3GPP TSG SA WG3 Security — S3#13 **S3-000311**
24-26 May, 2000

3GPP TSG SA WG3 Security — adhoc on MAP security
23 May, 2000
Yokohama, Japan

Document Title: **Using IKE for Layer I of MAP Security**

Source: T-Mobil / T-Nova

Document for: Discussion

1. Scope and Objectives

This document investigates the possibility of using the IPsec key management protocol IKE (Internet Key Exchange, cf. [RFC 2409]) for transporting session keys between Key Administration Centres (KACs) of different networks.
There are two reasons for proposing IKE instead of the message format formerly specified in 33.102 :

- Although the format specified in 33.102 was based on an ISO-Standard protocol for key transport, there do not seem to be off-the-shelf products available at the moment that utilise this key transport mechanism. This situation is different with IKE, which is a well-understood, standardised protocol as well. Since it has been agreed in SA3 to look for an "automated" solution for Layer I key transport in R'00, looking at IKE seems to be a possible way forward.
- It is anticipated that in the future more and more network elements will understand IP. As soon as this is the case, IPsec will probably be used for key management in the layers II and III. On the other hand, it is undesirable to have different key management protocols implemented in the different layers.

The document defines requirements for Layer I key transport and investigates, whether IKE can fulfil these requirements. The main purpose of the document is not to bring forward yet another key management protocol for Layer I, but to stimulate discussion about which solution for Layer I can be realised the quickest.

2. Some Background on IPsec and IKE

IPsec [RFC 2401] uses two protocols to provide traffic security -- Authentication Header (AH) and Encapsulating Security Payload (ESP). Both protocols are described in more detail in their respective RFCs [RFC 2402] and [RFC 2406].

- The IP Authentication Header (AH) provides connectionless integrity, data origin authentication, and an optional anti-replay service for IP packets.
- The Encapsulating Security Payload (ESP) protocol may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connection integrity, data origin authentication, and an anti-replay service.

Depending on the application's security requirements, both protocols can be used in combination or only individually. Because these security services use shared secret values (cryptographic keys), IPsec relies on a separate set of mechanism for putting these keys in place. (The keys are used for

authentication/integrity and encryption services.) A specific public-key based approach is IKE for automatic key management, but other automated key distribution techniques may be used.
The IPsec functionalities are based on the concept of a security association (SA). A Security Association (SA) is a relationship between two or more entities that describes how the entities will utilise security services to communicate securely. This relationship is represented by a set of information that can be considered a contract between the entities. The information must be agreed upon and shared between all the entities, comprising the encryption and hashing algorithms deployed, version number of key material for authentication and encryption, key lifetimes, and a label indicating the confidentiality level of the data.

The IPsec protocol ISAKMP (Internet Security Association and Key Management Protocol, [RFC 2408]) provides a common message format for securely negotiating the SA and authenticating the participating entities; authentication may either be based on pre-shared secrets and keyed hash-functions (e.g. HMAC) or on public-key certificates. Authentication is performed in the first of the two phases of the negotiation protocol, securing the negotiation process between the peers. It can be based on digital signatures, public key methods as well as on pre-shared secret keys. The second phase is then used to set up the SA parameters. That phase can also be used for changing the keys after some time of use. Depending on the level of confidentiality and the number of messages exchanged between both communicating peers during the negotiation process, several modes of operation are standardised for use in IKE (main mode [6 messages, identity protection], aggressive mode [3 messages, no identity protection], quick mode [3 messages, running in an encrypted channel established by either main or aggressive mode], new group mode [2 messages], cf. [RFC 2409]). As listed in [RFC 2407], some algorithms for encryption or authentication must be implemented in IPsec compliant software, whereas some algorithms are only optional:

- mandatory encryption algorithms: DES
- optional encryption algorithms: DES-CBC-IV64, DES-CBC-IV32, 3DES, RC4, RC5, IDEA, CAST, BLOWFISH, NULL (no encryption)
- mandatory authentication algorithms: MD-5, SHA
- optional authentication algorithms: DES-MAC

OAKLEY (cf. [RFC 2412]) is a Diffie-Hellman based protocol for key exchange using authentication in addition to the basic Diffie-Hellman protocol for providing protection against the "man-in-the-middle" attack. OAKLEY can be integrated into ISAKMP, both protocols together being called IKE, providing a secure, authentic key exchange protocol for two peer entities. For the Diffie-Hellman protocol based key exchange, three group types have been standardised in OAKLEY (MODP [modular exponentiation group]; optionally, ECP [elliptic curve group over GF[P]] and EC2N [elliptic curve group over GF[2^N]] can be implemented).

3. Requirements for Layer I

In layer I two single hosts have to exchange session keys in a confidential, authenticated way. The requirements on a key exchange protocol for layer I are therefore:

- Peer authentication
- Confidentiality, authenticity and integrity of keying material
- Establishment of different keys for the two directions

These requirements are fulfilled by IKE. Authentication of identities and cryptographic parameters may either be based on pre-shared secrets (possibly exchanged in course of a roaming agreement between the two different networks) or on public-key certificates and digital signatures. Moreover, in the so-called "main mode" consisting of six messages, IKE provides also identity confidentiality of the two parties, but it is doubted whether this is a requirement for layer I, so that the "aggressive mode" of IKE consisting of three messages should suffice. Note further that in IKE different keys for both directions are generated from the shared DH-secret g^{ab} by putting g^{ab} and an entity-specific parameter SPI (Security Parameter Index) into a pseudo-random function.

