
Nürnberg, 25.06.2004

GSO FH Nürnberg,
Fachrichtung Informatik,
FWPF Internet Security bei Prof. Dr. P. Trommler

ISAKMP / RFC 2408 summarized by Josip Istuk

---

1. Introduction

1.1 What is ISAKMP ?

ISAKMP is an acronym for Internet Security Association and Key Management Protocol. ISAKMP utilize security concepts necessary for establishing Security Associations and cryptographic keys in Internet environment by negotiating, establishing, modifying and deleting Security Associations and their attributes.
ISAKMP defines procedures, packet formats to negotiate, modify and delete Security Associations. It defines payloads for exchanging key generation and authentication data.
It's distinct from key exchange protocols in order to cleanly separate the details of Security Association management from the details of key exchange and serves as a common framework for agreeing to format of Security Association attributes.

1.2 Considering the pros and cons of ISAKMP

The separation - for example into Security Association management and details of key exchange or the separation into negotiating, modifying and deleting Security Associations - adds complexity.
This separation is critical for interoperability between systems with differing security requirements. Also it simplifies analysis of an ISAKMP server.
ISAKMP reduces the amount of duplicate functionality by centralizing the Security Association management and it can reduce connection setup time negotiating many Security Associations at once.

1.3 Security Association and Management

There are many VPNs and Intranets, which are geographically separated and have to interact between each other. Many of them have to interact with customers, suppliers, government and others. And each time something has to be negotiated. ISAKMP is not bound to any specific cryptographic algorithm, key generation technique, or security mechanism. So it's possible to negotiate different encryption algorithms, authentication mechanisms, and key establishment algorithms. ISAKMP provides the protocol

exchanges to establish a Security Association between negotiating entities followed by the establishment of a security association. The initial exchange provides a set of security attributes which allows protection for subsequent ISAKMP exchanges. Also it indicates the authentication method and key exchange of the further protocol. If the basic set is already negotiated the initial exchange may be skipped.

1.4 Authentication

Many authentication mechanisms are available. Strong authentication MUST be provided and a digital signature algorithm MUST be used on ISAKMP exchanges. Week authentication mechanisms are optional. Sending clear text or one-way hashed poorly-chosen keys with low entropy is week. Examples for strong authentication mechanisms are Digital Signature Standard (DSS) or RSA. Authentication based on digital signatures requires a trusted third party and for each entity a public and a private key. If the entity on the other end can't be authenticated, the Security Association is suspect and you are unable to trust it. A trusted third party is a Certificate Authority. A Certificate Authority provides an infrastructure for generation, verification, revocation, management and distribution for Certificates. The Internet Policy Registration Authority (IPRA) certifies Policy Certificate Authorities. However, ISAKMP is not bound to a specific signature algorithm or a specific certificate authority or specific certificate types. Although ISAKMP utilizes digital signatures, based on public key cryptography, there are other strong authentication systems which can be specified. This are systems rely on a trusted third party called a key distribution center (KDC), e.g. Kerberos, to distribute secret session keys.

1.5 ISAKMP Protection against denial of service

ISAKMP provides a "cookie" or an anti- clogging token (ACT) to make it easier to handle denial of service and prevents connection hijacking by linking the authentication, key exchange and Security Association exchanges. Absolute protection against denial of service is impossible.

1.6 Man-in-the-Middle Attack prevention

Man-in-the-Middle Attack prevention means prevention against interception, insertion, deletion and modification of messages, reflecting messages back at the sender, replaying old messages and redirecting messages. The linking of ISAKMP exchanges prevents the insertion of messages. The protocol state machine definition prevents that deleted messages will cause a partial Security Association to be created. Instead the state machine will clear all state and return to idle. A possible harm by reflected massages is also preventing by the state machine. Cookies make it impossible to harm an entity by replaying old messages. With ISAKMP strong Authentication the entity on the other end can't be anyone other then the intended one.

2. ISAKMP Terminology

2.1 ISAKMP Placement

The Figure 1 from the RFC 2408 shows a high level view of the placement:
The ISAKMP is an application layer protocol with a defined access to the IP layer. The Definition of the Domain of Interpretation (DOI) and the Definition of Key Exchange is clearly separated from other parts of the protocol.

