A Survey on IPSEC Key Management Protocols

Jong-Hyeon Lee
jhl21@cl.cam.ac.uk

University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG England

Abstract. The working group IPSEC of the Internet Engineering Task Force (IETF) is considering IP-layer key management standards. Currently several protocols have been suggested as candidates of the IP security key management standards. They are ISAKMP, Oakley, SKIP, and Photuris. SKEME is another suggestion for an IP-layer key exchange mechanism but is not a suggested Internet Draft.
In this paper, we present a survey of these protocols and a comparison among them. A brief analysis on these protocols is also included. The potential threats to these protocols and problems in implementation are also described. We suggest resolutions for these problems.

1 Introduction

The Internet is now expanding and the connection to the Internet is becoming easier. The applications of the Internet are increasing and diversifying continuously. Furthermore, many security-sensitive applications are emerging such as electronic commerce, banking, and so on. The need of the Internet security became clear.

To meet such needs, the working group IPSEC of the Internet Engineering Task Force (IETF) is currently considering next generation IP-layer security. Specifically the IETF decided that IPSEC was a mandatory requirement for a compliant implementation of IPv6. It was decided upon because the community felt that without such a mandatory feature, security would not be implemented in a lot of products, even though there is a pressing need for security on the Internet. The reasons for this belief are many and varied and beyond the scope of this document. Suffice it to say that IPSEC technology is mandatory in IPv6. Basic requirements for this mandatory protocol are strong security and interoperability.

The key management protocol is an essential and important issue of IP security. Several protocols have been suggested for IP security key management standard. They are ISAKMP, Oakley, SKIP, and Photuris. In addition to them, SKEME is another key management protocol for IP security, although it is not suggested as an Internet Draft.

In this paper, there will be given a survey of these protocols. Based on this survey, we will show a comparison between these protocols and a brief analysis on them. The potential threats to these protocols and considerable weak points in implementation will be described.

2 Protocol Survey

Several key management protocols are suggested and are updated continuously. These are ISAKMP [23], Oakley [24], SKIP [6], Photuris [17], and SKEME [18]. All of them are using the Authentication Header (AH) [4] and the Encapsulating Secure Payload (ESP) [5] which are required in the RFC 1825 Security Architecture for the Internet Protocol [3]. In this section, the survey of these protocols will be described.

These key management protocols is designed for current and next generation IP protocols, that is, IPv4 and IPv6. They can operate over TCP/UDP or IP directly and they are connected to TCP/UDP via specified port. Some protocols are compatible other protocols and some protocols are not. The scope of each protocol is different each other. Some protocols are defined generally and widely and some protocols specifically.

2.1 ISAKMP

ISAKMP stands for the Internet Security Association and Key Management Protocol and is suggested by D Maughan, M Schneier, J Turner, and M Schertler of the National Security Agency and the Terisa Systems Incorporated [23].

ISAKMP is a protocol which provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchanges. It supports Security Association (SA) and key management in an Internet environment. It also defines the procedures for the authentication of peers, creation and management of SAs, key generation techniques, and treatments for denial-of-service and reply attacks.

A Security Association is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. SA establishment is a part of the key management protocol defined for IP based networks. SA supports different encryption algorithms, authentication mechanisms, and key establishment algorithms for other security protocols, as well as IP security.

When processing an outgoing IP packet for authentication, the first step is for the sending system to locate the appropriate security association. All security associations are unidirectional. When accessing SA attributes, entities use an identifier referred to as the Security Parameter Index (SPI) [3–5]. The selection of the appropriate SA for an outgoing IP packet is based at least upon the sending user id and the destination address. When host-oriented keying is in use, everyone sending the user id will share the same SA to a given destination. When user-oriented keying is in use, then different users or possibly even different applications of the same user might use different SAs.

ISAKMP provides the protocol exchanges to establish a SA between negotiation server entities followed by the establishment of a SA by the negotiation server entities on behalf of some protocols such as AH/ESP.

A digital signature algorithm is used within ISAKMP. The protocol provides a facility for identification of different certificate authorities, certificate types (X.509, PKCS #7, PGP, DNS SIG and KEY records), and the exchange of the certificates identified.

