3GPP TSG SA WG3 Security — S3#26 **S3-020666**
19 - 22 November 2002
Oxford, UK

Source: **Nokia**

Title: **TLS versus IPsec for HTTP security**

Document for: **Discussion / Decision**

Agenda Item: **7.17**

1. Introduction

This discussion paper is based on S3-020528 HTTP Security [1], which presents one potential security solution for the use of HTTP with IMS so as to introduce another data channel between the user and the network.

UMTS Authentication and Key Agreement mechanism (AKA) can be used when performing HTTP Digest authentication [2]. Other than authentication, there is a need for user data protection.

In this discussion paper more specific information is given about the advantages of using TLS for HTTP security instead of IPsec. Compared with IPsec, TLS is optimized for HTTP data security.

2. TLS – IPsec comparison

3GPP R5 chose SIP as IMS signaling protocol. Initially SIP (RFC 2543) specifies UDP as the default transport protocol. Then IPsec was chosen since it can protect all traffic regardless of transport protocols. Later, IETF moved SIP direction to be more connection oriented, and mandated TCP as transport protocol. Thus, the previous disadvantage of TLS goes away, since TCP could be assumed available when using HTTP in the context of IMS. In current SIP specification RFC3261, the TLS is recommended as mean to provide security for UE and Proxy, by utilizing sips: to indicate the usage. Thus, TLS is a reasonable solution for HTTP in connecting with IMS network.

TLS [3] was designed for HTTP. Other applications directly on top of transport layer, such as SMTP or FTP can also utilize TLS. IETF has standardized TLS over HTTP. RFC 2818 describes how to use TLS to secure HTTP connections [4]. RFC 2817 explains how HTTP1.1 Upgrade mechanism can apply TLS to an open HTTP connection (HTTPS) [5]. Particularly, HTTPS is the dominant approach to securing HTTP.

2.1 HTTP awareness

HTTPS offers a possibility for HTTP application to mandate the usage of TLS by utilizing https:// . This is very important for HTTP, since historically most of web servers allow HTTP connection without underneath security. Consider the usage of HTTP is for “managing address-lists and authorization and service-related policies” (S2 LS, s3-020664) purpose, awareness of data protection is a sensible principle.

IPsec SA is established before any application can utilize the protection service. In other words, at this m the application can not be sure the low level IPsec is in place.

2.2 Connection closure and resumption

IPsec as the layer it functions, is in general for all transport protocols. When TCP connection is closed, IPsec SA is unaware of it. Thus often IPsec is established stable for a certain period, such as VPN between cooperate sites, between GGSNs. In HTTP case, the service policy needs to be defined for how long to keep the SA standing for all traffic. Comparatively if TLS is used, when a HTTP peer would like to close the connection, TLS shall send (server/client) close, followed with TCP FIN. This shall indicate to close TLS and TCP connection.

If system is configured to reuse TLS session, it is done by client to recall the session ID of TLS that was previously assigned and used. Then a quick handshake is done, to get new key material, session key and IV. In IPsec case, since SA keeps active stably, it can not be resumed. To refresh SA, the two peers need to negotiate a new SA, and delete the old one. Then SA refreshment is again a policy configuration that needs to be defined.

2.3 Proxies

HTTPS (HTTPS=HTTP+TLS) works directly between client and server. Regular HTTP proxy should establish a TCP connection with server by a method CONNECT defined in RFC2817 [5]. Then it is possible for the proxy to divert the request from UE to the corresponding servers based on the Request-URI of HTTPS.

In contrast, IPSec offers protection at the IP level. Ability to tunnel through proxies must be considered if there is proxies before Authentication Proxy (see S3-020528 [1]) or if Authentication Proxy forwards connection to other proxy. Thus the regular HTTP proxy may aware of the client, but not the identity of the other end other than IPsec knowledge.

3. Conclusion

This contribution introduces the advantages when using TLS with HTTP connection.

TLS is now a recommended protocol for SIP users which makes it now suitable for securing HTTP connections. Also, to provide the end-to-end security, security should be provided under the awareness of the application layer, that is HTTP application.

It is proposed to this S3 plenary meeting to consider the advantage of TLS for HTTP security, and adopt it as a working assumption for further development.

4. References

[1] 3GPP Tdoc S3-020528 HTTP Security

[2] IETF RFC 3310: Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)

[3] IETF RFC 2246: The TLS Protocol

[4] IETF RFC 2818: HTTP over TLS

[5] IETF RFC 2817: Upgrading to TLS Within HTTP/1.1