3GPP TSG SA WG3 Security – S3 #13 **S3-000328**

May 24-26, 2000

Yokohama, Japan

(Ad-hoc meeting on MAP Security, May 23, 2000)

Source: Motorola

Title: Use of IPSec IKE for layer 2 key distribution

Document for: Discussion

Agenda item: tbd

Abstract

Use of IPSec IKE for the "layer 1" process of network-to-network key distribution may be the preferred solution. If layer 2 is accomplished by a similar mechanism, then it is essential that the Network Elements (NEs) generate their own public/private key pairs in order to achieve the full benefits of Public Key Cryptography.

1. Introduction

Network security layer 2 is described in 3G TS 33.102 v3.4.0 (UMTS Security Architecture). In particular, section 7 of 3G TS 33.102 describes a three-layer process for providing security of network messages. The first of these, layer 1, establishes a session key Ks between a pair of "Key Administration Centers" (KACs) by means of an asymmetric key exchange. Layer 2 then distributes this key to Network Elements (NEs) that will subsequently use it to apply protection to network messages. The mechanism for protecting network messages is performed by layer 3.

Similarities between the key distribution requirements of layer 1 and layer 2 tend to encourage the selection of similar mechanisms in order to achieve commonality of design. In 3G TS 33.102, a method for layer 1 based on ISO/IEC 11770-3 is described, and the layer 2 solution as proposed is based on the same mechanism.

It may also be prudent to consider a layer 1 mechanism based on IPSec IKE, due to its widespread popularity and implementation in IP products. If this mechanism were to be chosen for network security layer 1, then it would likely become a prime candidate for the layer 2 process.

This analysis examines some characteristics of IPSec IKE that should be considered if it were to be chosen as the layer 2 distribution mechanism between KACs and NEs.

2. "Main Mode" Preferrence

IPSec IKE is a two-phase protocol. Phase 1 utilizes either 3 messages ("aggressive mode") or 6 messages ("main mode"), between two endpoints, to establish a session key. Once a session key has been established, phase 2 is performed between the two endpoints in order to complete the Security Association (SA) which enables both endpoints to protect messages transferred between them.

Thus, the KAC-KAC session key KS may be distributed between a KAC and a Network Element by

performance of IPSec IKE (both phases), followed by symmetric ciphering and integrity checksum calculation on a single message containing KS.

During Phase 1, use of the aggressive mode, with only three messages, is more efficient for most applications. However, the use of aggressive mode requires that identity information be sent without the application of ciphering. This is undesirable in a complex network environment because of possible signal tracing and targeted attacks. Hence the increased identity confidentiality afforded by the 6-message "main mode" seems a prudent choice, despite the increase in network traffic over the aggressive mode. This increase of network traffic is further justified by the anticipated low usage of network security layer 1 and layer 2 protocols.

3. NE Self-Generation of Public Key/Private Key Pairs

In 3G TS 33.102, it is suggested, in the introduction section of Annex E, that "KACs of the different networks…generate and distribute asymmetric key pairs for the network elements…" In some instances this may be an accepted practice. However, it can be shown that the combined usage of IPSec IKE and KAC-generated asymmetrical key pairs for NEs would reduce the protocol to transferring a symmetric key via a secure channel to NEs.

This may be explained as follows. In using IKE for a layer 2 key establishment, the KAC and NE execute a Diffie-Hellman key agreement. Suppose that a KAC were to send a key pair (Public Key, Private Key) to an NE via a secure channel. (It is noted that the use of a secure channel to transport a Private Key is considered to be a complex problem in a commercial environment.) Later, during the layer 2 process, the NE would send the Public Key generated by the KAC to the same KAC. However, since the KAC already knows all components of the exponent, it could have pre-calculated the result. Thus the NE contributes no new information to the key agreement process, which includes the performance of modular exponentiation.

Therefore the use of IPSec IKE requires that the Network Elements generate their own Public Key, Private Key pairs.

4. Anticipated Changes to 3G TS 33.102

The following sections will likely be affected if IPSec IKE is used as a mechanism for both layer 1 and layer 2 key exchanges.

Section 7.1.1 As required by IPSec IKE description for layer 1

Section 7.2.2 Replace the detailed description of ISO/IEC 11770-3 with IPSec IKE for layer 1.

Section 7.3 Minor changes to reflect the fact that IPSec IKE must be performed between each KAC and NE prior to distribution of the KAC-KAC key Ks from the KAC to the NE.

5. Recommendation

It is recommended that 3GPP TSG SA WP3 modifies 3G TS 33.102 by the selection of IPSec IKE as the layer 1 key distribution process, and that the same mechanism be adopted for layer 2. Once this is accomplished, it is recommended that the considerations as stated above be considered to obtain optimum usage of IPSec as a layer 2 mechanism. Subsequent CRs will need to address specific changes to 3G TS 33.102 to implement these recommendations.