IKE/IPSec

Network Infrastructures A.A. 2020/21

Outline

SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

Outline

SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

What is Network Security?

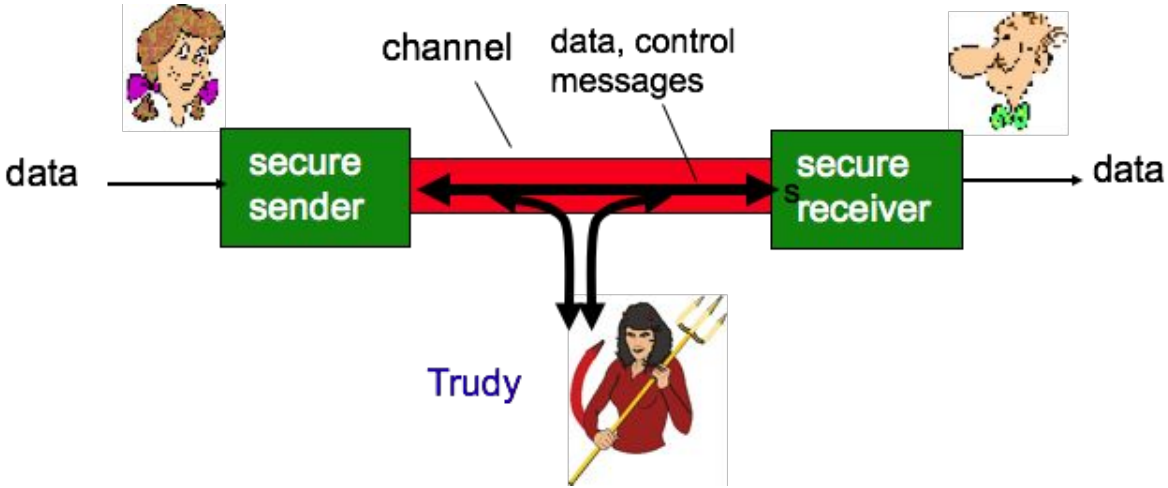
SAPIENZA
UNIVERSITÀ DI ROMA

- Network Security Services:
  - **confidentiality:** only sender, intended receiver should “understand” message contents
    - sender encrypts message
    - receiver decrypts message
  - **authentication:** sender, receiver want to confirm identity of each other
  - **message integrity:** sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
  - **access and availability:** services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

SAPIENZA
UNIVERSITÀ DI ROMA

- well-known in network security world
  - Bob, Alice want to communicate “securely”
  - Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

SAPIENZA
UNIVERSITÀ DI ROMA

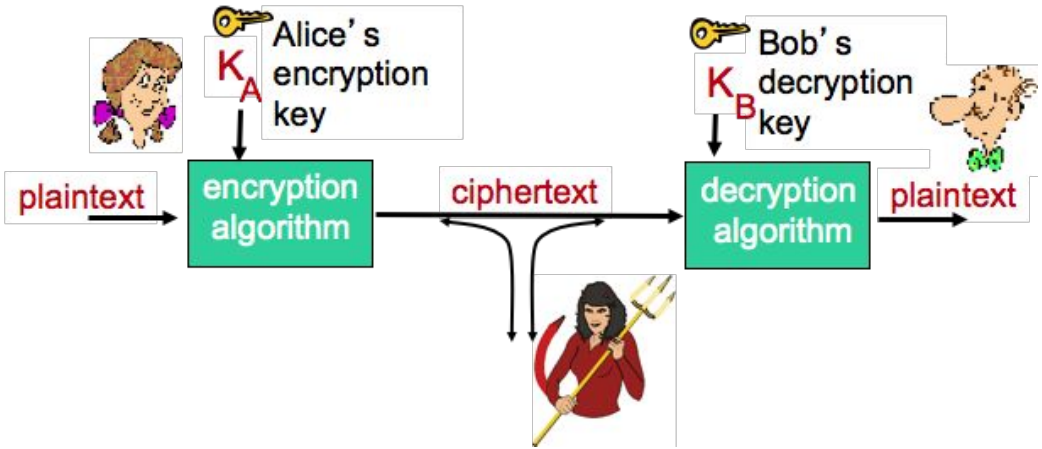
- … well, real-life Bobs and Alices!
  - Web browser/server for electronic transactions (e.g., on-line purchases)
  - on-line banking client/server
  - DNS servers
  - routers exchanging routing table updates
  - other examples?

There are bad guys (and girls) out there!

SAPIENZA
UNIVERSITÀ DI ROMA

- **Q:** What can a “bad guy” do?
- **A:** A lot!
  - eavesdrop: intercept messages
  - actively insert messages into connection
  - impersonation: can fake (spoof) source address in packet (or any field in packet)
  - hijacking: “take over” ongoing connection by removing sender or receiver, inserting himself in place
  - denial of service: prevent service from being used by others (e.g., by overloading resources)

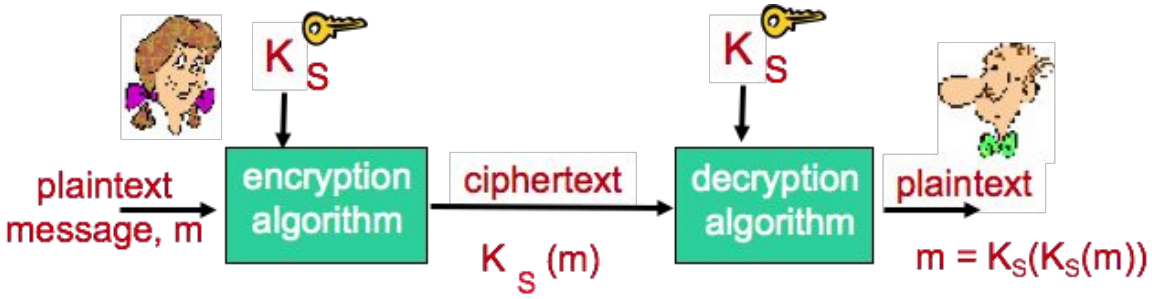
The language of cryptography



- m plaintext message
- $K_A(m)$ ciphertext, encrypted with key K_A
- $m = K_B(K_A(m))$

