3GPP TSG SA WG3 Security – S3#23 **S3-020214**

14 - 17 May 2002

Victoria, BC, Canada

Source: **SSH Communications Security Corp**

Title: **Usage of PF_KEY API in IPSec/ESP Parameter Handling for SIP Integrity**

Document for: **Discussion**

Agenda Item: **T.B.D**

1. Introduction

PF_KEY [1] is a socket protocol family used by trusted privileged key management applications to communicate with an operating system's key management internals. In the case of parameter handling for SIP integrity, PF_KEY would mean an API between UMTS AKA and IPSec ESP implementation. However, numerous limitations and shortcomings make usage of PF_KEY questionable between UMTS AKA and IPSec implementation at UE.

This contribution considers PF_KEY limitations.

2. Limitations of PF_KEY

There are several limitations that cannot be configured / need to be updated with the RFC 2367.

SA types

The PF_KEY specifies only AH and ESP (and refers to the old RFCs1827 and 1827). The document does not specify IPComp.

As default, there seems not to be a way to configure SA bundles (AH + ESP). Bundles can probably be done a loose interpretation of the SADP_GETSPI calls but this is not documented in the specification.

Algorithms

Only the following algorithms are specified

- hmac-md5
- hmac-sha1
- des-cbc
- 3des-cbc
- null algorithms

Some implementations have added cast128-cbc, blowfish-cbc, and rijndael-cbc as private allocations (they have only meaning within the same IPSec implementation) as well as algorithms for compression algorithms of IPComp.

SA encapsulation mode

No method to configure encapsulation. Probably the encapsulation mode is taken from the SA proxy IDs (transport for host-to-host and tunnel for others). This also means that there is no way to configure NAT-T's UDP encapsulation or other additional encapsulations like L2TP.

Some implementations have a private SA extension for selecting the encapsulation mode.

IKE identities

The IKE identities are stored in the SADB. The PF_KEY only supports IP addresses (with an optional prefix length), fully qualified domains names (FQDN), and email addresses (USER@FQDN). There is no support for distinguished names (DN) or generic names (GN).

3. Alternatives in PF_KEY Usage

Due to problems defined in the above Chapters, PF_KEY API cannot be used as defined in [1]. The alternatives in PF_KEY usage are

1. To extend RFC 2367 with necessary configuration parameters either
    a. Updating RFC 2367 to reflect 3GPP needs.
    b. Make private allocations for 3GPP use.
2. To write a new specification describing the parameters required for IPSec/ESP usage for SIP integrity. No implicit reason is seen, why this specification should be an informational IETF RFC. 3GPP specification should be sufficient.

4. Proposal

SA3 #23 are asked to consider a new specification describing the required parameters for IPSec/ESP usage for SIP integrity instead of extending PF_KEY API to be suitable for 3GPP needs.

The majority of identified PF_KEY API problems are not related to the current requirements of 3GPP, but these requirements can be assumed to change in the future. In these situations, the usage of PF_KEY might cause restrictions and require new extensions.

Reference

[1] D. McDonald & C. Metz & B. Phan, “RFC 2367: PF_KEY Key Management API, Version 2”, July 1998.