For the public key cryptography, the key exchange function in ISAKMP includes key establishment method, authentication, symmetry, perfect forward secrecy (PFS), and back traffic protection. ISAKMP users should choose additional key establishment algorithms based on their requirements. ISAKMP does not specify a specific key exchange and communication protocol with trusted third parties or certificate directory services. There is a proposal for using Oakley key exchange in conjunction with ISAKMP [16].

There are preparation for some threats. To protect the computer resources from denial-of-service, ISAKMP uses anti-clogging-token "cookie". ISAKMP also prevents connection hijacking by linking the authentication, key exchange and SA exchanges. Middleperson attacks include interception, insertion, deletion, and modification of messages, reflecting messages back at the sender, replaying old messages and redirecting messages. The linking of the ISAKMP SA exchanges prevents the insertion of messages in the protocol exchange. The ISAKMP protocol state machine is defined so deleted messages will not cause a partial SA to be created, the state machine will clear all state and return to idle. The state machine also prevents reflection of a message from causing harm. The requirement for a new cookie with time variant material for each new SA establishment prevents attacks that involve replaying old messages. The ISAKMP authentication requirement prevents an SA from being established with other than the intended party. Messages may be redirected to a different destination or modified but this will be detected and an SA will not be established. In ISAKMP draft, there are some recommendations for abnormal situation.

ISAKMP supports the Internet Security Domain of Interpretation (DOI). DOI identifier is used to interpret the payloads of ISAKMP payloads, that is, it supports naming and interpretation of security services. DOI defines situation, security policy, and syntax for specification of proposed security services, scheme for naming security-relevant information including encryption algorithms, key exchange algorithms, security policy attributes, and certificate authorities. The "situation" means the set of information that will be used to determine the required security services. Furthermore, users can define new DOIs. ISAKMP requires that all systems must support the Internet Security DOI.

Using DOI, users can design their own security environment such as security policies, cryptographic algorithms, and modes. In the conjunction between ISAKMP and Oakley, D Harkins and D Carrel in Cisco Systems specified Oakley modes in DOI such as main mode, aggressive mode, quick mode, and new group mode [16]. D Piper in the same company suggested IP security DOI for ISAKMP [25].

In November 1996, new draft on in-line keying within the ISAKMP is suggested by W Sommerfeld [26]. It seems to be a trial to support some character-

istics of SKIP within ISAKMP framework. It could be used with ISAKMP and Oakley.

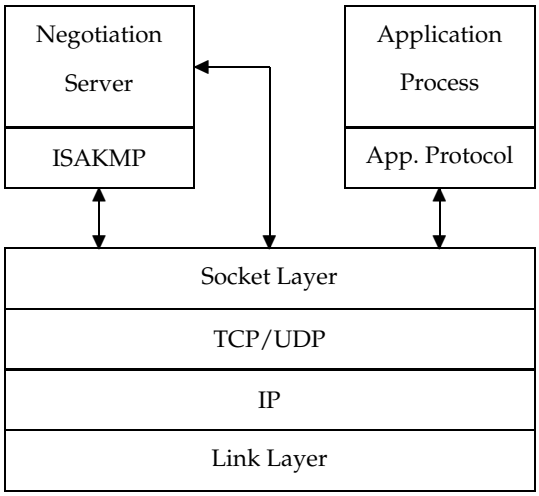

Fig. 1. ISAKMP Relationships

Fig. 1 illustrates the relationship between ISAKMP and other protocol stacks. The UDP port of ISAKMP is 500 which is assigned by the Internet Assigned Numbers Authority (IANA).

2.2 Oakley

Oakley is a general key exchange protocol which is suggested by HK Orman of the University of Arizona [24]. The keys that are generated by Oakley might be used for encrypting data with a long-time privacy lifetime, 20 years or more. Oakley is used to establish a shared key with an assigned identifier and associated authenticated identities for the two parties.

Oakley is a key determination protocol which supports perfect forward secrecy and user-defined abstract group structures for the Diffie-Hellman algorithm. It is designed to be a compatible component of the ISAKMP for managing security associations.

Oakley has the following characteristics:

- Oakley uses the Diffie-Hellman exponentials for determining a shared key and achieves perfect forward security using the shared key.
- To avoid denial-of-service attack, Oakley adopts anti-clogging tokens (”cookies”). In Oakley, Cookies are used not only for anti-clogging but also for key naming. The pair of cookies of two parties becomes the key identifier.

