authentication. Of course, it can be argued that Siemens solution does not use HTTP Digest for mutual authentication, however, then the potential MitM problem is even more serious in Siemens proposal, if the compromised client implementation fails to authenticate the server at TLS layer. In contrast, AKA automatically includes server authentication that improves the strength in Nokia and Ericsson's solution.

2.2 Number of TLS connections

The solutions proposed by Nokia and Ericsson are based on the use of one TLS session between the UE and the HTTP authentication proxy. Siemens proposes key derivation for each separate application over IMS. Since each application may belong to different service providers, it is required that each application should not read user data from each other's database. So the design proposes that same UE would start separate TLS connections when accessing different application servers. See the figure below:

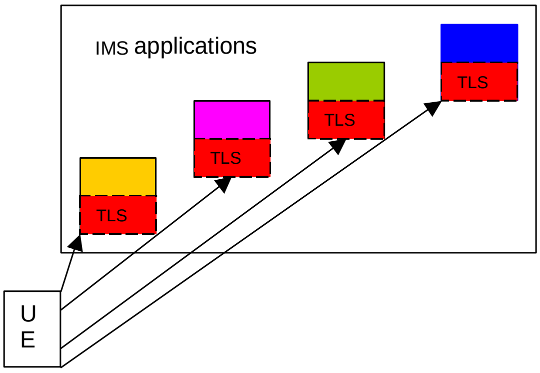

Figure 1: The scalability problem if HTTP authentication proxy is not used

Each new service/authentication must be extended to support exactly the same TLS model. This introduces several drawbacks:

- Usability: Establishing several TLS tunnels takes time due to the TLS handshake, the public-key cryptography calculation involved and the application layer authentication. Since IMS based services are likely to be integrated, it's very likely that user may update his personal data for all related services at the same time. For example, subsequent use of a conferencing system (e.g. a user arranging a conference) and the Presence Ut interface (e.g. adding a friend into the watcher's list) would require separate TLS establishment into these Application Servers.

- The terminal has difficulties to access to multiple application servers for comparing user data due to lack of resource in mobile to support multiple TLS simultaneously. This is needed when UE needs to access to several servers, and often it is the case due to the integrated SIP services, that multiple sessions may run at the same time. For example, a user who is chatting with his buddy could at the same time add the buddy to his list, and allow access of the buddy into a new fun group.

- All application servers need to have separate TLS connection with every UE.

- Investment on parallel TLS sessions is simply redundant.

These drawbacks do not exist in Nokia's and Ericsson's proposals. One Authentication Proxy with one TLS implementation is sufficient to handle all the connections towards all servers. If this optimization is removed, then the same functionality must be repeated and encapsulated into every server as the figure shown above. Therefore, it is recommended that SA3 adopts the working assumption that the number of TLS sessions should be minimized.

Note that the solutions proposed by Nokia and Ericsson are as minimized as they can theoretically be since only one TLS session is required. Note also that in both solutions the proxy can co-exist with an Application Server if required by implementation.

2.3 IMS service profiles and backwards compatibility

The IMS service profile contains a set of IMPUs of the subscription, application server's contact address, service trigger information and references to authorized applications. UE's registration will subscribe those IMPUs and the services included in that particular IMS service profile (with other implicit registration set, but not ALL profiles). A UE will have several service profiles, and each profile pointing to different set of services. This is how service profiles are defined in [23.228]:

> "The IMS Service profile is defined and maintained in the HSS and its scope is limited to IM CN Subsystem. The service profile is downloaded from the HSS to the S-CSCF. Only one service profile per Public user identity is downloaded to the S-CSCF at a given time (such as at registration, update of a profile etc.) based on the Public user identities being served by the S-CSCF. Nothing precludes that multiple service profiles can be defined in the HSS for a subscription. Each Public user identity is associated with one and only one Service Profile. Each service profile is associated with one or more Public user identities." [23.228]

Solution from Siemens does not work with IMS service profile. The initial filter criteria mentioned in Siemens proposal only gives S-CSCF the information about the applications stored in that service profile, but not all of applications. When UE registers with one IMPU, e.g. IMPU1 in yellow in Figure 2, the HSS forwards the corresponding service profile to a S-CSCF. This means that only IMPU1 and the applications associated with it are reachable by S-CSCF during that registration. S-CSCF cannot send derived keys to such application servers that are not associated with IMPU1. Application servers associated with IMPU2 cannot be served.

Furthermore, Application Server associated with IMPU2 could receive AKA keys from two ISIMs. If IMPU2 is registered using these two ISIMs to IMS in parallel, it is not clear which key to use with Application server.