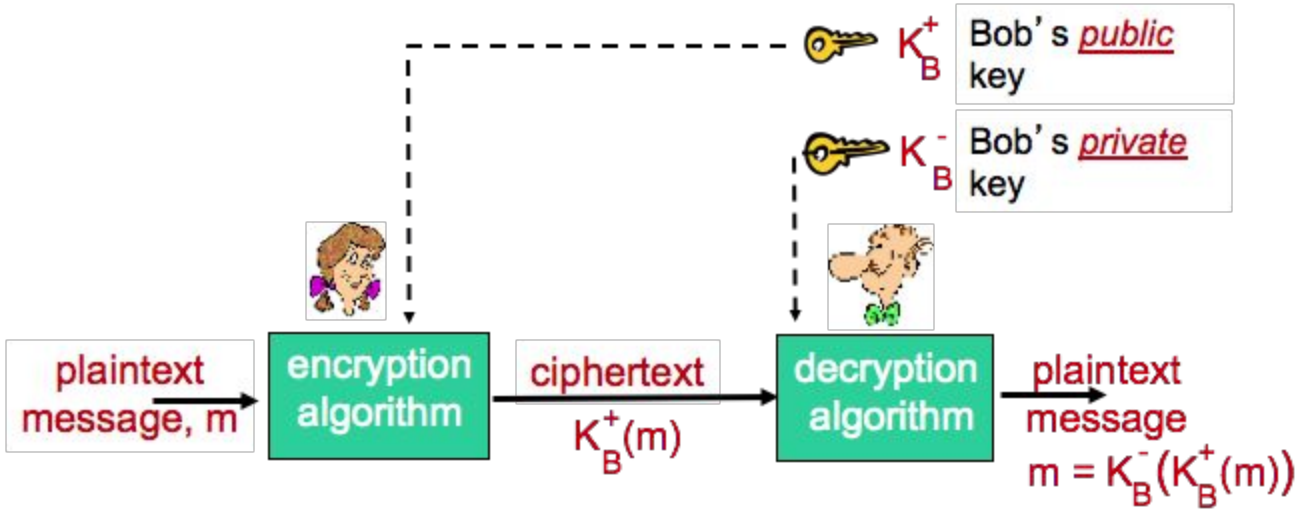
Symmetric key cryptography

SAPIENZA
UNIVERSITÀ DI ROMA



- symmetric key crypto: Bob and Alice share same (symmetric) key: K_S
  - e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- **Q:** how do Bob and Alice agree on key value?

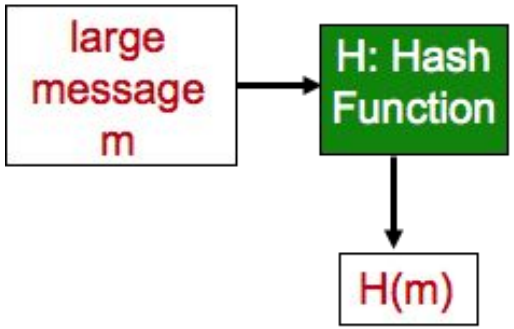
Public key cryptography



Message digests

SAPIENZA
UNIVERSITÀ DI ROMA

- computationally expensive to public-key-encrypt long messages
- **goal:** fixed-length, easy- to-compute digital "fingerprint"
  - apply hash function **H** to **m**, get fixed size message digest, **H(m)**
- Hash function properties:
  - many-to-1
  - produces fixed-size msg digest (fingerprint)
  - given message digest x, computationally infeasible to find m such that x = H(m)



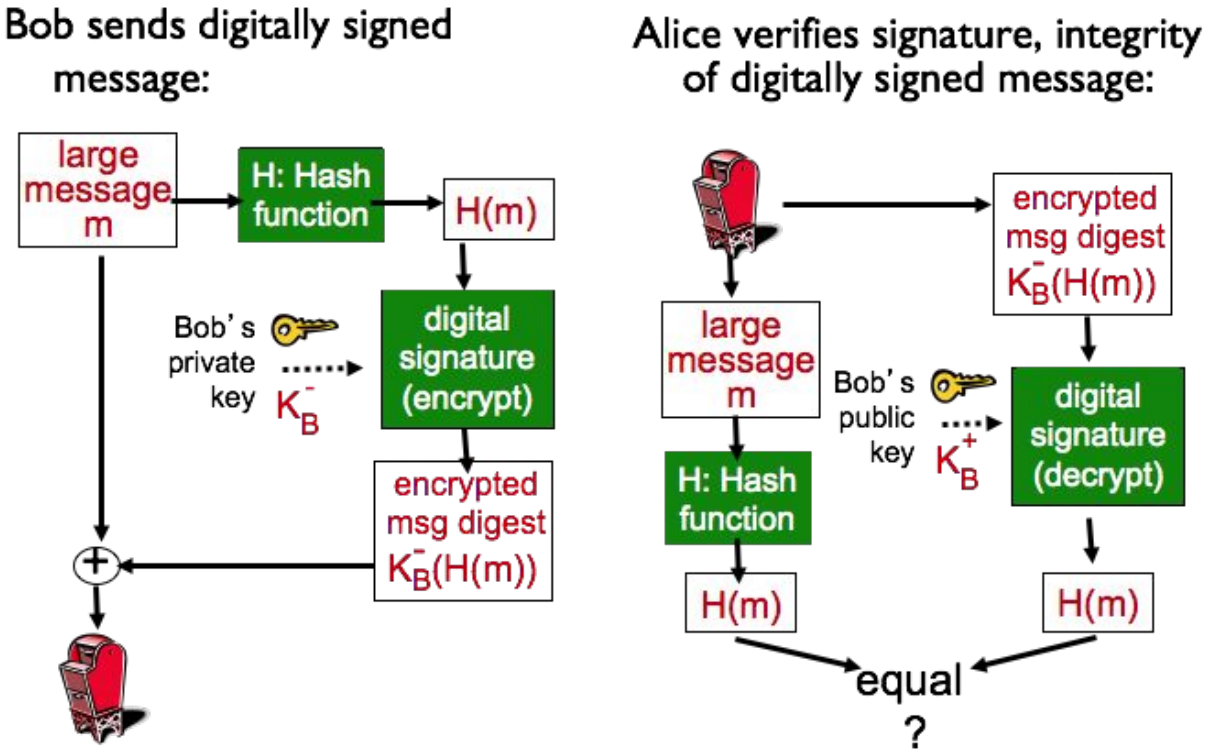
Digital signatures

SAPIENZA
UNIVERSITÀ DI ROMA

- cryptographic technique analogous to hand-written signatures:
  - sender (Bob) digitally signs document, establishing he is document owner/creator
  - verifiable, nonforgeable: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document
- Alice thus verifies that:
  - Bob signed m
  - no one else signed m
  - Bob signed m and not m‘
- **non-repudiation**:
  - Alice can take m, and signature KB(m) to court and prove that Bob signed m