- Oakley allows the two parties to select mutually agreeable algorithms for the protocol.
- Authentication in Oakley does not depend on encryption using the Diffie-Hellman exponentials. It validates the binding of the exponentials to the identities of the parties.
- Before authentication, it is not necessary for the two parties to compute the shared exponentials.
- Oakley defines how the two parties can select group representation and operation for performing the Diffie-Hellman algorithm.
- Oakley has several options for key distribution. In addition to the classic Diffie-Hellman exchange, it can be used to derive a new key from an existing key and to distribute an externally derived key by encrypting it.
- Oakley permits the use of authentication based on symmetric encryption or non-encryption algorithms.
- Oakley supports various types of certificates such as PKCS #7 Certificates, PGP Certificates, DNS signed keys, Kerberos tokens, and X.509 Certificates.

If the two parties need to use a Diffie-Hellman key determination scheme that does not depend on the standard group definition, they have the option of establishing a private group. In order to maximize the security of the modular exponentiation group, one can take Sophie-Germaine primes, P = 2Q + 1, where P and Q are prime. While maintaining a reasonable degree of security, one can also choose a Schnorr subgroup generated by primes P and Q with P = kQ + 1, where k is small.

The description of the group is hidden from eavesdroppers, and the identifier assigned to the group is unique to the two parties. Such messages are encrypted. The two parties store the mapping between the group identifier and the group descriptor.

The only requirement for this protocol environment is that the underlying protocol stack must support the IP address of the remote party for each message. Theoretically, Oakley could be used directly over IP or UDP, if port number assignments were available. Actually, a conjunction between Oakley and ISAKMP is proposed [16]. The system running Oakley must provide a random number generator for nonce generation.

2.3 SKIP

SKIP is a key management scheme for session-less datagram oriented protocols such as IPv4 and IPv6. SKIP is suggested by A Aziz, T Markson, and H Prafullchandra in Sun Microsystems, Incorporated [6]. It stands for Simple Key-management for Internet Protocols.

SKIP is based on in-line keying. Each packet is encrypted in a key which is provided in the packet itself, encrypted in a key that is setup between communication peers.

SKIP uses authenticated Diffie-Hellman public values and each principal has this value. Let i and j be secret values of principals I and J, respectively,

and let $g^i \pmod p$ and $g^j \pmod p$ be public values of I and J, respectively. The shared secret $g^{ij} \pmod p$ is used as the basis for a key-encrypting key to provide IP packet based authentication and encryption. This value is called the long-term secret. The key for block cipher K_{ij} is derived from $g^{ij} \pmod p$ by taking the low order key-size bits of $g^{ij} \pmod p$. The minimal size of $g^{ij} \pmod p$ is 512 bits and the typical size of K_{ij} is within the range of 40–256 bits.

K_{ij} is used to encrypt a transient key K_p which is used as a key to encrypt/authenticate an IP packet. To keep K_{ij} for a relatively long period of time, the IP data traffic is not encrypted by K_{ij}. Since this key is used to encrypt only other keys, and not traffic, it is referred to as a master key.

In general, packets may be both encrypted and authenticated. Key separation is important when performing both encryption and authentication. Two separate keys named E_{K_p} and A_{K_p} are derived from K_p, that is, they are decrypted from the packet header. E_{K_p} and A_{K_p} are used as the encryption key and the authentication key, respectively. They are derived as follows:

$$E_{K_p} = h(K_p|\textit{Crypt Algorithm}|02\text{h}) \quad | \quad h(K_p|\textit{Crypt Algorithm}|00\text{h})$$
$$A_{K_p} = h(K_p|\textit{MAC Algorithm}|03\text{h}) \quad | \quad h(K_p|\textit{MAC Algorithm}|01\text{h})$$

where $h()$ is a pseudo-random, one-way hash function which is defined as the key separation part of the K_{ij} algorithm. As key-encryption algorithms (K_{ij} algorithms), there are three algorithms such as DES-CBC, 3-key Triple DES-CBC, and IDEA-CBC. As traffic encryption algorithms (*Crypt Algorithm*), there are two algorithms such as DES-CBC and 3-key Triple DES-CBC. As MAC algorithms (*MAC Algorithm*), 128-bit keyed MD5, DES-CBC MAC, and keyed SHA. The compression algorithms are reserved to IANA. Fig. 2 illustrates key generation flow in SKIP.