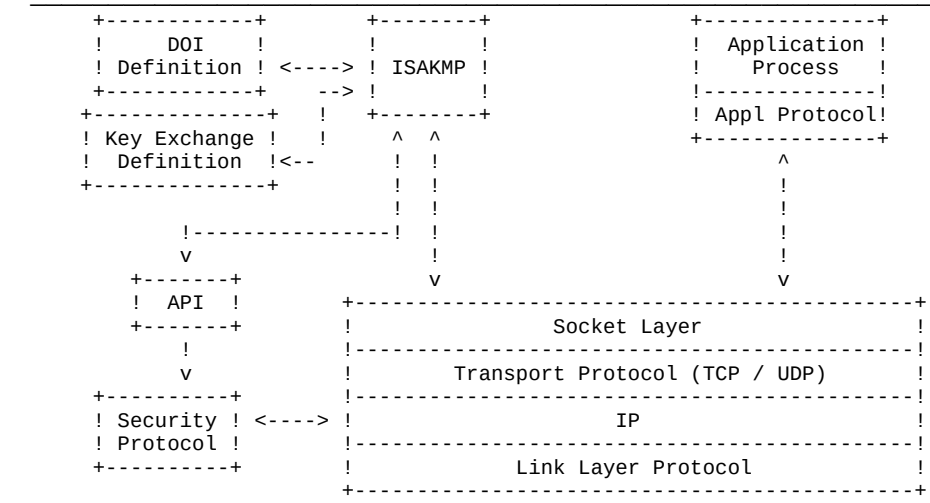

Figure 1: ISAKMP Relationships

2.2 Negotiation Phases

How mentioned above, ISAKMP offers two phases of negotiation. In the first phase entities decide on how to protect further negotiations. The second phase establishes Security Association for other security protocols. Also it can be used to establish many Security Associations.

2.3 Identifying Security Associations

ISAKMP uses cookie fields in its header to identify Security Associations. Other security protocols use the Message ID field and the SPI field in the ISAKMP Header to identify Security Associations during the Security Association establishment. Interpretation of these fields depends on the operation taking place. For interpretation of the Security Associations during various operations the following fields are necessary to be set:

#	Operation	I-Cookie	R-Cookie	Message ID	SPI
(1)	Start ISAKMP SA negotiation	X	0	0	0
(2)	Respond ISAKMP SA negotiation	X	X	0	0
(3)	Init other SA negotiation	X	X	X	X
(4)	Respond other SA negotiation	X	X	X	X
(5)	Other (KE, ID, etc.)	X	X	X/0	NA
(6)	Security Protocol (ESP, AH)	NA	NA	NA	X

The initiator includes the Initiator Cookie in the ISAKMP Header. The responder includes the Initiator and the Responder Cookie fields in the Header. After first phase all subsequent communications between entities include these two cookies. Third line represents the initiator using a Message ID and the Security Parameter Index (SPI). The fourth line shows what other responds on Security Association negotiation have to do. For more Details how to identify the Security Associations please have a look into the RFC 2408.

2.4 Implementations

ISAKMP can be implemented over IP or any other transport protocol. Implementations MUST include send and receive capability for ISAKMP using UDP on port 500. UDP Port 500 has been assigned to ISAKMP by the Internet Assigned Numbers Authority. RESERVED Fields within ISAKMP payloads are used strictly to preserve byte alignment and MUST be set to zero when a packet is issued. If not the receiver SHOULD discard the packet. The generation of cookies is implementation dependent. But same basic requirements MUST be satisfied. For more Details see the RFC 2408, section 2.5.3.

