3GPP TSG SA WG3 Security — S3#25 **S3-020528**
8 - 11 October 2002
Munich, Germany

Source:	**Nokia**
Title:	**HTTP Security**
Document for:	**Discussion /Decision**
Agenda Item:	**7.17**

Abstract

This paper is a study of HTTP security under request from SA2 WG. One solution very much based on IETF existing protocol is presented. It also combines 3GPP Digest AKA for authentication as advantage.

1. Introduction

SA2 is currently working on a number of IMS related work items for release 6 including the stage 2 for the Presence Service. Proposals have been presented in SA2 suggesting the use of HTTP within IMS for various service-related purposes. It has also been identified within SA2 that there are possible Security and Charging issues currently with the use of HTTP as part of the IMS. Though they have not yet identified any particular use scenarios for HTTP however it is likely that such scenarios will be identified by SA2 within release 6.

SA2 asked SA3 and SA5 to comment and investigate potential security and charging issues related to the use of HTTP within IMS for service related purposes (e.g. for UE control of service provisioning and manipulation of service related data, etc) [1].

This discussion paper is based on S2´s LS S2-022609, which requests SA3´s investigation on Security issues in use of HTTP with IMS. We have studied security implementations and one potential solution, where Authentication Proxy (AP), is introduced. It takes care of security on behalf of certain application servers e.g. Presence. As such the HTTP security function can be implemented with IMS system rather independently and efficiently.
We have also compared potential security protocols for HTTP security, namely IPsec and TLS.

2. HTTP Security

2.1. User authentication in the home network

By using the Authentication Proxy (AP) it is possible to authenticate UE on behalf of all Application services, based on AKA protocol. Only one HTTP security association is created between UE and Authentication Proxy.

UE shall be able to initiate an HTTP session. In this case, user authentication is performed between UE and AP using AKA over HTTP Digest, so the user does not need to have any password-like in the original design of HTTP Digest. Authentication Vectors (AV) for HTTP connection can be fetched from the HSS to the Authentication Proxy via Diameter based interface similar to the Cx interface (hereafter written as *Cx-like*). Re-use of the IMS authentication scheme can simplify the implementation in UE and Application servers. Also the sequence number management of AKA protects against replay attack. Note that, before establishment of HTTP session, TLS connection must be done first according to IETF RFC2818 [2]. In an alternative case, IPSec ESP connection can be established. In the next clause the two alternatives are compared. For the sake of simplicity, TLS is assumed in the figure below.

Figure 1 illustrates the solution that provides security for HTTP based connection in case where UE is in Home Network.

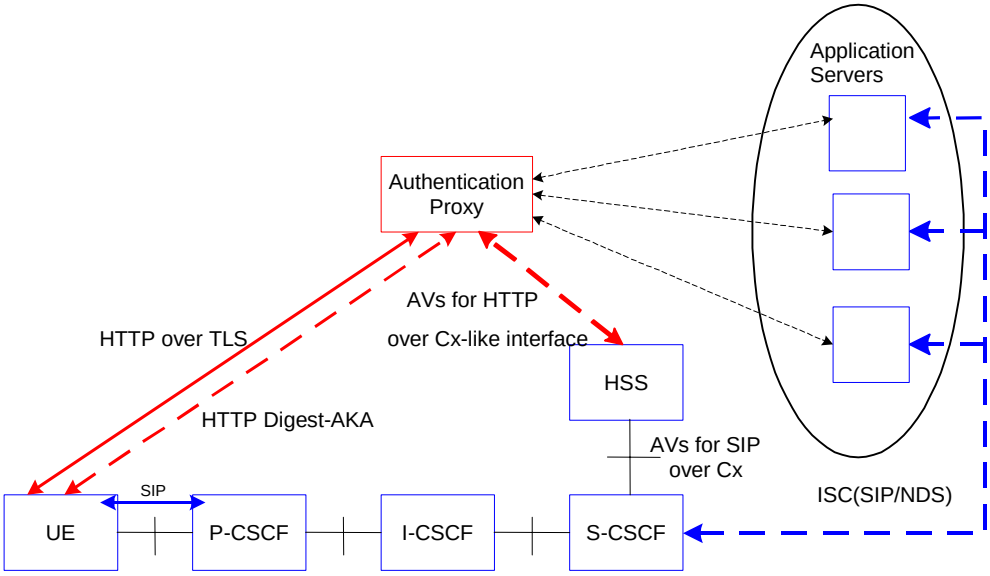

Figure 1. Security of HTTP connection for IMS data

In this solution HTTP security is independent from the IMS security. The common parts between Application servers and IMS are the same Digest AKA mechanism and the same user name (IMPI). SIP is used between UE and IMS, and also through ISC interface. Cx and Cx-like interfaces are Diameter based and also protected over NDS/IP.

This solution does not require registration of UE to the IMS before accessing to some Application Server, if this service requires HTTP transport only. This independence also allows operators to add Application service later on the top of existing IMS.

2.2. Transport security

TLS (SSL also) was designed for applications directly on top of transport layer, such as HTTP, SMTP or FTP. Both the HTTP and TLS require reliability of data delivery, thus usually run on top of TCP stack. Now that TCP is mandated in IMS, the use of TLS seems to be a permitted solution for HTTP.