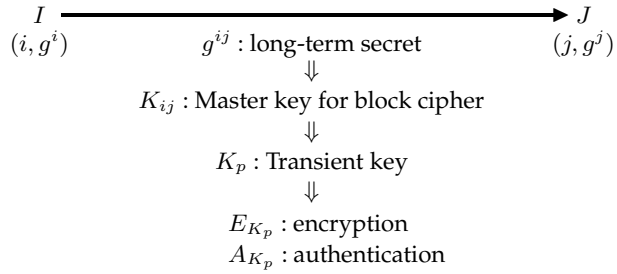

Fig. 2. Key Generation Flow in SKIP

To establish K_{ij}, a manual key agreement or a public key agreement can be used. A public key agreement system is defined as a system where one combines another's public value and one's own private value to compute a pairwise shared secret. It is distinguished from the public key cryptosystem with

the trapdoor. It is also specified by the algorithm identifier used to identify the public key in the certificate or by an equivalent mechanism such as a secure DNS.

An advantage of SKIP is that the protocol for setting up shared keys is lightweight. If both nodes already have the other nodes' public key certificate, no packet exchanges are required as the arriving data packet will contain sufficient information for the receiving node to compute the shared key and respond accordingly. Due to the lightwieght feature, SKIP will also likely be faster at recovery from normal system failure such as reboot when a host communicates with a significant number of peers.

There are some considerations for well-known attacks. Against middleperson attacks, SKIP uses authenticated Diffie-Hellman public values that includes a signature operation with principals' private keys. By use of a transient key and the master key, the security of SKIP against known/chosen key attacks depends on the security of the key encryption algorithm against known/chosen text attacks. In order to prevent denial-of-service attacks, the recommended solution by the proposers of SKIP is to pre-compute and cache the master key, based either on the usage pattern of the system or through administrative action. It is also recommended that the keys belonging to the administrator should be in the pre-computed cache used to prevent denial-of-service attack.

Several extensions for SKIP were suggested by the proposers of SKIP such as the extension for IP multicast [8], perfect forward secrecy [9], algorithm discovery protocol [7], encoding of an unsigned Diffie-Hellman public value [10], and X.509 encoding of Diffie-Hellman public values [11].

2.4 Photuris

Photuris is an experimental session-key management protocol intended for use with the IP security architecture such as AH and ESP. It is suggested by P Karn, WA Simpson of Qualcomm Inc. and DayDreamer, respectively.

It is designed for defense against resource clogging, perfect forward secrecy, and privacy protection of the exchange parties. It is primarily used for creating virtual private networks, establishing sessions for mobile users and networks operating over bandwidth-limited links, and short-lived sessions between numerous clients and servers.

Photuris is independent of any particular party identification method or certificate format. Support for symmetric key party identification is required to be implemented, and asymmetric key party identification is optionally supported by extensions.

The concept of "cookie" (anti-clogging token) is first introduced by the proposers of Photuris and, of course, cookie is adopted to Photuris against denial-of-service attacks.

2.5 SKEME

SKEME is a key exchange mechanism with scalability and flexibility. It is suggested by H Krawczyk of IBM TJ Watson Research Center. It is motivated by Photuris and evolved as an extension of the Modular Key Management Protocol (MKMP) [15].

It provides modes to perform fast and frequent key refreshment. The modes are as follows:

- basic mode which provides both public key based key exchange and perfect forward secrecy
- share only mode which provides public key based key exchange without performing the Diffie-Hellman algorithm
- pre-shared key mode which provides previously shared key based key exchange and perfect forward secrecy
- fast re-key mode based on symmetric key techniques only like MD5.

SKEME provides anonymity and allows repudiation of communication by avoiding the use of digital signatures. Like Photuris, it uses cookie against denial-of-service attacks.

2.6 AH

AH stands for the IP Authentication Header and is in the standards track of IETF as RFC 1826 [4]. It is proposed by R Atkinson of the Naval Research Laboratory.

The purpose of AH is to provide integrity and authentication for IP datagrams. Using asymmetric digital signature algorithm, AH can provide non-repudiation. Confidentiality and protection from traffic analysis are not provided by the AH.