3. ISAKMP Payloads

3.1 ISAKMP Header Format

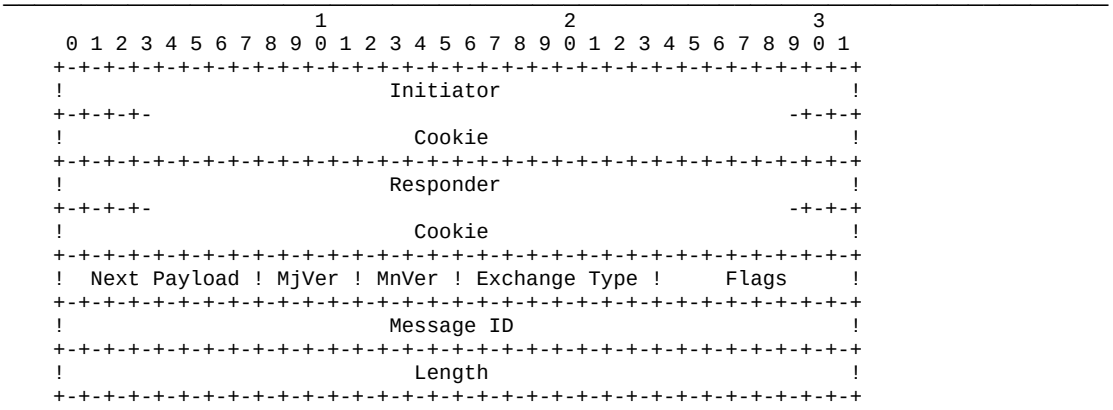

Figure 2: ISAKMP Header Format

The Initiator Cookie, which is 8 octets long, initiate Security Association establishment, Security Association notification, or Security Association deletion. The Responder Cookie, which is 8 octets long too, is responding to a Security Association establishment request, Security Association notification, or Security Association deletion. The "Next Payload" field indicates the type of the first payload in the message. The format for following payloads is defined in the "Generic Payload Header". Here are the possible values of this field:

Next Payload Type	Value
NONE	0
Security Association (SA)	1
Proposal (P)	2
Transform (T)	3
Key Exchange (KE)	4
Identification (ID)	5
Certificate (CERT)	6
Certificate Request (CR)	7
Hash (HASH)	8
Signature (SIG)	9
Nonce (NONCE)	10
Notification (N)	11
Delete (D)	12
Vendor ID (VID)	13
RESERVED	14 - 127
Private USE	128 - 255

The Major and Minor Version fields indicate the version of the used protocol. Implementations based on versions of a lower number SHOULD decline packets from an entity with a higher version number. First it should be compared the Major and then the Minor number. If the Major Versions are equal but the Minor version numbers are not, the entity with the lower protocol number SHOULD not accept the packets from the other entity. The Exchange Type, which is one octet long, indicates the type of exchange being used. These are the possible exchange types:
NONE, Base, Identity Protection, Authentication Only, Aggressive, Informational
Some are reserved for future ISAKMP use. It's possible to define Exchange Types with the Domain of Interpretation. Last, there are some reserved for private use:

Exchange Type	Value
NONE	0
Base	1
Identity Protection	2
Authentication Only	3
Aggressive	4
Informational	5
ISAKMP Future Use	6 - 31
DOI Specific Use	32 - 239
Private Use	240 - 255

The Flags indicates specific options for the transmission. Beginning with the least significant bit, the bit 0 is the Encryption Bit. If it's set to 1, all data following the header is encrypted. The bit 1 is the Commit Bit. It's used for signal key exchange synchronization to ensure that encrypted material is not reserved earlier then the Security Associations are established. The Authentication Only Bit is the bit 2 and allows an integrity checking with a Notify payload but without encryption. The remaining bits of the Flags field MUST be set to 0 before transmitting. The Message ID, which is 4 octets long, is a unique ID used to identify protocol state during Phase 2 negotiations. This value is randomly generated by the initiator entity. The Length field of the ISAKMP header shows the total length of the message and the header together in octets.

3.2 Generic Payload Header

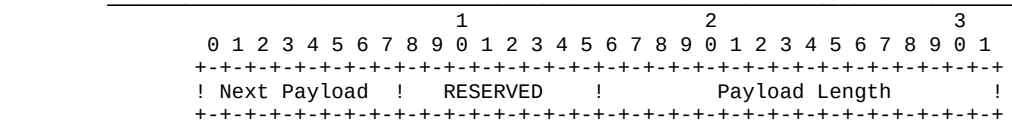

Figure 3: Generic Payload Header

The Next Payload field, which is 1 octet long, is an Identifier for the payload type of the next payload in the message. If the field is set to 0, the current payload is same as in the last message. The Payload Length, which is 2 octets long, gives the length in octets of the current payload, including the generic payload header. The RESERVED bits are unused and to be set to 0.

3.3 Data Attributes

These Data Attributes are not an ISAKMP payload, but are contained within ISAKMP payloads for example the Transform Payload. The length of the Data Attributes can either be 4 octets or defined by the Attribute Length field. This flexibility decreases the amount of overhead.

