J. Floroiu
Fokus Fraunhofer

Internet-Draft
Expires: April 14, 2005

October 15, 2004

An User-to-User Authenticated Key Exchange Mechanism Based on the UMTS Authentication and Key Agreement (AKA) draft-floroiu-u2u-ake-00.txt

Status of this Memo

Intellectual Property Rights (IPR) Statement

Copyright Notice

Abstract

The present draft describes an user-to-user (u2u) authenticated key exchange mechanism based on the UMTS AKA mechanism [1]. The proposed scheme is based on the generation of security tokens (in fact encrypted public Diffie-Hellman keys) by the peer's operator. Such a security token along with credential information contained within the peer's AKA Authentication Vector (AV) enables two communicating peers to securely derive a shared key.

Introduction

Many protocols define security extensions aimed at protecting the data traffic or signalling between two communicating peers. Most of the security extensions are based on symmetric cryptography due to the relative computational efficiency of the symmetric cryptographic algorithms as compared to the asymmetric ones.

The establishment of a shared key between two communicating parties however requires a key establishment protocol and the presence of an infrastructure able to provide the credentials necessary to achieve the mutual authentication of the parties.

The present draft describes a mechanism based on "security tokens" issued by the peer's Home Subscriber Server (HSS) that enables two peers to securely derive a shared key using relatively unexpensive cryptographic operations. The exchange requires three trips and may be easily piggybacked into other signalling protocols (for example SIP).

Notations

|	concatenation
E(K,P)	encryption of payload "P" using the key "K"
A, B	A's respectively B's identity
AUTN	AKA Authentication Token
RAND	AKA Random Challange
XRES	Expected Response
IK	AKA Integrity Key
CK	AKA Cipher Key
..._X	a certain piece of information pertaining to entity "X"

1. Security Token Acquisition

Figure 1 illustrates the message exchange that enables a user to acquire a security token from the peer's HSS entity. This phase must precede the actual establishment of a secure connection between the two parties.

In the example, user A gets a public Diffie-Hellman key encrypted by B's HSS, along with B's credentials that later on will help B derive the encryption key. The exchange is assumed to take place over authenticated channels.

In the first message A provides the peer's identity and its public Diffie-Hellman key and gets it back encrypted with one of the B's private key along with the B's credentials that correspond to that key. HSS_A is assumed to be able to route the message based on B's identity to the appropriate HSS, with whom it must necessary share a trust relationship.

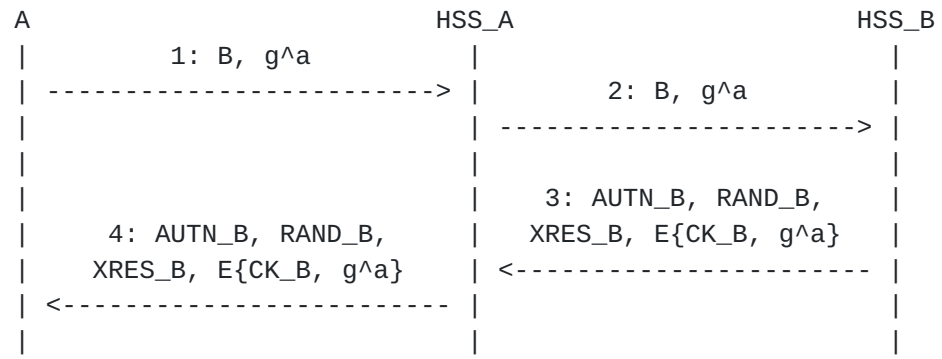

Figure 1

2. The Key Exchange

It is assumed that A and B have acquired such tokens prior to initiating an authenticated key exchange (Figure 2).

A initiates the key exchange by sending the security token along with a challange to B. B checks the authenticity of AUTN_B, derives CK_B and retrieves g^a. It then picks up a security token <AUTN_A, RAND_A, XRES_A, b, E{CK_A, g^b}> it has acquired from A's operator and computes the shared key K = g^(ab). Finally it replies in message 6 with the public part of the security token and the response encrypted with the shared key K.

Upon receiving message 6, A follows similar steps to authenticate the token and retrieve the shared key K. The exchange concludes with message 7, which contains A's response, based on which B can decide whether the party is indeed genuine and the exchange was sucessful.

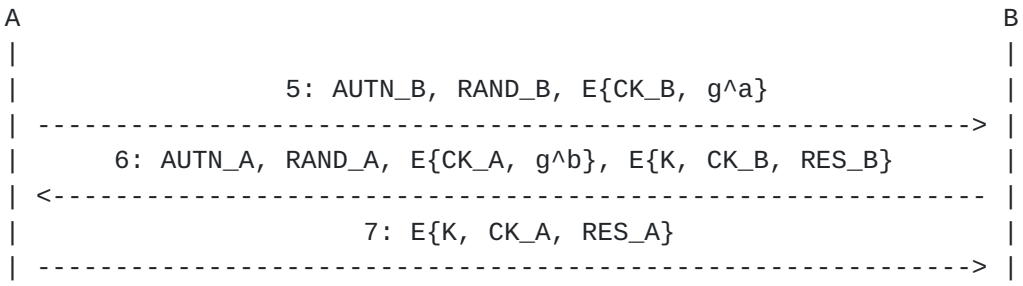

Figure 2

In order to enable the peers to verify that the original public Diffie-Hellman keys have not been modified on the fly (for instance by the HSS entities themselves), the shared keys used in the first phase to compute the security tokens are included in the messages 6 and 7. Both parties will therefore be able to check the integrity of the security tokens, which up to this stage have been opaque data.

Later versions of the draft will document the error sequences, currently missing.

3. Security Considerations

The main goal of the proposed protocol is to avoid the HSS entities to act as man-in-the-middle during the authenticated key exchange between two parties. As determined so far this purpose seems to be achieved, further analysis is however necessary.

4. IANA COnsiderations

None.

References

[1] 3GPP TS 33.102 v6.0.0 Security architecture, September 2003;

Author's Address

John W. Floroiu

Fokus Fraunhofer Institute for Open Communication Systems
Kaiserin Augusta Allee 31
10589 Berlin, Germany
Email: floroiu@fokus.fraunhofer.de

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Full Copyright Statement