Digital signature = signed message digest

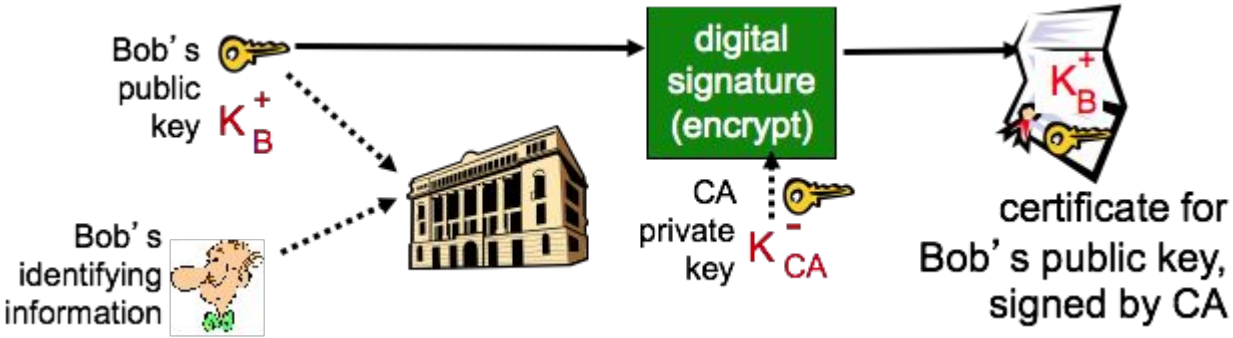
SAPIENZA
UNIVERSITÀ DI ROMA



Certification authorities

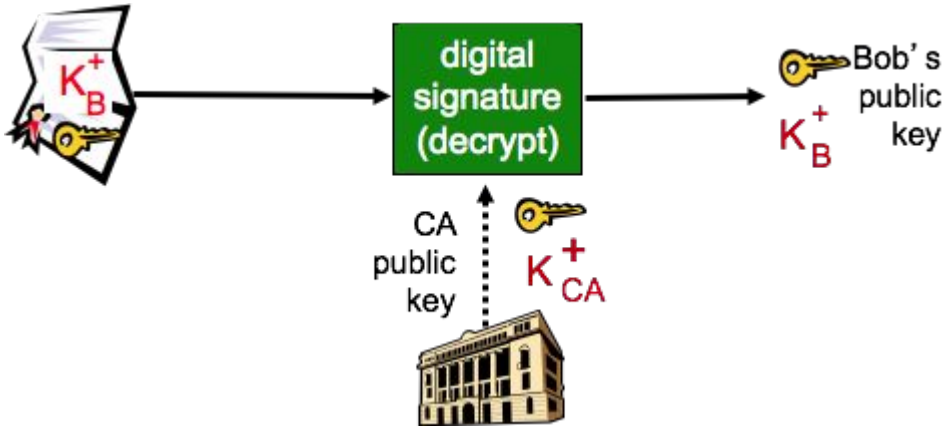
SAPIENZA UNIVERSITÀ DI ROMA

- Certification Authority (CA): binds public key to particular entity, E
- E (person, router) registers its public key with CA
  - E provides “proof of identity” to CA
  - CA creates certificate binding E to its public key
  - certificate containing E’s public key digitally signed by CA – CA says “this is E’s public key”



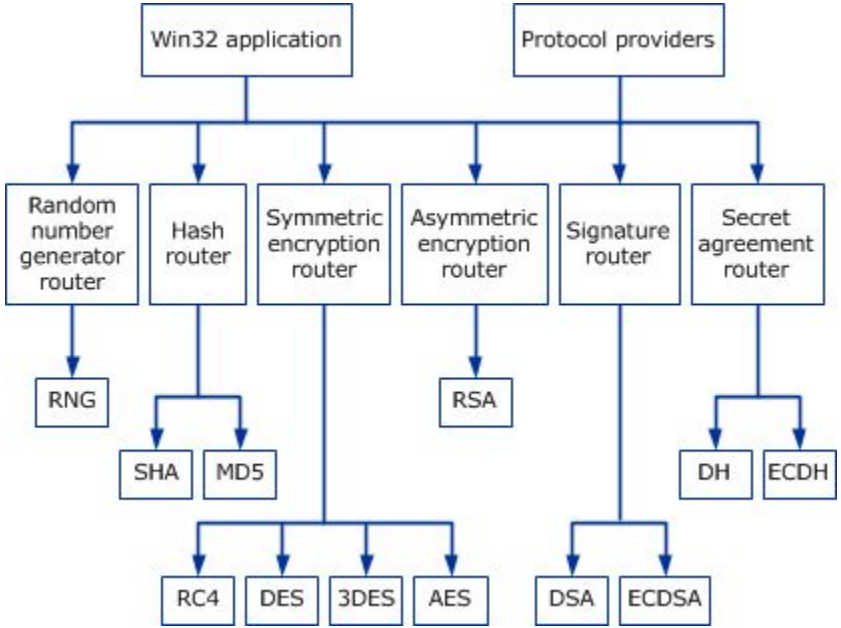
Certification authorities

- when Alice wants Bob's public key:
  - gets Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



Some Crypto Algorithms

SAPIENZA
UNIVERSITÀ DI ROMA



Outline

SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

IP Security

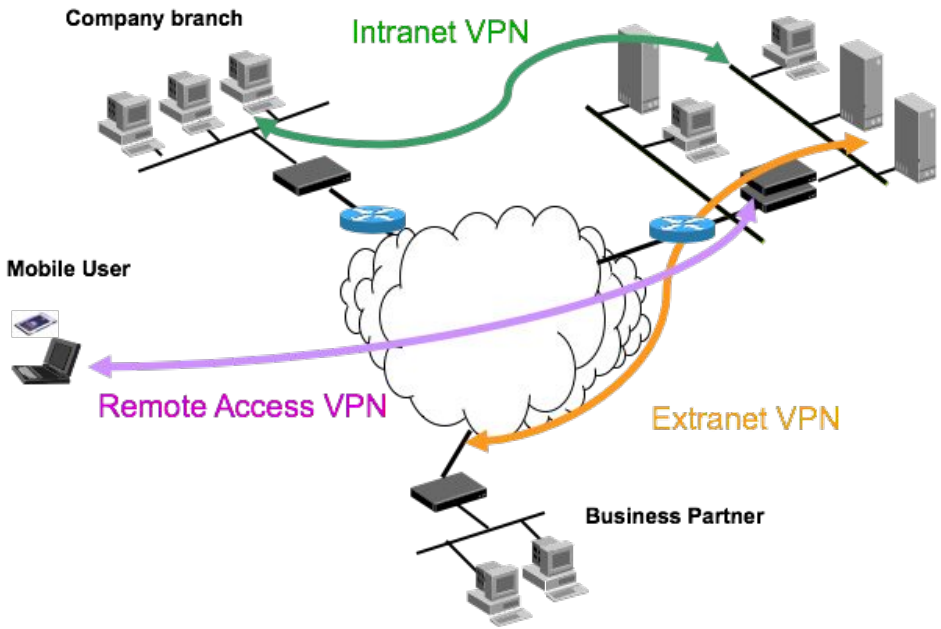
SAPIENZA
UNIVERSITÀ DI ROMA

- IP-level security encompasses three functional areas:
  - **authentication**
    - assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header
    - assures that the packet has not been altered in transit
  - **confidentiality**
    - enables communicating nodes to encrypt messages to prevent eavesdropping by third parties
  - **key management**
    - it is concerned with the secure exchange of keys

IP Security Scenarios

SAPIENZA
UNIVERSITÀ DI ROMA

- IPSec provides the capability to secure communications across a LAN, private and public WANs, the Internet



Routing Applications

SAPIENZA
UNIVERSITÀ DI ROMA

- IPSec can play a vital role in the routing architecture required for internetworking
  - A router advertisement comes from an authorized router
  - A neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged
- Without such security measures, an opponent can disrupt communications or divert some traffic
- Routing protocols such as OSPF should be run on top of security associations between routers that are defined by IPSec

IPSec Documents

SAPIENZA
UNIVERSITÀ DI ROMA

- RFC 2401: An overview of a security architecture
- RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
- RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
- RFC 2408: Specification of key management capabilities

- Support for these features is mandatory for IPv6 and optional for IPv4

IPSec Services

SAPIENZA
UNIVERSITÀ DI ROMA

- IPSec provides security services at the IP layer by enabling a system
  - to select required security protocols
  - determine the algorithm(s) to use for the service(s)
  - put in place any cryptographic keys required to provide the requested services
- Two protocols are used to provide security:
  - an authentication protocol designated by the header of the protocol (AH)
  - a combined encryption/authentication protocol designated by the format of the packet for that protocol (ESP)
- The services are
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