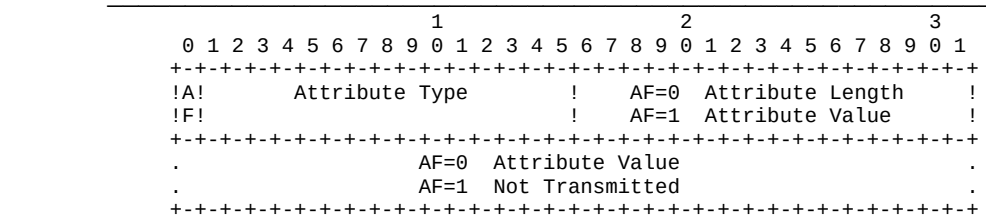

Figure 4: Data Attributes

If the AF Flag is set to 1, the Attribute Length is 4 octets and the Attribute Value is in the last two octets.

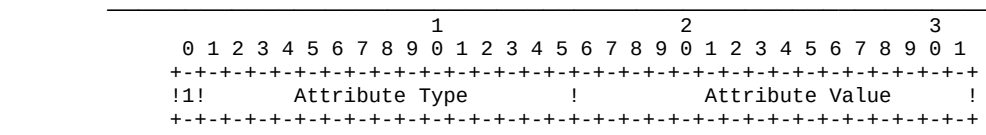

Figure 5: Data Attributes, bit 1 is 1

If the AF Flag is set to 0, the Attribute Length has to be in the octet 3 and 4. The Attribute Value begins with the 5th octet and its length is variable:

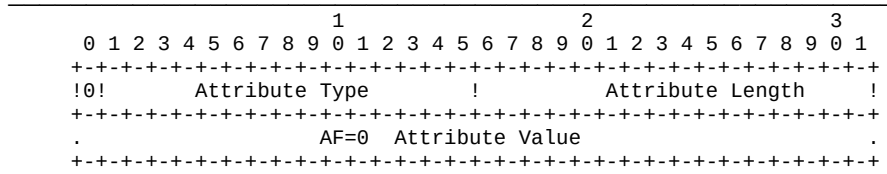

Figure 6: Data Attributes, bit 1 is 0

3.4 Security Association Payload

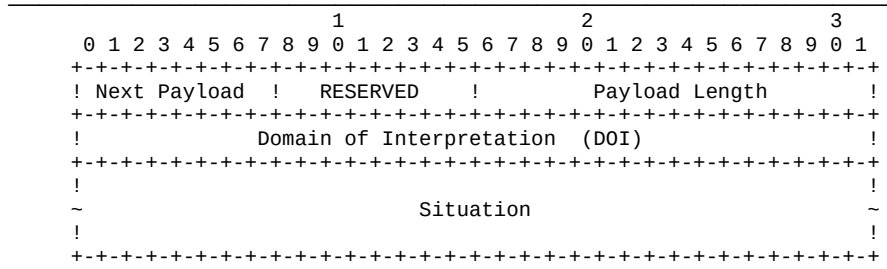

Figure 7: Security Association Payload

The DOI field identifies the specific DOI. The Situation field is a DOI specific field.

3.5 Proposal Payload

The Proposal Payload contains a proposal what security mechanisms, or transforms, to be used to secure further communications:

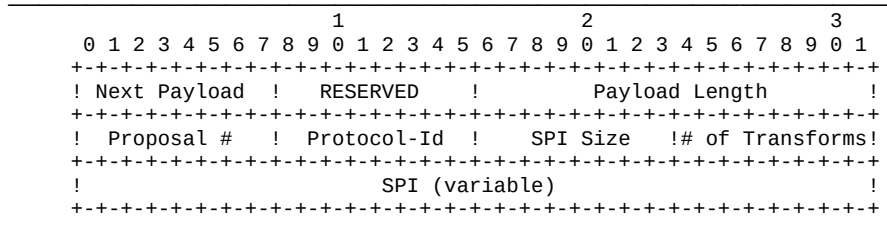

Figure 8: Proposal Payload Format

There are some further payloads:
- Transform Payload
- Key Exchange Payload
- Identification Payload
- Certificate Payload
- Certificate Request Payload
- Hash Payload

- Signature Payload
- Nonce Payload
- Notification Payload
- Delete Payload
- Vendor ID Payload

For more details see the RFC 2408.

