Internet Security Association and Key Management Protocol

(ISAKMP)

draft-nsa-isakmp-01.txt, .ps

Mark Schertler
INFOSEC Computer Science Division
National Security Agency

phone: (301) 688-0850
email: mjs@tycho.ncsc.mil

REQUIREMENTS

- Flexible KMP Architecture

  Mechanism Independence
  - Key Exchanges
  - Authentication Mechanisms
  - Encryption Algorithms

  Security Attribute Negotiation

  Migration Path For Future Security Developments

- Base Key Exchange for Interoperability
- Utilize Current Networking Infrastructure
  - IP Based Networks (Internet, Clover)
- Utilize Commercial Products With Subsequent Security Functionality

ISAKMP FEATURES

- Fixed Field Header
  Replay Prevention
  - Time Variant Cookie

  Good Protocol & Software Engineering Practice

- Initialization - Selectable ISAKMP Protection
  - Authentication Mechanism
  - Key Exchange Algorithm
  - Encryption Algorithm

- Authentication and Key Establishment
  Key Exchange Algorithm Independent
  Strong Authentication Mechanism Required
  - Multiple Certificate Authority Support

ISAKMP FEATURES (Continued)

- Security Association Establishment
  Independent Protocol Definition and Security Attribute Definition
  Bundling of Attribute Definitions
  - SA Set
  - Attribute List

  Extendable Attribute Definition
  - examples: Compression, MTU

  Upgrade Current Security Association

- Discrete Payloads
  Separate Protocol Information by Function
  Good Protocol & Software Engineering Practice

- Transport Non-Reliance
  Unaffected By Transport Vulnerabilities
  Good Security, Protocol & Software Engineering Practice

GENERAL PACKET FORMAT

```
                    1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Message Type  |   Exchange    |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              SPI                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                        Initiator Cookie                       |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                        Responder Cookie                       |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                            Payload                            |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```


GENERAL PACKET FORMAT (continued)

- Security Parameter Index (SPI) - Indicates security association being created. A Security Association indicates the algorithms and mechanisms used for subsequent data transfer protection.
- Message Type - Identifies contents of ISAKMP Payload Field and provide ISAKMP message sequencing.
- Exchange - Identifies type of exchange being preformed
- Length - Payload length in octets
- Payload - Field contents identified by message type. There is a unique payload format for each function (authentication, key exchange, security association)

ISAKMP MESSAGE TYPES

- **ISA_INIT** - Initial exchange to present basic security attributes.
- **ISA_AUTH&KE** - Exchanges authentication and key information.
- **ISA_AUTH** - Exchanges authentication information only.
- **ISA_KE** - Exchanges key information only.
- **ISA_NEG** - Performs security attributes presentation and agreement exchange.
- **ISA_COMMIT** - Performs optional commit so initiator and responder can synchronize local establishment of SA before beginning secure communication.

ISAKMP MESSAGE TYPES (continued)

- **ISA_MODIFY** - Performs updating of an SA.
- **ISA_DELETE** - Informational function to inform remote entity that an SA has been deleted.
- **ISA_NOTIFY** - Supports exchange of information not directly related to the SA, but used to manage, activate, deactivate or support security services. Error Messages are an example.

ISAKMP PAYLOADS

- Discrete Payloads For Each Security Mechanism
  Authentication Payload
  Key Exchange Payload
  Security Association Payload
- Payloads (1 or more) Follow ISAKMP Header

SECURITY ASSOCIATION PAYLOAD FORMAT

```
                    1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| SA Syntax Type|   SA Flags    |  Payload Length or Num of Sets  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                         SA Attributes                         |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- SA Syntax Type - Defines Security Attributes representation (Lists or Sets)
- SA Flags - Control Bits to indicate the next ISAKMP packet transferred.
- SA Attributes - Security Attributes represented as Lists or Sets.

SECURITY ATTRIBUTES

- Security Attribute Transfer Format
  List:
  - Each attribute required to create a Security Association (SA) and all options for each attribute.

  Set:
  - Complete Security Association.
- Security Association and Security Attribute Registration
  Internet Assigned Number Authority (IANA)
  - SMI Security Codes