IPSec Services

SAPIENZA
UNIVERSITÀ DI ROMA

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	X	X	X
Connectionless Integrity	X		X
Data origin auth	X		X
Rejection of replayed packets	X	X	X
Confidentiality		X	X
Limited traffic flow confidentiality		X	X

Outline

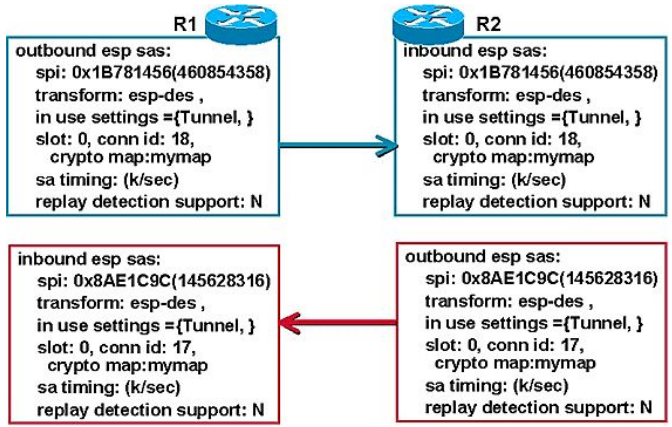
SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

Security Associations

SAPIENZA UNIVERSITÀ DI ROMA

- An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it
- If a peer relationship is needed, for two-way secure exchange, then two security associations are required
- Security services are afforded to an SA for the use of AH or ESP, but not both



Security Association

SAPIENZA
UNIVERSITÀ DI ROMA

- A security association is uniquely identified by three parameters:
  - **Security Parameters Index** (SPI):
    - local significance only
    - enable the receiving system to select the SA for processing the current packet
  - **IP Destination Address**
    - only unicast addresses are allowed
    - address of the destination endpoint of the SA
  - **Security Protocol Identifier**
    - AH or ESP

SA Parameters

SAPIENZA
UNIVERSITÀ DI ROMA

- In each IPSec implementation there is a Security Association Database that defines the parameters associated with each SA
- A security association is defined by the following parameters:
  - Sequence Number Counter
  - Anti-Replay Window
  - AH Information (Authentication algorithm, keys, key lifetimes, etc)
  - ESP Information (Encryption and authentication algorithm, keys, initialization values, key lifetimes, etc)
  - Lifetime of this Security Association
  - IPSec Protocol Mode (tunnel, transport)
  - Path MTU

SA Selectors

SAPIENZA
UNIVERSITÀ DI ROMA

- IPSec provides the user with considerable flexibility in the way in which IPSec services are applied to IP traffic
- The means by which IP traffic is related to specific SAs is the nominal Security Policy Database (SPD)
- an SPD contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic
- Each SPD entry is defined by a set of IP and upper-layer protocol field values, called selectors
- selectors are used to filter outgoing traffic in order to map it into a particular SA

SPD + SAD

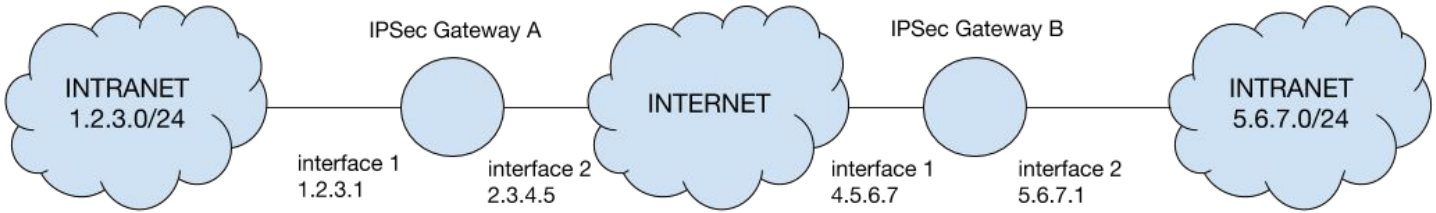
SAPIENZA
UNIVERSITÀ DI ROMA

SPD of Gateway A, Interface 2

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	2.3.4.5	500	4.5.6.7	500	BYPASS	IKE
*	1.2.3.0/24	*	5.6.7.0/24	*	ESP tunnel to 4.5.6.7	Protected VPN traffic
*	*	*	*	*	BYPASS	all other peers

SAD of Gateway A

SPI	SPD selector values	Protocol	Algorithms, keys, algorithm state
spi1	TCP, 1.2.3.0/24, 5.6.7.0/24	ESP tunnel from 4.5.6.7	....
spi2	....	ESP tunnel to 4.5.6.7	....