4. ISAKMP Exchanges

4.1 Exchange Types

The following pages describe the procedures for Security Association establishment and modification. There are five defaults Exchange Types defined. These exchanges define the content and ordering of massages. Most of them will be composed with these basic types. The ordering of the messages and of their payload is the primary difference between exchange types. If the defined exchanges do not satisfy some application requirements, the needed exchange types have to be defined with the DOI.

4.2 Security Association Establishment

To build messages for the Security Association negotiation and establishment the Security Association, Proposal and Transform payloads are used. The Proposal and Transform payloads will be only used during Security Association establishment and negotiation. With the Proposal payload the initiating entity negotiate the security mechanisms with the responding entity. There is a possibility to combine multiple protocols to protect the communications. If is intended to use more then one protocol together, this Proposals MUST have the same number. If it's meant to use one security mechanism or another, the Proposal numbers have to monotonically increase for each alternative. With this mechanism a logical AND / OR is realized. With the Transform payload the initiating entity have a possibility to negotiate multiple mechanisms or transforms for a given protocol. The Proposal payload identifies the Protocol to be used. With the Transform payload the initiating entity presents several possible supported transforms. A single transform MUST be selected by the receiving entity. Otherwise the entire proposal MUST be reject.

4.3 Security Association Establishment Example

In the example there is a Proposal for a combined protection suite with two different protocols. The first protocol is presented with two transforms supported by the proposer. The second protocol has a single transform.