SA SET FORMAT

```
                    1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Set Number   |            Supports           | Num of Attrs  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Attribute Class        |         Attribute Type          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Attribute Class        |         Attribute Type          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Set Number - Unique Identifier for each proposed set.
- Supports - Security Service Supported. Examples - IP AH, IP ESP
- Num of Attrs - Number of attributes in proposed set.
- Attribute Class - Examples: Encryption Algorithm, Hash Algorithm
- Attribute Type - Examples: Encryption Algorithm: DES, IDEA, 3DES

SA LIST FORMAT

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Attribute Class         |             Count             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Attribute Type         |         Attribute Type        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Attribute Type         |         Attribute Type        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Attribute Class - Examples: Encryption Algorithm, Hash Algorithm.
- Count - Number of proposed type for a class.
- Attribute Type - Examples for Encryption Algorithm are DES, IDEA, Triple DES.

IP SECURITY ASSOCIATION ATTRIBUTES

Security Association Attributes defined in Security Architecture for IP

- Authentication Header (AH)

Authentication Algorithm	Required for AH
Authentication Mode	Required for AH
Authentication Key(s)	Required for AH
- Lifetime	Recommended for All

- Encapsulating Security Payload (ESP)

Encryption Algorithm	Required for ESP
Encryption Mode	Required for ESP
Encryption Transform	Required for ESP
Encryption Key(s)	Required for ESP
- Lifetime	Recommended for All

IP SECURITY ASSOCIATION ATTRIBUTES (cont.)

- Encapsulating Security Payload (ESP) (continued)

IV or Cryptographic Synchronization	Required for ESP
- Present / Absence	
- Size	
Authentication Algorithm	Recommended for ESP
Authentication Mode	Recommended for ESP
Authentication Key(s)	Recommended for ESP
- Lifetime	Recommended for All

• SA Lifetime	Recommended for All
• Sensitivity Level	Required for All MLS Systems
•	Recommended for All Other systems

IP AUTHENTICATION

- IP Keying Requirements - Security Architecture of IP
  User-Oriented Keying
  Host-Oriented Keying
- Require two levels of authentication / certificates
  Host Certificates
  User Certificates

IP AUTHENTICATION (continued)

- Certification Authorities
  - DNS Servers with Eastlake/Kaufman Security Extensions
  - PEM - Internet Policy Registration Authority (IPRA)
  - RSA Commercial Certificate Authorities
  - PGP Internet Key Servers - examples Stable Large E-mail Database (SLED)
  - PGP Web of Trust
  - Future - Banks, Credit Card Companies and U.S. Post Office
- Certificate Formats
  DNS Security Extensions - KEY RR + SIG RR
  RSA, DSS, PEM, MISSI - X.509 certificates
  PGP - RSA public key infrastructure

AUTHENTICATION PAYLOAD FORMAT

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                     Authentication Data                       |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Authentication Authority     |           RESERVED            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Authentication Type          |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                          Certificate                          |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Authentication Authority - IANA issued identifier
- Authentication Type - Type Of Authentication Data (e.g. Certificate Format)
- Authentication Data - Data To Authentication Peer Entity

IP KEY EXCHANGE

- Requirements
  Public Key Technique
  Perfect Forward Secrecy (Back Traffic Protection)
  Secure - stand the test of time
- Additional Requirements
  Key Exchange Interchangeability
- Key Exchange Algorithms
  Numerous
  - Diffie-Hellman
  - Photuris: Diffie-Van Oorschot-Wiener STS
  - X9.42 Enhanced Diffie-Hellman
  - RSA
  - Photuris Variant
  - KEA
  - Key Escrowed (Data Recovery) Exchanges
  - ... Future Developments

KEY EXCHANGE PAYLOAD FORMAT

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              KEI              |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
|                     Key Exchange Payload                      |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Key Exchange Identifier (KEI) - Indicates Key Exchange Algorithm Used.
  KEIs must be specified in separate RFC and/or registered with IANA
- Key Exchange Payload - Data Required By The Algorithm

PROTOCOL EXCHANGES

- SA Establishment
  Base Exchange To Support Interoperability
  Identity Protection
- SA Modification
- SA Deletion
- SA Notification

SA ESTABLISHMENT

Initiator		Responder
SA Initiation [Attributes]	=>	
	<=	SA Initiation [Attributes]
Authentication payload[CA, Type, Certificate]+ Key Exchange payload [KEI, parameters]	=>	
	<=	Authentication payload [CA, Type, Certificate]+ Key Exchange payload [KEI, parameters]
SA Negotiation [Attributes]	=>	
	<=	SA Negotiation [Attributes]
SA Commit (optional)	=>	
SECURE TRAFFIC		

SA ESTABLISHMENT WITH IDENTITY PROTECTION

Initiator		Responder
SA Initiation [Attributes]	=>	
	<=	SA Initiation [Attributes]
Key Exchange [KEI, parameters]	=>	
	<=	Key Exchange [KEI, parameters]
Authentication [CA, Type, Length, Certificate]	=>	
	<=	Authentication [CA, Type, Length, Certificate]
SA Negotiation [Attributes]	=>	
	<=	SA Negotiation [Attributes]
SA Commit (optional)	=>	
SECURE TRAFFIC		

- Benefits:
  - Personnel Identity protected from passive attackers
- Cost:
  - Extra Exchange

SA MODIFY

Initiator		Responder
SECURE TRAFFIC		
SA Modify [Attributes]	=>	
	<=	SA Modify [Attributes]
Authentication payload [CA, Type, Certificate]+ Key Exchange payload [KEI, parameters]	=>	
	<=	Authentication payload [CA, Type, Certificate]+ Key Exchange payload [KEI, parameters]
SA Commit (optional)	=>	
SECURE TRAFFIC		

SA DELETE

Initiator		Responder
SECURE TRAFFIC		
SA Delete [SPI]	=>	
	<=	SA Delete [SPI]

SA NOTIFY

Initiator		Responder
SECURE TRAFFIC		
SA Notification [SPI, Information]	=>	
SECURE TRAFFIC		

PROTOTYPE SPECIFICS

- Security Associations
  Internet SA
  Fortezza SA
- Authentication Mechanisms
  Internet SA
  - RSA with PGP Certificates
  - RSA with RSA Certificates
  Fortezza SA
  - Fortezza Certificates
- Key Exchanges
  Internet SA
  - Diffie-Van Oorschot-Wiener STS (Photuris)
  Fortezza SA
  - Fortezza KEA
- Transport Protocol - UDP

PROTOTYPE DEVELOPMENT

- Prototype Development Begun
  SunOS 4.1.3
  gcc 2.6.x
  Security Associations
  - Internet Algorithms
  - Fortezza Card Algorithms

  Modeling Tools (Foresight, SPIN)
- Future - Integration with IPv4 and IPv6 ESP & AH
  Kernel Data Structure and Interface
  IP Security Association Database
  - Separate RFC for SA Database Definition

CONCLUSIONS

- Modular Design
- Flexible KMP Architecture
  Security Association Negotiation
  Mechanism Independence
- Extendable
  Security Attributes
- Development Begun
- All Help Welcome
  Security Attributes Definitions
  Key Exchanges Definitions
  Design Issues
  Document Review
  Implementing