AH is normally inserted after an IP header and before the other information being authenticated. Without changing the Internet infrastructure, the authentication data is carried in its own payload. Systems that are not participating in the authentication may ignore the authentication data.

The IP Authentication Header includes the Security Parameters Index (SPI) and Authentication data. RFC 1826 does not include a key management structure. The only coupling between key management protocol and AH is with the SPI. SPI is a 32-bit pseudo-random value identifying the security association for the datagram. Authentication data consists of a variable number of 32-bit words and is usually calculated using a message digest algorithm either by encrypting that message digest or by keying the messaged digest in directly.

In some cases a packet which causes an error to be reported back via ICMP might be so large as not to entirely fit within the ICMP message returned. In such cases, it might not be possible for the receiver of the ICMP message to authenticate independently the portion of the returned message. This could mean that the node receiving such an ICMP message would either trust an unauthenticated ICMP message, which might in turn create some security problem, or

not trust it and hence not react appropriately to some legitimate ICMP message required a reaction.

2.7 ESP

ESP stands for the IP Encapsulating Security Payload and is in the standards track of IETF as RFC 1826 [4]. It is proposed by R Atkinson of the Naval Research Laboratory.

ESP is a mechanism for providing integrity and confidentiality to IP datagrams. It may also provide authentication, depending on which algorithm and algorithm mode are used. Non-repudiation and protection from traffic analysis are not provided by ESP. This mechanism may be used to encrypt either a transport-layer segment (e.g., TCP, UDP, ICMP, IGMP) or an entire IP datagram. Encapsulating the protected data is necessary to provide confidentiality for the entire original datagram.

The Encapsulating Security Payload is structured somewhat differently from other IP payloads. The first component of the ESP payload consists of the unencrypted fields of the payload. The second component consists of encrypted data. The fields of the unencrypted ESP header inform the intended receiver how to properly decrypt and process the encrypted data. The encrypted data component includes protected fields for the security protocol and also the encrypted encapsulated IP datagram.

Furthermore, this specification does not have a specific key management protocol and the only coupling between key management mechanisms and ESP is the Security Parameter Index (SPI). The SPI is a 32-bit pseudo-random value identifying the security association for this datagram. The SPI is the only mandatory transform-independent field.

In the usage, the entire received datagram is authenticated, including both the encrypted and unencrypted portions, while only the data sent after the ESP header is confidential. In this usage, the sender first applies ESP to the data being protected. The other plaintext IP headers are then prepended to the ESP header and its now encrypted data. Finally, the IP Authentication Header is calculated over the resulting datagram according to the normal method. Upon receipt, the receiver first verifies the authenticity of the entire datagram using the normal IP Authentication Header process. Then if authentication succeeds, decryption using the normal IP ESP process occurs. If decryption is successful, then the resulting data is passed up to the upper layer.

There are some security considerations for ESP. Cryptographic transformations for ESP which use a block-chaining algorithm and lack a strong integrity mechanism are vulnerable to a cut-and-paste attack [12].

If user-oriented keying is not employed, then the algorithm in use should not be an algorithm vulnerable to any kind of chosen plaintext attack. Chosen plaintext attacks on DES are described in [13] and [22]. The use of user-oriented keying is recommended in order to become resilient to any sort of chosen plaintext attack and to make cryptanalysis more difficult.

3 Comparison

Basically, these algorithms are using the Diffie-Hellman key exchange protocol to support perfect forward secrecy. In the case of SKEME, users can take the mode which does not use the Diffie-Hellman key exchange mechanism if the perfect forward secrecy is not required.

All of them are using the AH and the ESP which are required in the RFC 1825 Security Architecture for the Internet Protocol. It is a treatment for obtaining basic integrity, confidentiality, and authentication.

All protocols support a protection mechanism against denial-of-service attacks. All of them but SKIP use an anti-clogging token "cookie". SKIP suggests a way to pre-compute and cache the master key.

SM Bellovin recommended moving towards the cryptographic processing towards the transport layer. Then for TCP, each new socket is mapped to new pair of SPIs, and for UDP, the binding must be between a socket and every destination node [12]. ISAKMP reflects this idea on it. When the socket is destroyed, all of its associated SPIs must be destroyed as well.