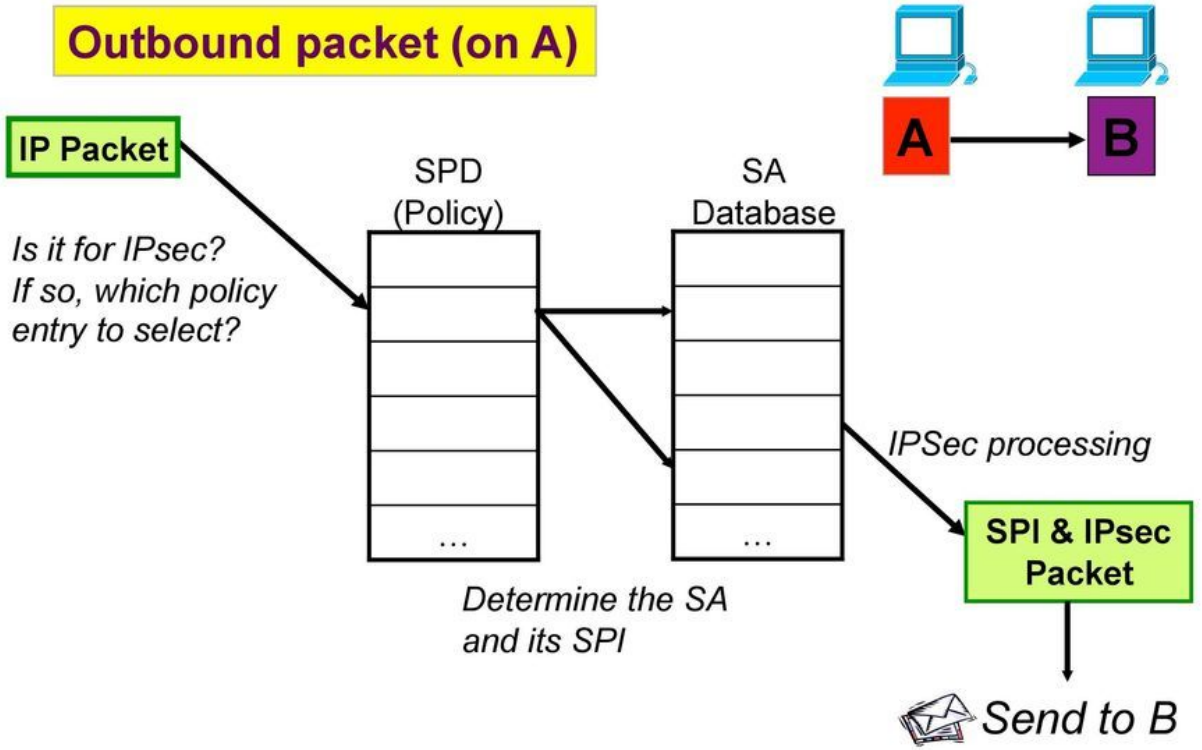
SPD + SAD: Outbound traffic

SAPIENZA
UNIVERSITÀ DI ROMA

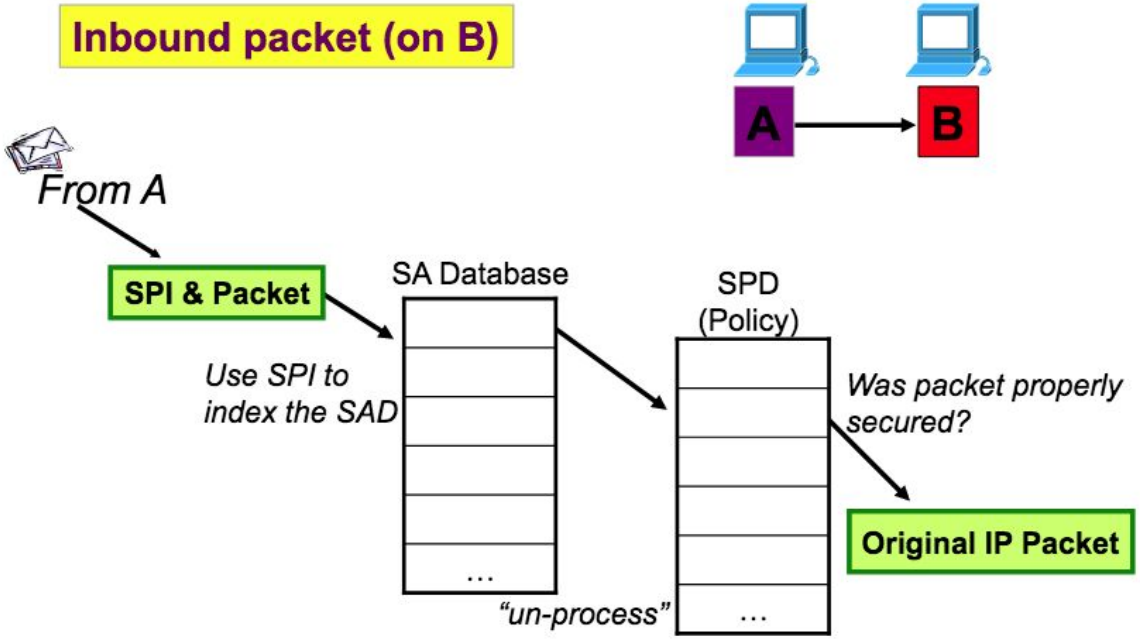
- Outbound processing obeys the following general sequence for each IP packet
  - Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry
  - Determine the SA if any for this packet and its associated SPI
  - Do the required IPSec processing (i.e., AH or ESP processing)
- Selector parameters
  - Destination IP Address
  - Source IP Address
  - Transport Layer Protocol
  - Source and Destination Ports

SPD + SAD: Outbound traffic

SAPIENZA
UNIVERSITÀ DI ROMA



SPD + SAD: Inbound traffic



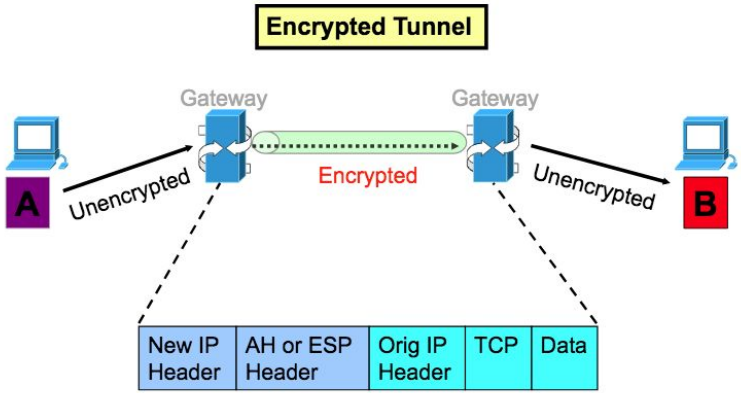
Transport and Tunnel Modes

SAPIENZA UNIVERSITÀ DI ROMA

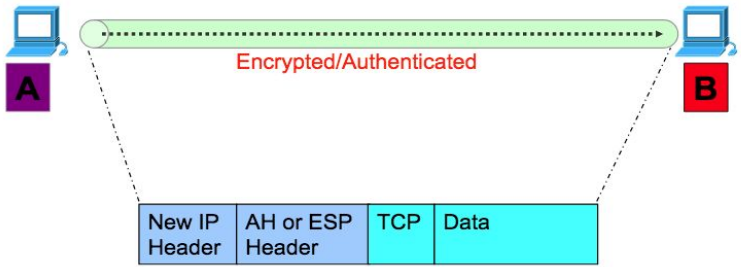
- Both AH and ESP support two modes of use:
  - Transport mode provides protection primarily for upper-layer protocols
    - Typically used for e2e communication between two hosts (e.g., a client and a server, or two workstations)
    - **ESP in transport mode:** encrypts and optionally authenticates the IP payload but not the IP header
    - **AH in transport mode:** authenticates the IP payload and selected portions of the IP header
  - Tunnel mode provides protection to the entire IP packet
    - the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header
    - used when one or both ends of an SA are a security gateway
    - a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec

Transport and Tunnel Modes

SAPIENZA
UNIVERSITÀ DI ROMA



Tunnel mode



Transport mode

Tunnel Mode and Transport Mode Functionality

SAPIENZA UNIVERSITÀ DI ROMA

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header	Encrypts entire inner IP packet
ESP with Auth.	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header	Encrypts entire inner IP packet. Authenticates inner IP packet