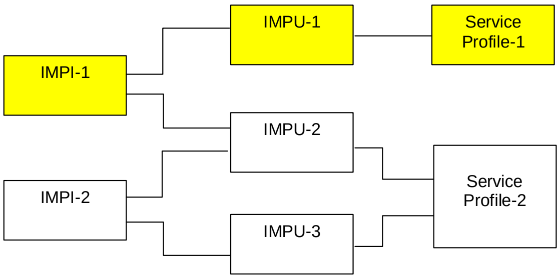

Figure 2: IMS service profile

In Siemens solution, the same complexity also applies to the UE side. Each IMS registration will cause update of Application Server specific passwords in the UE. There are also other issues that are problematic from UE point of view. For example, it is not clear how the UE locally assigns the passwords to the identities of different Application Servers, how the change of passwords is timed and synchronized, how the passwords are updated in secure way, and how to recover from situation where UE and Application Server possess different passwords.

There is also a more fundamental problem related to Siemens proposal as also pointed out by CN1 in [S3-030325]. IMS is currently seen as a “service enabler” for new IMS based services. The general principle should be that this new core network is kept as static as possible. Introducing new features for this infrastructure will automatically create potential backwards compatibility problems. For example, Siemens proposal would create separate Release 5 and Release 6 S-CSCF’s. This could mean that different UE’s need to be allocated to different S-CSCF’s depending on the service. It is not under the responsibility of SA3 to decide on solutions But it is understood that it will introduce additional change to service delivery in current S2 specification. Such decisions should be taken in SA2. SA3 is strongly recommended that service specific S-CSCF shall be avoided.

In Nokia and Ericsson’s proposals, all the connections between UE and the application servers are handled through Authentication Proxy. There is no need to change IMS specifications.

2.4 Key lifetime management

At a glance, it may look simpler approach to distribute the derived key to all the network elements than to re-use AKA. However, the key management is one of the most problematic issues in security design that should be taken into consideration from initial phase of designing. Usually, a design of key management based on stable, existing protocols is far better than the one relying on the spreading of keys in a fixed system architecture. In Siemens proposal, there are several open issues in the key lifetime management, e.g.:

a) What is the lifetime of a key, and who defines it? How does the UE know when the keys should be updated?

b) How to be sure that the UE and Application Server possess the same key?

c) How to recover if the keys are different? IMS registration prior of TLS handshake is not very efficient recovery mechanism, and introduces one further delay.

2.5 Future extensions

When new application servers are added over IMS, Siemens proposal turns out to have scalability problems. Key derivation and key lifetime management increase the load to S-CSCF especially due to variation of the services in each UE profile. In contrast, Nokia’s and Ericsson’s proposals are more steady to support growth of new services in long run.

It is suggested that the key management problem in the Siemens proposal has to be analysed in detail in order to avoid future surprises.

Future extension may also include services to non-IMS users. IETF protocol can be easily adopted to Nokia & Ericsson proposal to enable them.

3. CN1 group view

Regarding to feasibility of Siemens proposal, CN1 [S3-030325], states the drawbacks if relying on authentication to IMS registration:

- It causes backward compatibility problems;
- It puts additional processing load on the S-CSCF; the processing load is multiplied by the number of application servers involved.

Explicitly, CN1 points out that registration to IMS should be used exclusively for authentication of the UE to the IMS. In other words, Ut interface is independent from IMS registration and authentication. These changes to IMS seem to have significant impact to the stage 3 specifications.

4. Conclusions

This document compared two approaches to HTTP security with Presence/Ut interface. One approach is based on the use of HTTP authentication proxy and is promoted by Nokia and Ericsson. The other approach is based on IMS registration and has been promoted by Siemens.

Nokia and Ericsson see several problems in re-using IMS registration for HTTP security. The solution may seem simple, however, it includes inherent complexity and will cause many changes to existing IMS specifications as also pointed by CN1 work group.

It is suggested that SA3 adopts a working assumption that the solution in the Ut interface shall be based on the use of HTTP authentication proxy.

5. References

[23.228] IP Multimedia Subsystem (IMS); Stage 2.

[S3-030223] Key management for the use of http at the Mt reference point in the IMS, source: Siemens, SA3#28.

[S3-030224] Security protocols for the use of HTTP at the Mt reference point in the IMS, source: Siemens, SA3#28.

[S3-030245] HTTP Security in Mt interface, source: Ericsson, SA3#28.

[S3-030256] Analysis of HTTP authentication, source: Nokia, SA3#28.

[S3-030325] LS on security solutions for the Ut reference point, source: CN1, N1-030933.