Consider compatibility between protocols. SKIP is in-band keying, where the session key is part of the packet. Both Photuris and Oakley are out-of-band keying, where an exchange takes place before data transmission. This difference in approach makes compatibility hard.

Table 1 shows brief comparison among five protocols described previously. In the case of SKEME, some data are not enough to compare to other protocols, because SKEME is not suggested as an Internet Draft. The stripe "–" means that there is no information. The symbols $\bigcirc$, $\triangle$, or $\times$ means that it is better, intermediate, or worse than others, respectively.

There are problems in descriptions of group generators for the Diffie-Hellman exponentiation. Photuris recommends 2 for the generator [17]. Oakley explains that the available range for the generator is $[2, p-2]$, where p is the modulo [24]. In the conjunction between ISAKMP and Oakley [16], the group with generator 2 is defined as Oakley default group. SKIP takes an example generator to be 2 [6]. Bleichenbacher's attack shows that signatures can be forged independently of the choice of modulo p when an implementor chooses 2 as the generator g of the group [14]. R Anderson recommends that p and g are chosen with care: implementors must check that $(p-1)/\gcd(r, p-1)$ is not too smooth, where $r = (p-1)/g \pmod{p}$, or must work in a subgroup of prime order [2].

With the sole exception of SKIP, they do not describe security in multicast communications explicitly. SKIP extension for IP multicast is proposed as an Internet Draft [8]. Under a multicast environment, the key management mechanism must negotiate a number of parameters for each security association and any other information. An important part of multicast key management is scalable re-keying, where the re-key operation needs to scale with the size of the multicast group and SKIP support in-line scalable re-keying.

There are two suggested multicast key management protocols. They are Group Key Management Protocol (GKMP) and Scalable Multicast Key Distribution. In the case of SKIP, the feature of one master key for a multicast group

Item	ISAKMP	Oakley	SKIP	Photuris	SKEME
Proposers	D Maughan et al.	HK Orman	A Aziz et al.	P Karn et al.	H Krawczyk
Proposed Organisation	National Security Agency & Terisa	University of Arizona	Sun Microsystems	Qulacomm & DayDreamer	IBM TJ Watson Research Center
Date of Latest Update	22.11.1996	5.1996	14.8.1996	6.1996	1996
Main Function	- SA - Key Mngmt	- Key Exchange - PFS	- Key Mngmt - Key Separation - Key Exchange - PFS	- Session-key Mngmt -PFS	- Key Exchange - PFS
Considered Attacks	- Middleperson attack - Connection Hijacking - Clogging	- Clogging	- Middleperson attack - Known-key Attack - Clogging	- Clogging	- Clogging
Mechanism against Clogging	- Pre-computed and cached master key	- Cookie	- Cookie	- Cookie	- Cookie
Interoperability	Oakley	ISAKMP	–	–	–
Multicast support	△	△	○	–	–
Compatibility	○	△	△	△	–
Future Support	○	○	○	×	–
No. of Related Drafts	3	1	5	1	–
Transport Layer (Port No.)	UDP (500)	TCP/UDP	TCP/UDP	UDP (468)	–

Table 1. Comparison between protocols

can be a problem for GKMP. Actually, IP multicast is an unreliable operation. There can be no assurance that all the group members in fact have received the new traffic key. This remains a subject for further study and several studies on multicast key management are underway.

In IETF IPSEC WG meeting in Montreal in June 1996, J Gilmore announced that there is no new draft available addressing the previously discussed deficiencies of Photuris. There was no evidence of broad support for Photuris at that meeting.

The IPSEC interoperability test which is sponsoring by RSA's S/WAN Initiative has been started. The participants are in two groups, each supporting a key management protocol - ISAKMP/Oakley and SKIP. A third group using manual key management is also participating. Currently, SKIP processed more tests for various products than ISAKMP/Oakley.

4 Analysis

ISAKMP is a well-designed general key management framework for IP security that supports Security Association. Each socket connection can be controlled by

the associated SPIs. SKIP has also preferable features. It works well in applications that are well-suited to UDP like network management, multicast protocols, or DNS. But SKIP does not operate in a model that permits multiple associations between two nodes. It is needed if there are mutually suspicious users on different transport connections. The preferable SKIP functionalities would be considered within the ISAKMP framework.