Outline

SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

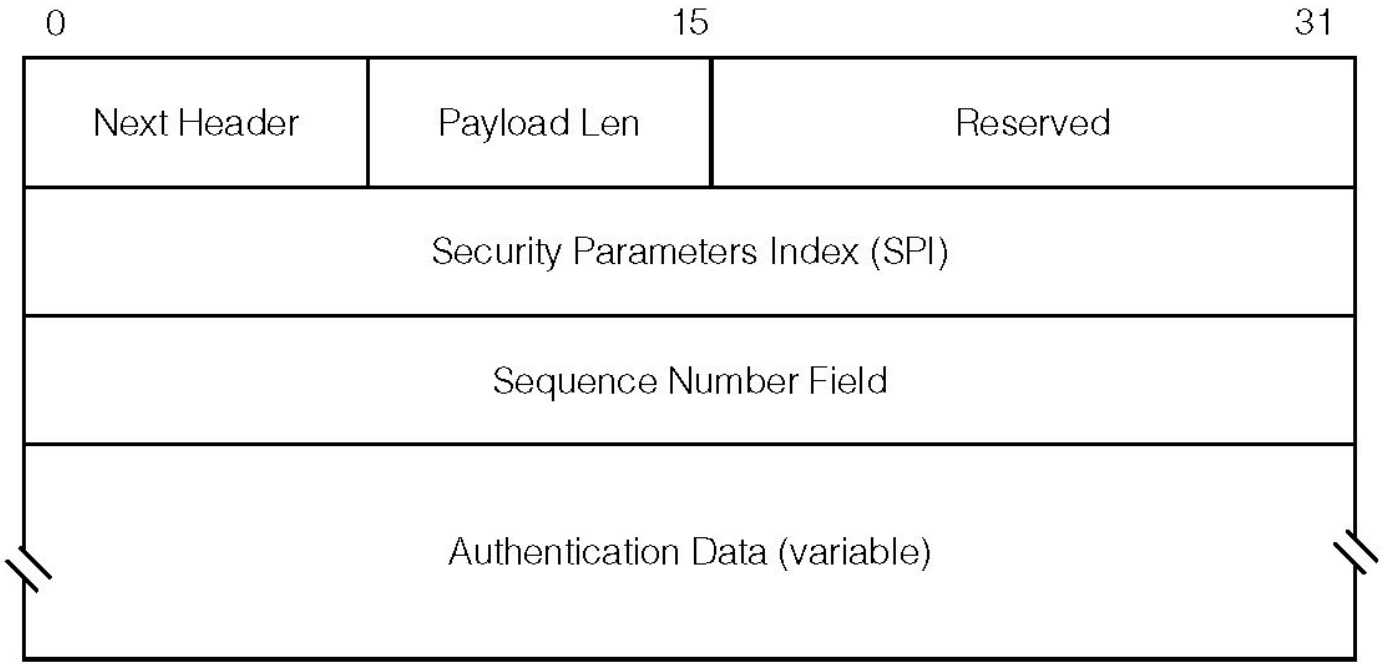
Authentication Header

SAPIENZA
UNIVERSITÀ DI ROMA

- The Authentication Header provides support for data integrity and authentication of IP packets
  - undetected modification to a packet's content in transit is not possible
- enables an end system to authenticate the user and filter traffic accordingly
- AH prevents and protects against
  - address spoofing attacks
  - replay attack

Authentication Header

SAPIENZA
UNIVERSITÀ DI ROMA



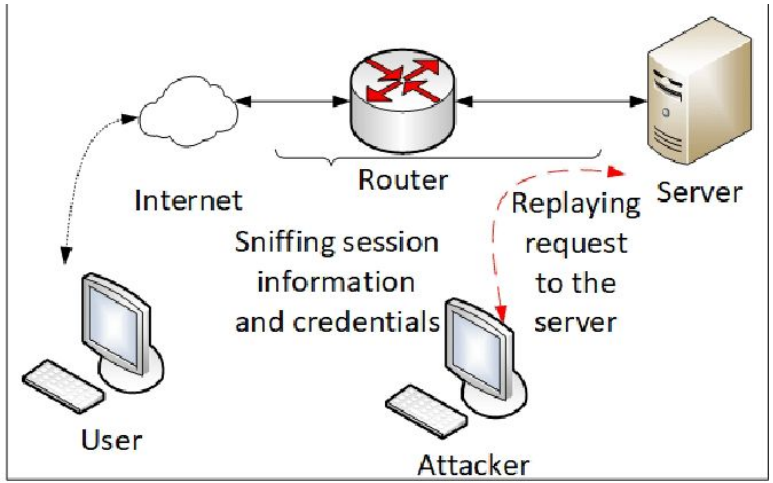
Authentication Header

SAPIENZA
UNIVERSITÀ DI ROMA

- **Next Header** (8 bits)
  - identifies the type of header immediately following this header.
- **Payload Length** (8 bits)
  - length of Authentication Header in 32-bit words, minus 2
- **Reserved** (16 bits)
- **Security Parameters Index** (32 bits)
  - identifies a security association.
- **Sequence Number** (32 bits)
  - a monotonically increasing counter value, discussed later.
- **Authentication Data** (variable):
  - a variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value (ICV), or MAC, for this packet

Anti-Replay Service

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination



Anti-Replay Service

SAPIENZA
UNIVERSITÀ DI ROMA

- **Sender side**
  - The Sequence Number field is designed to thwart such attacks
  - When a new SA is established, the sender initializes a sequence number counter to 0
  - Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field
    - thus, the first value to be used is 1
  - If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past $2^{32}-1$ back to zero
  - If the limit of $2^{32}-1$ is reached, the sender should terminate this SA and negotiate a new SA with a new key

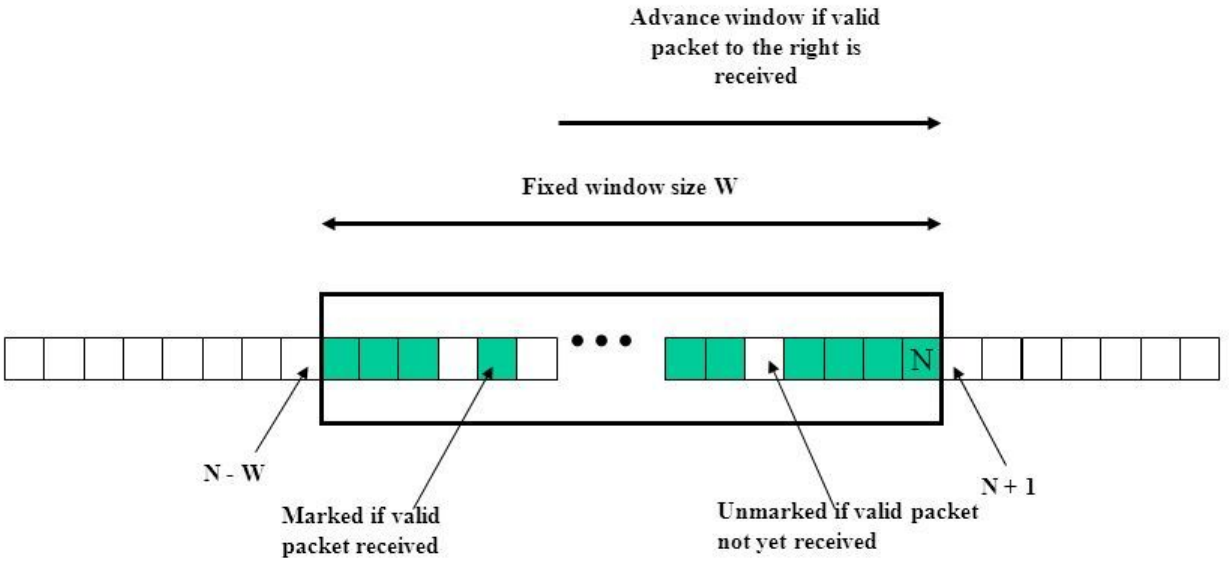
Anti-Reply Service

SAPIENZA
UNIVERSITÀ DI ROMA

- **Receiver side**
  - challenge: IP is a connectionless , unreliable service, and does not guarantee that packets will be delivered in order (or simply delivered)
  - the receiver should implement a window of size **W**, with a default of W = 64
    - If the **received packet falls within the window and is new**, the MAC is checked
      - If the packet is authenticated, the corresponding slot in the window is marked
    - If the **received packet is to the right of the window**, the MAC is checked.
      - If the packet is authenticated
        - the window is advanced so that this sequence number is the right edge of the window
        - the corresponding slot in the window is marked
    - If the **received packet is to the left of the window**, or if authentication fails, the packet is discarded (auditable event)