3.1. Requirements on the SAs for securing MAP based on IKE

The following information has identified to be included as part of the SA for successful securing the MAP communication:

a) the encryption algorithm ID
b) the key version number
c) the key used to encrypt the communication
d) the protection modes
e) a "remove all" indicator

Based on the flexibility offered by the definition of the IP Security DOI [RFC 2407] and the underlying ISAKMP [RFC 2408] used by IKE, the following suggestions are made as a starting point for further discussions to provide the necessary MAP securing data in the existing data structures (listed in the sequence of the requirements list above):

a) A set of 10 ESP encryption algorithms and 3 AH authentication algorithms (listed above in Section 2) has been defined for use in ISAKMP, where only the DES, MD5, and SHA algorithm implementation is mandatory. If none of the 10 existing ESP encryption algorithms [RFC 2407, see p. 10 and 26] and the 4 authentication algorithms [RFC 2407, see p. 8, 14, and 26] would be suitable for MAP security, either additional algorithms could be officially registered by IANA (Internet Assigned Numbers Authority) for that purpose, private algorithms could be used together with algorithm identifiers from the value domain marked "private", or a "private" MAP specific encapsulating mode, which then should also comprise that MAP specific encryption algorithm, could be defined [RFC 2407, see p. 14].
b) – no information on the meaning of "key version number" available – Since no such attribute is currently specified in IKE, a user specified attribute "key version number" could be defined and transmitted using the Data Attributes fields [RFC 2408, p. 26]
c) The standard key exchange mechanisms provided by the IPsec protocols could be used
d) The standard IPsec situation definition [RFC 2407, see p. 3] could probably be used to specify the required protection mode(s).
e) For a "remove all indicator", a first suggestion would be the use of the Delete Payload fields [RFC 2408, p. 41] to remove an existing SA. A second suggestion would be the use of a special SA Life Type / SA Duration value (e.g. with remaining life time of 0 sec or 0 bytes to indicate the termination of the secured connection) [RFC 2407, see p. 13].

In the case that requirements for securing MAP communication are not satisfied up to a reasonable level based on the currently available protocols, one may think of extending the IKE by using additional ISAKMP payload types to carry that additional information which could not be covered by the current payload types. Such changes could be introduced and standardised [RFC 2408, p. 22 and 76] to be interoperable with other applications and software providers without modifying the whole protocol structures.

3.2. Options for using IKE

Having run IKE between two Key Administration Centres, one has two options:

- "Misuse" the keys transported by IKE by using it also for MAP security
- Put a dedicated MAP-security key into an IP-packet which is protected as an ESP

The first option seems to be more straightforward (and is possibly quicker), but is perhaps more difficult to implement. Moreover, it is not clear how a key transported that way can be further used for layer II by using the same protocol between KAC and network elements. One possibility is to use IKE’s client mode, which is mentioned in [RFC 2409, Sec. 2] as “where the negotiating parties are not the endpoints for which security association negotiation is taking place.” It is to be investigated whether this client mode can be used for layer II.

The second option is "heavier" but has the advantage that other key-related information (log files, serial numbers etc.) can be transported along with the key by putting it into another ESP (if IP is used for transport between the KACs) or another protected MAP dialogue (if MAP is used as transport mechanism).

4. Products

There are quite some products available today which implement IPsec and IKE; among others one should name:

- Radguard ciPro (www.radguard.com): Hardware-based security gateways
- PGPnet: Purely software based solution, but good alternative for single-host applications (such as the one in Layer I).
- Utimaco SafeGuard VPN (www.utimaco.de/english)

5. Conclusion

IKE seems to be well suited for key exchange in Layer I. Its biggest advantages are the availability of off-the-shelf products and its being future-proof in light of the envisaged transport of MAP over IP. Moreover, regular key updates and/or changes of algorithms can be easily accomplished within the IKE framework. IKE might, however, be a bit "heavyweight" if used for the sole purpose of key exchange in Layer I.

Our discussion has been independent of the transport mechanism for the IKE related messages, be it IP or MAP. Moreover, it should be noted that the use of IPsec for Layer I is independent of the transport mechanism for MAP in the lower layers, be it SS7 or IP. The problem of how to cope with the situation that some NEs may run MAP over SS7 and others MAP over IP in future therefore still needs to be investigated.

6. References

[RFC 2401] Security Architecture for IP
http://www.ietf.org/rfc/rfc2401.txt

[RFC 2402] IP Authentication Header
http://www.ietf.org/rfc/rfc2402.txt

[RFC 2406] IP Encapsulating Security Payload (ESP)
http://www.ietf.org/rfc/rfc2406.txt

[RFC 2407] IP Security Domain of Interpretation
http://www.ietf.org/rfc/rfc2407.txt

[RFC 2408] Internet Security Association and Key Management Protocol (ISAKMP)
http://www.ietf.org/rfc/rfc2408.txt

[RFC 2409] The Internet Key Exchange (IKE)
http://www.ietf.org/rfc/rfc2409.txt

[RFC 2412] The OAKLEY Key Determination Protocol
http://www.ietf.org/rfc/rfc2412.txt