In the IPSEC mailing list, J Schiller, the Security Area Director of the IPSEC Charter, recommended that ISAKMP with Oakley should be the the mandatory implement standard for key management and that SKIP would be an elective standard for it.

By our comparison among these protocols, ISAKMP can be also the best candidate for the Internet security key management infrastructure with key exchange protocol Oakley. These protocols are well-designed protocol suites, but there are some problems in them. Some comments on them are suggested in this section.

In ISAKMP, the Certification Authority (CA) is identified by two octets. The implies that ISAKMP admits a maximum of 64K CAs in the world. This number is not enough for CAs in the world. The United Kingdom Healthcare sector alone will consume about a fifth of this resource; there are some 12,000 healthcare providers (hospitals, primary care practices, and so on) each of which will certify the keys of its own staffs.

In general, we would expect that even three octets would be inadequate for CAs. If each employer certifies its employees, and each merchant certifies keys supplied to or by its customers like the case of SET [19–21], then four octets will be required even with a completely compressed namespace. But there will likely be sound performance reasons for not waiting this space to be densely packed. So this field should be of variable length.

Similarly, the use of a 32-bit sensitivity label and a 256-bit compartment bitmap may be adequate for the US DoD but is unlikely to be sufficient for commercial and professional applications. In the medical field, for example, the British Medical Association (BMA) security policy [1] may assume the role played in the DoD by Bell LaPadula. There, security associations involve access control lists that will typically contain a list of names of clinical professionals (doctors, nurses, pharmacists, and so on) who are authorised to read and append to a particular object.

Given the volatility of staff in the hospital sector in particular, the number of possible access control lists could become very large over time. Thus for performance reasons it would be inconvenient to have to use some central service to map them to compartment bitmaps. It would be much preferable to include these lists explicitly.

Similar considerations apply in commerce; whether or not systems explicitly instantiate the Clark-Wilson model, they can contain large quantities of protection state and astronomically large numbers of valid access combinations (e.g., under separation of duty policies). Expressing such policies compactly and efficiently in distributed systems requires more structure than a simple 256 bit

integer. For these reasons, the security label, access control list or capability should be a variable length field.

ISAKMP also specified only four bits to identify version number. If it is successful and is used widely, it will persist for many decades and it will be required to support many kinds of functionality. Then 16 versions are not enough for this protocol.

We observe that the Labeled Internet Domain of Interpretation has not yet been developed in much detail and assume that this is because it is still rather tentative. Hopefully, non-military policies such as Clark-Wilson and the BMA policy can be supported before it becomes cast in stone. That way, ISAKMP will be able to meet its goal of supporting the establishment of security associations for all possible security protocols and applications, not just military ones.

In Oakley, it would be nice to have key separation between send and receive keys, for the sake of applications that use MACs together with some kind of tamper resistance to secure remote control (e.g., of telephone exchanges and prepayment electricity token dispensers).

It is a rather bad idea to include a claim for the strength of a given group. There is no real agreement on how strong various large moduli are. For example, P Leyland considers that a 700-bit modulus corresponds to about 75-80 bits of security, while Oakley requires 2000-bit moduli with 90-bit shared keys. The claim for the strength of a group is not necessary.

Some guidelines on the use of pseudorandom number generators would be a good idea (the provisions attached to DSA resulted from previous nagging from us). In particular, it should be impossible to get the same pseudorandom number twice unless either (a) the messages, security context etc are the same; or (b) a collision is found in a hash function such as SHA. It is quite easy to ensure this and still make good use of any real environmental randomness that might be present.

5 Summary

We have described a brief survey of key management protocols for IP layer which are, with exception of SKEME, being suggested to the IETF IPSEC Working Group as an Internet Draft. We made a comparison between them and found their weak points and potential implementation problems. We also suggested resolutions to these problems. We recommended that ISAKMP with Oakley is the best choice for key management protocol among these protocols.