Anti-Replay Service

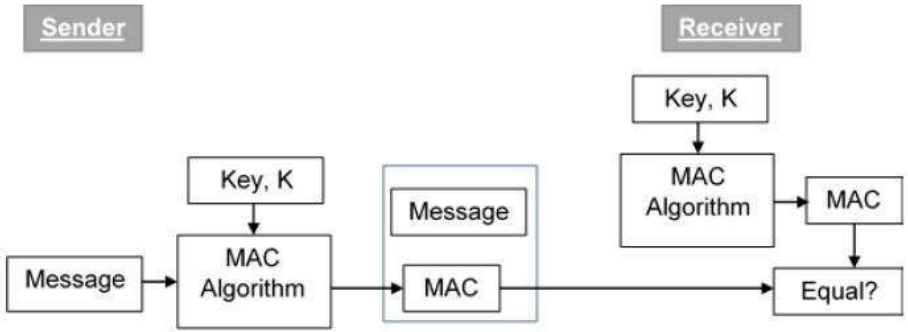
SAPIENZA
UNIVERSITÀ DI ROMA



Integrity Check Value

SAPIENZA
UNIVERSITÀ DI ROMA

- Integrity of information refers to protecting information from being modified by unauthorized parties
- Message Authentication Code (MAC) used to provide integrity and authentication of messages
  - generates an authenticator taking as input the message **m** and a secret key **K**



Integrity Check Value

SAPIENZA UNIVERSITÀ DI ROMA

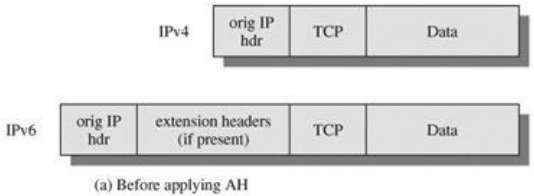
- The Authentication Data field holds a value referred to as the Integrity Check Value
- The ICV is a message authentication code produced by a MAC algorithm
  - HMAC-MD5-96 or HMAC-SHA-1-96
- the full HMAC value is calculated but then truncated by using the first 96 bits, which is the default length for the Authentication Data field
- The **MAC is calculated over**
  - IP header fields that either do not change in transit (immutable) or that are predictable in value upon arrival at the endpoint for the AH SA
  - The AH header other than the Authentication Data field
  - The entire upper-level protocol data, which is assumed to be immutable in transit

Integrity Check Value

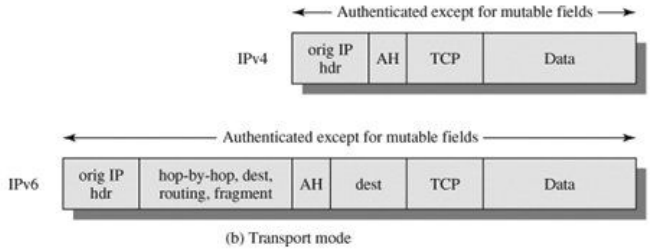
- For IPv4, examples of immutable fields are
  - Internet Header Length
  - Source Address
- An example of a mutable but predictable field is the Destination Address (with loose or strict source routing).
- Examples of mutable fields that are zeroed prior to ICV calculation are
  - the Time to Live
  - the Header Checksum

Scope of AH Authentication

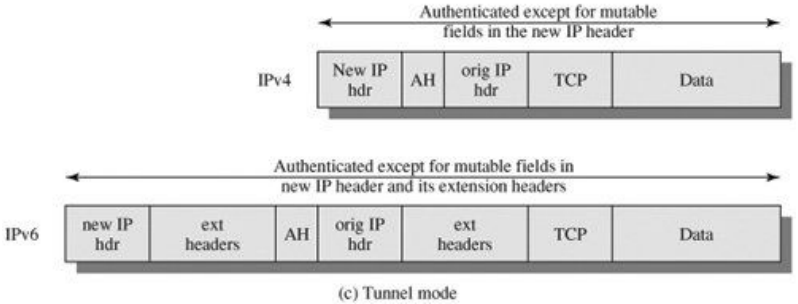
SAPIENZA
UNIVERSITÀ DI ROMA



(a) Before applying AH



(b) Transport mode



(c) Tunnel mode

Outline

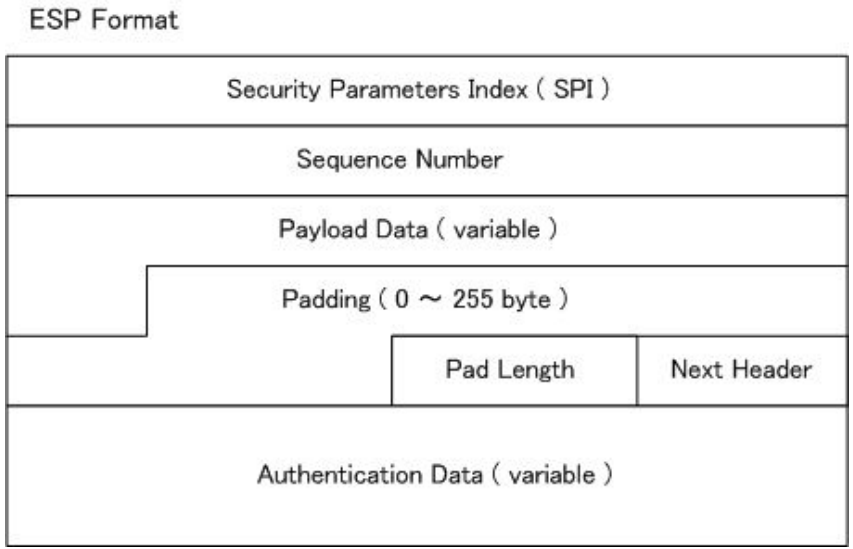
SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

Encapsulating Security Payload

SAPIENZA
UNIVERSITÀ DI ROMA

- The Encapsulating Security Payload provides confidentiality services
  - ESP can also provide an authentication service

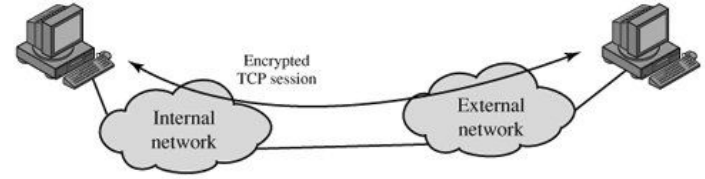


Encapsulating Security Payload

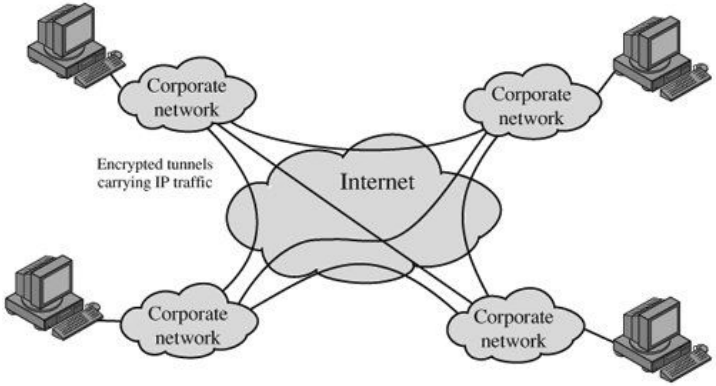
SAPIENZA
UNIVERSITÀ DI ROMA

- Security Parameters Index (32 bits)
- Sequence Number (32 bits)
- Payload Data (variable)
- Padding (0255 bytes)
- Pad Length (8 bits)
  - indicates the number of pad bytes immediately preceding this field
- Next Header (8 bits)
- Authentication Data (variable)
  - contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field