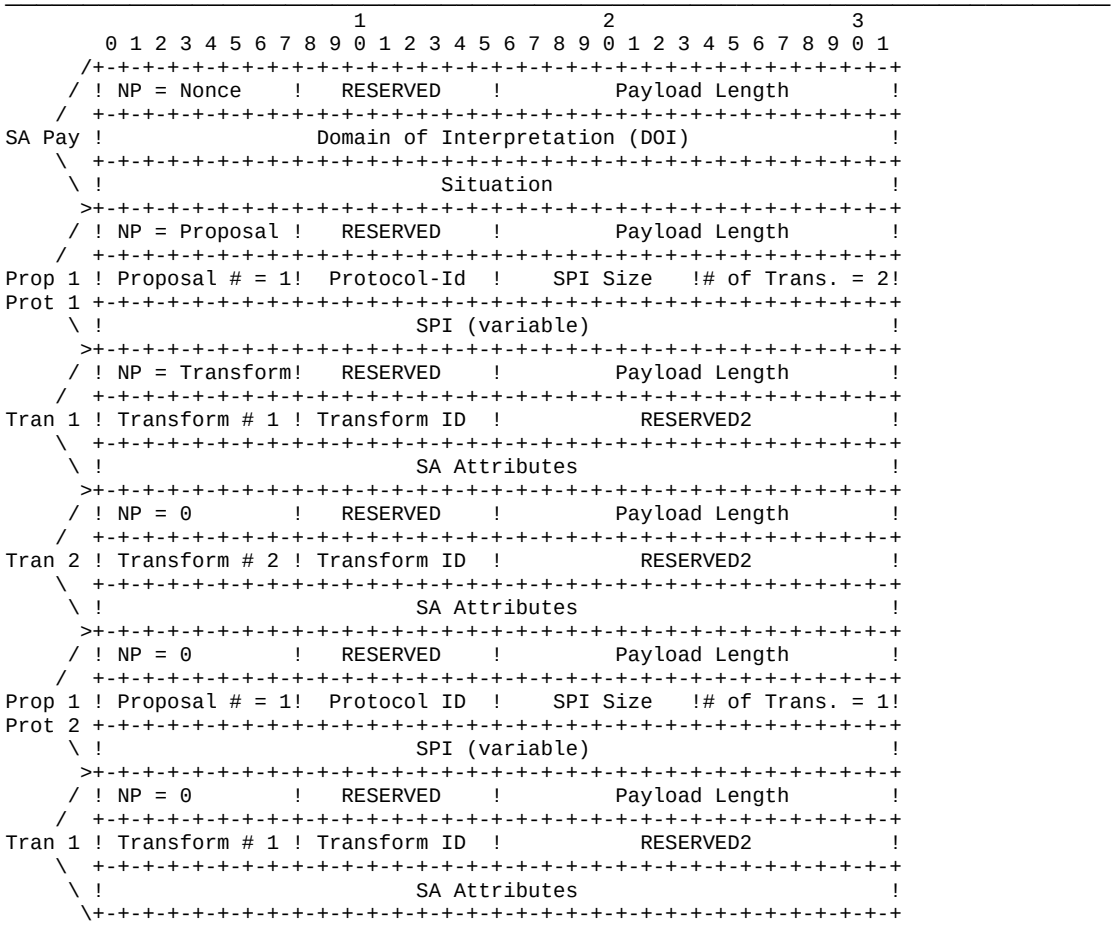

Figure 8: Security Association Establishment Example

4.4 Security Association Modification

The Security Association Modification is accomplished by creating a new Security Association and then deleting the old one. The Deletion of the old Security Association can be done anytime after the new Security Association is established. This proceeding avoids a situation where Security Association attributes do not exist. Potential vulnerabilities in synchronizing modification of existing Security Association attributes will not appear.

4.5 Other ISAKMP Exchanges

The Base Exchange allows transmitting Key Exchange and Authentication related information together but without protection and encryption. The Identity Protection Exchange allows separating the Key Exchange information from the Identity and Authentication related information. So at the expense of two additional messages the communicating identities are protected. The Authentication Only Exchange allows transmitting only Authentication related information without being encrypted and so

without the expense of computing keys. However it may be that the communication is already protected for example by the first phase of negotiations. The Aggressive Exchange is designed to allow combining the Security Association, Key Exchange and Authentication-related information into one message. This processing reduces the number of round-trips at the expense of unprotected identities. But the identities may be already exchanged before. The Informational Exchange is a one-way transmit ion that can be used for security association management. For further information on ISAKMP Exchanges please consult the RFC 2408.

5. ISAKMP Payload Processing

5.1 Processing with payloads

In the following section it is described how to process with the described payloads and exchanges. In order to provide the possibility to analyze the communications all events should be logged to a system audit file. The basic processing provides protocol reliability, minimizes threats and prevents so such as denial of service and replay attacks.

5.2 General Message Processing

Generally all processing SHOULD check if the packet length is the same as the length of the received packet. If it's not the same the message MUST be rejected and the receiving entity MUST do some actions:
The event "UNEQUAL PAYLOAD LENGTHS" MAY be logged in the appropriate system audit file. An Informal Exchange with this event back MAY be sent back. Generally when an entity is transmitting an ISAKMP message, following actions MUST be done:
A timer has to be set and a retry counter to be initialized. If the timer expires, the ISAKMP message is resent and the retry counter is decremented. If the retry counter reaches zero, the event, RETRY LIMIT REACHED, MAY be logged in the appropriate system audit file. The protocol machine clears all states and returns to IDLE.

5.3 ISAKMP Header Processing

When creating a message following actions MUST be done:
Create the respective cookie, determine the relevant security characteristics of the session, construct the ISAKMP Header fields and payloads and transmit the message. When receiving a message you MUST verify the Initiator and Responder cookies. If the cookie validation fails, the message must be discarded and the event INVALID COOKIE MAY be logged and an Informational Exchange about this MAY be sent to the transmitting entity. You MUST check the fields Next Payload, Versions, Exchange Types, Flags, Message ID and each time if validation fails it MAY be logged the suitable event and MAY be sent a suitable Informational Exchange. After this the processing of the ISAKMP message continues using the value in the Next Payload field.

5.4 Generic Payload Header Processing

When ever creating one of the described ISAKMP Payloads the Generic Payload Header is placed at the beginning. Then you MUST place the value of the Next Payload, the zero in the RESERVED field, and the Payload Length field.
When receiving a Generic Payload Header, you MUST prove the Next Payload field, the RESERVED and the Next Payload. If a validation fails, a suitable event MAY be logged and a suitable Informational Exchange message MAY be sent.

5.5 Other Processing

There are some further processing described in the RFC 2408 which are very similar built:
Security Association Payload Processing
Proposal Payload Processing
Transform Payload Processing
Key Exchange Payload Processing
Identification Payload Processing
Certificate Payload Processing
Certificate Request Payload Processing
Hash Payload Processing
Signature Payload Processing
Nonce Payload Processing
Notification Payload Processing
Delete Payload Processing

6. My Conclusions

ISAKMP is a well designed protocol aimed at the Internet of the future. The massive growth of the Internet will lead to great diversity in network utilization, communications, security requirements, and security mechanisms. ISAKMP contains all the features that will be needed for this dynamic and expanding communications environment.
Sometimes the benefits are achieved for the expense of additional communication or additional processing or additional threats.