References

1. RJ Anderson, "An Update on the BMA Security Policy" in *Workshop on Personal Information*, 1996
2. RJ Anderson and S Vaudenay, "Minding your p's and q's" in *Advances in Cryptology – ASIACRYPT '96* (1996, to appear)

3. R Atkinson, "Security Architecture for the Internet Protocol", RFC 1825, Internet Engineering Task Force, August 1995
4. R Atkinson, "IP Authentication Header", RFC 1826, Internet Engineering Task Force, August 1995
5. R Atkinson, "IP Encapsulating Security Payload", RFC 1827, Internet Engineering Task Force, August 1995
6. A Aziz, T Markson, and H Prafullchandra, "Simple Key-Management For Internet Protocols (SKIP)", Internet-Draft, IPSEC WG (14 August 1996)
   `File: draft-ietf-ipsec-skip-07.txt`
7. A Aziz, T Markson, and H Prafullchandra, "SKIP Algorithm Discovery Protocol", Internet-Draft, IPSEC WG (5 August 1996)
   `File: draft-ietf-ipsec-skip-adp-01.txt`
8. A Aziz, T Markson, and H Prafullchandra, "SKIP Extensions for IP Multicast", Internet-Draft, IPSEC WG (5 August 1996)
   `File: draft-ietf-ipsec-skip-mc-01.txt`
9. A Aziz, T Markson, and H Prafullchandra, "SKIP Extensions for Perfect Forward Secrecy", Internet-Draft, IPSEC WG (5 August 1996)
   `File: draft-ietf-ipsec-skip-pfs-01.txt`
10. A Aziz, T Markson, and H Prafullchandra, "Encoding of an Unsigned Diffie-Hellman Public Value", Internet-Draft, IPSEC WG (5 August 1996)
    `File: draft-ietf-ipsec-skip-udh-01.txt`
11. A Aziz, T Markson, and H Prafullchandra, "X.509 Encoding of Diffie-Hellman Public Value", Internet-Draft, IPSEC WG (5 August 1996)
    `File: draft-ietf-ipsec-skip-x509-01.txt`
12. SM Bellovin, "Problem Areas for the IP Security Protocols" in *Proceedings of the 6th USENIX Security Symposium*, USENIX Association (1996) pp 205–214
13. E Biham and A Shamir, "*Differential Cryptanalysis of the Data Encryption Standard*", Springer-Verlag, New York, 1993.
14. D Bleichenbacher, "Generating ElGamal Signatures Without Knowing the Secret Key" in *Advances in Cryptology – EUROCRYPT '96*, Springer LNCS **1070** (1996) pp 10–18
15. P Cheng, J Garay, A Herzberg, and H Krawczyk, "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX" in *Proceedings of the 5th USENIX Security Symposium*, USENIX Association (1995) pp 41–54
16. D Harkins and D Carrel, "The Resolution of ISAKMP with Oakley", Internet-Draft, IPSEC WG (November 1996)
    `File: draft-ietf-ipsec-isakmp-oakley-01.txt`
17. P Karn and WA Simpson, "The Photuris Session Key Management Protocol", Internet-Draft, IPSEC WG (June 1996)
    `File: draft-ietf-ipsec-photuris-11.txt`
18. H Krawczyk, "SKEME: A Versatile Secure Key Exchange Mechanism for Internet" in *Proceedings of SNDSS '96*, IEEE (1996) pp 114–127
19. MasterCard International and VISA International, *Secure Electronic Transaction Specification, Book1: Business Description*, 1996
20. MasterCard International and VISA International, 1996 *Secure Electronic Transaction Specification, Book2: Programmer's Guide*, 1996
21. MasterCard International and VISA International, 1996 *Secure Electronic Transaction Specification, Book3: Formal Protocol Definition*, 1996
22. M Matsui, "Linear Cryptanalysis Method for DES Cipher" in *Advances in Cryptology – EUROCRYPT '93*, Springer LNCS **765** (1994) pp 386–397

23. D Maughan, B Patrick, and M Schertler, "Internet Security Association and Key Management Protocol (ISAKMP)", Internet-Draft, IPSEC WG (22 November 1996)
`File: draft-ietf-ipsec-isakmp-06.txt`
24. HK Orman, "The OAKLEY Key Determination Protocol", Internet-Draft, IPSEC WG (May 1996)
`File: draft-ietf-ipsec-oakley-01.txt`
25. D Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", Internet-Draft, IPSEC WG (November 1996)
`File: draft-ietf-ipsec-ipsec-doi-01.txt`
26. W Sommerfeld, "Inline Keying within the ISAKMP Framework", Internet-Draft, IPSEC WG (November 1996)
`File: draft-ietf-ipsec-inline-isakmp-00.txt`