3GPP TSG SA WG3 Security – S3#23 **S3-020213**

14 - 17 May 2002

Victoria, BC, Canada

Source:	**SSH Communications Security Corp**
Title:	**Deriving unidirectional keys for IPSec protection of SIP messages between UA and P-CSCF**
Document for:	**Discussion**
Agenda Item:	**T.B.D**

1 Introduction

TD S3z020058 considered a creation of unidirectional key for IPSec at ME with algorithms negotiated in security mode set-up. However, the additional security achieved through this procedure is not great compared to the required functionality and a simpler mechanism would be desirable.

This contribution considers a simpler mechanism similar to key creation in Internet Key Exchange (IKE) protocol key derivation.

2 Key Derivation in IKE

In IKE, encryption and data origin authentication key generation is done in the following way:

The pre-shared key is first used to calculate SKEYID according to (1)

SKEYID = prf(pre-shared-key, Ni_b | Nr_b) (1)

where

SKEYID is the secret on which all subsequent secrets are based

PRF is Pseudo-Random Function

pre-shared-secret is the secret shared by both initiator and responder

Ni_b and Nr_b are the initiator’s and responder’s nonces

and the derived SKEYID is used both for keying material (2,3,4) and for hashes (5,6).

SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0) (2)

SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1) (3)

SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2) (4)

HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b) (5)

HASH_R = prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b) (6) where

SKEYID_d is the secret used for IPSec key generation.

SKEYID_a is the key used to provide data origin authentication for IKE messages.

SKEYID_e is the key used to encrypt and decrypt IKE messages.

CKY-I and CKY-R are the cookies of the initiator and responder.

g^xr and g^xi are the Diffie-Hellman public number of the initiator and responder.

Dii_b and Dir_b are the identities of the initiator and responder.

SAi_b is the entire SA payload.

There are still other issues related to the creation of IPSec keys, but this information is sufficient for unidirectional key generation for IPSec from CK and IK.

3 Unidirectional Key Derivation from CK and IK

Both IK and CK are already negotiated secrets between UE and P-CSCF and can be used to create unidirectional keys in the following way:

IK_U = prf(IK, protocol, SA_ID_U | 0)

IK_P = prf(IK, protocol, SA_ID_P | 1)

CK_U = prf(CK, protocol, SA_ID_U | 0)

CK_P = prf(CK, protocol, SA_ID_P | 1)

Where

IK_U and IK_P are the integrity keys, IK_U is from UE to P-CSCF and IK_P from P-CSCF to UE.

prf is the pseudo-random function (PRF) used here is the integrity protection algorithm negotiated with sip-sec-agree [3].

protocol is the used security protocol (AH or ESP in the case of IPSec).

SA_ID_U and SA_ID_P are SPIs, SA_ID_U is SPI from UE to P-CSCF and SA_ID_P is SPI from P-CSCF to UE.

0 and 1 are values represented by a single octet that indicate the direction of SA and to guaratee that inputs of PRF are unique for both directions.

Compared to the mechanism used in IKE, SKEYID is replaced with IK or CK and some parameters have been replaced with others or dropped away. Additional parameters such as lifetime can be added to PRF input.

3.1 PRF Output Truncation and Expansion

Depending of the selected PRF, the output value might differ from the 128 bits and the procedures of truncation and expansion must be defined.

3.1.1 Truncation

If PRF output is greater than 128 bits, only the128 leftmost bits will be used. See Chapter 5 in [2] for more information.

3.1.2 Expansion

If the selected PRF does not provide enough keying material, PRF output shall be expanded with the following method until sufficient amount of keying material has been obtained.

IK_U = IK1 | IK2 | IK3 ...

where

IK1 = prf(IK_U, 0)
IK2 = prf(IK_U, IK1)
IK3 = prf(IK_U, IK2)
...

The method is similar to IK_P, CK_U and CK_P. If the final keying material is greater than 128 bits, the material must be truncated as described in Chapter 3.1.1 Truncation

4 Benefits

This functionality will

- Avoid a negotiation of additional algorithms in [3].
- Follow some known key generation mechanism that is found to be effective and relative secure.
- Reduce complexity of unidirectional key derivation.
- Reduce overhead in algorithm negotiation.

5 Proposal

SA3 #23 are asked to consider the presented mechanism instead of negotiating specific key derivation algorithms for bilateral keys.

Reference

[1] D. Harkins & D. Carrel, ”RFC 2409: The Internet Key Exchange (IKE)”, November 1998.

[2] H. Krawczyk & M. Bellare & R. Canetti, “RFC 2104: HMAC: Keyed-Hashing for Message Authentication”, February 1997.

[3] J. Arkko & et al., ”Internet draft: Security Mechanism Agreement for SIP Sessions”, April 2002