Compared with IPsec, TLS obviously is optimized for HTTP data security. It resolves credentiality closely with application located in client and server. There have been various practices in the Internet, such as banking, e-purchasing, using TLS/SSL for HTTP as protocol. Standard has been established secure and mature in this aspect [4]. Comparatively, IPsec is sufficient to provide data security in hop level, but not session level.

2.3. Authentication Proxy

The Authentication Proxy supports application protocol (HTTP) level authentication of user identity and also establishes integrity and confidentiality protected connection based on TLS between UE and AP. The mutual authentication between UE and AP is based on Digest AKA using IMPI as a user identifier.

HTTP Digest AKA-procedure is a replica of the similar procedure specified by 3GPP and used in IMS for the authentication of UE over Digest AKA (AKA-procedure is executed during the SIP registration). Digest AKA is supported both by UE and S-CSCF.

AP is actually an HTTP–alike server, which terminates the TLS-connections and it has the ability to route traffic between the UE and the Application Servers. The security association may be maintained between sessions and it is renewed in each run of the AKA procedure.

The use of TLS between the UE and the Authentication Proxy to protect HTTP connection does not require additional standardisation work in IETF. UE is authenticated using HTTP Digest-AKA via the secure TLS connection.

To make sure the contacted AP is the intended server, it is recommended to process server authentication by requesting server's certificate. When IMS service is located at the home network, the verification shall be easy, because usually the root certificate of the home CA is available in terminal.

After a successful mutual authentication over TLS-protected 1st hop UE can have access to several application servers over a single security association.

AP may also establish TLS connections between AP and Application servers but this part is not further discussed in this contribution.

2.4. Interface between Authentication Proxy and HSS

Existing 3GPP Cx application could be reused for the IMS based services. Although the Cx application contains more complicated commands, only the authentication commands are needed. Authentication Proxy should therefore, only use them and thereby according to the Cx application the HSS shall not initiate other commands, because there is no 'SIP registration state' in the Diameter client node (e.g. S-CSCF). HSS does not see any distinction whether S-CSCF or AP requesting the authentication items.

The current Cx specification mandates that the server name, i.e. S-CSCF name, is included into the Multimedia-Auth-Request (MAR). This is needed in IMS, e.g. in the initial registration, so as to route SIP messages to the S-CSCF. AP requesting authentication items does not need to include the server name. HSS can decide to maintain the existing IMS registration state, e.g. the name of the S-CSCF, and not overwrite the S-CSCF name with the new name.

In Cx, the integrity key is mandatory and the confidentiality key optionally returned in the Multimedia-Auth-Answer (MAA) command. Application servers may not need these keys.

This is the content we see in *Cx-like* interface.

2.4.1. Sequence number management

By using a common system for sequence number management, IMS provides network authentication for SIP between UE and S-CSCF as well as for HTTP between UE and AP. The Authentication Center (AuC) functionality in HSS creates Authentication Vectors (AVs) using master secret key K of IMS, which is the key in ISIM for both SIP/IMS and HTTP security systems. Some of the generated AVs are used by SIP security system as is defined in the 3GPP TS 33.203 [3] and some are used by HTTP security system.

The Authentication Proxy asks one AV via interface from HSS/AuC for each HTTP-user authentication (between UE and AP).

Stored in ISIM in UE there is only one common set of sequence numbers for SIP/IMS domain and HTTP/Application domain. This sequence number management method is operator-specific. However, the recommended method is to store an array of sequence numbers in the ISIM. In that case, some of the indices in the array can be reserved for Application domain usage. Fetching only one AV at a time guarantees that the disturbance caused by the second domain is minimised. Each AV should be used only once.

The sequence number management method between IMS and Application domains in UE is similar to the one used in 3GPP TS 33.102 [4] between Packet Switched (PS) and Circuit Switched (CS) access network domains. Also there, CS and PS domain run AKA procedures independently of each other while using similar AVs. Re-synchronisation of the sequence numbers is also done similarly as for PS and CS domains in the cases where synchronisation is needed.

3. Conclusion and proposal

This contribution establishes a separate data channel than SIP connection. It does not assume the access to IMS previously. The study has shown that it is possible to offer authentication and other security services to different application servers in the Application cloud with only one Authentication Proxy. Then less performance is consumed in UE, because there is no need to connect to each Application Server separately to establish several security associations. Also, there are similar benefits on the network side: all Application servers may share the same security associations. The advantages of this scheme are also the re-use of AKA and partial functionality of the Cx interface.

Without Authentication Proxy sequence number management of SAs is much more complicated, separate authentications to every application server would cause extra delay and terminal burden; several connections to HSS decrease the system security.

The use of TLS to protect HTTP traffic is seen as a better solution as the use of IPsec, although the latter was chosen in the case of IMS security. This preference follows the general trend in the IETF and Internet domain services.

It is proposed to start the analysis based on knowledge investigated as baseline. And it is also proposed to query from SA2 for the deployment detail of HTTP feature and its security function required.

4. References

[1] 3GPP Tdoc S3-020475 Liaison on Security and Charging Issues with use of HTTP within IMS

[2] IETF RFC 2818: HTTP over TLS

[3] 3GPP TS 33.203 Access security for IP-based services v5.3.0

[4] 3GPP TS 33.102 Security Architecture v5.0.0