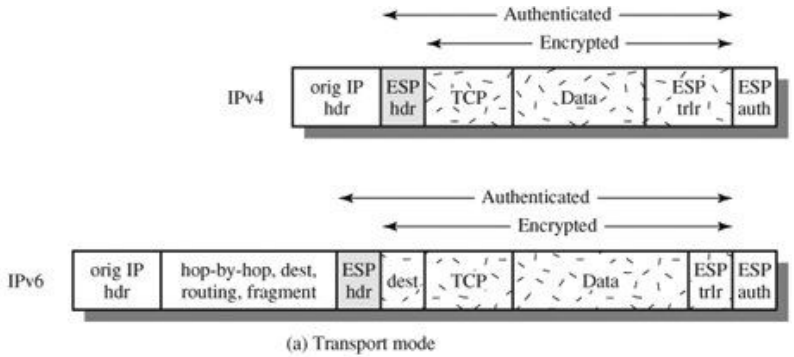
Transport Mode vs Tunnel Mode



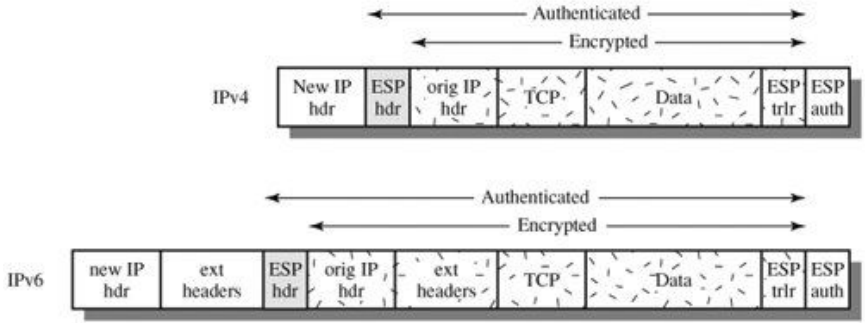
(a) Transport-level security



(b) A virtual private network via tunnel mode



(a) Transport mode



(b) Tunnel mode

Outline

SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

Combining Security Associations

SAPIENZA
UNIVERSITÀ DI ROMA

- An individual SA can implement either the AH or ESP protocol but not both
- Sometimes a particular traffic flow will call for the services provided by both AH and ESP
- The term security association bundle refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPSec services
- The SAs in a bundle may terminate at different endpoints or at the same endpoints

Authentication + Confidentiality

SAPIENZA UNIVERSITÀ DI ROMA

- Encryption and authentication can be combined in order to transmit an IP packet that has both confidentiality and authentication between hosts
- **ESP with Authentication Option**
  - Transport mode ESP
    - Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected
  - Tunnel mode ESP
    - Authentication applies to the entire IP packet delivered to the outer IP destination address (e.g., a firewall), and authentication is performed at that destination
    - The entire inner IP packet is protected by the privacy mechanism, for delivery to the inner IP destination

Authentication + Confidentiality

SAPIENZA UNIVERSITÀ DI ROMA

- Encryption and authentication can be combined in order to transmit an IP packet that has both confidentiality and authentication between hosts
- **Transport-Tunnel Bundle**
  - use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA
    - In this case ESP is used without its authentication option
    - advantage (w.r.t. ESP + auth opt SA) is that the authentication covers more fields, including the source and destination IP addresses
    - disadvantage is the overhead of two SAs versus one SA

Authentication + Confidentiality

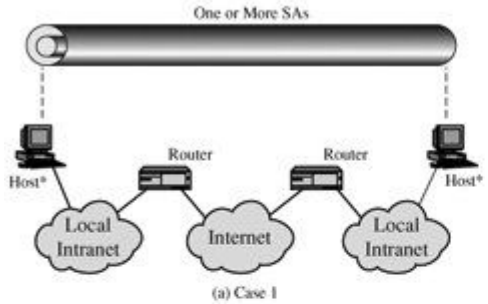
SAPIENZA
UNIVERSITÀ DI ROMA

- Encryption and authentication can be combined in order to transmit an IP packet that has both confidentiality and authentication between hosts
- **Transport Adjacency**
  - use bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
  - use of authentication prior to encryption might be preferable for several reasons
    - because the **authentication data are protected by encryption**, it is impossible for anyone to intercept the message and alter the authentication data without detection
    - it may be desirable to store the **authentication information** with the message **at the destination** for later reference

Combinations of SA

SAPIENZA
UNIVERSITÀ DI ROMA

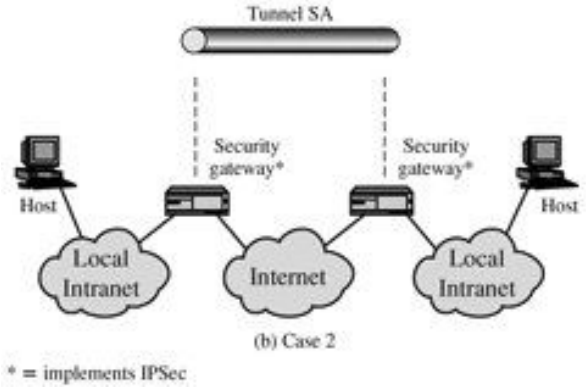
- All security is provided between end systems that implement IPSec
- For any two end systems to communicate via an SA, they must share the appropriate secret keys
- Some possible combinations:
  - AH in transport mode
  - ESP in transport mode
  - ESP followed by AH in transport mode (an ESP SA inside an AH SA)
  - Any among the previous ones inside an AH or ESP in tunnel mode



Combinations of SA

SAPIENZA
UNIVERSITÀ DI ROMA

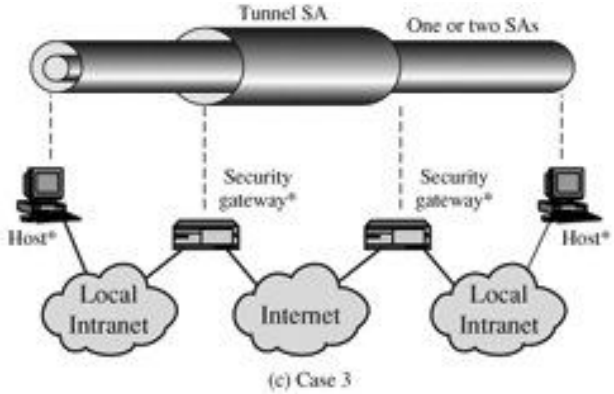
- Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPSec
- This case illustrates simple virtual private network support
- Only a single tunnel SA is needed for this case
    - The tunnel could support AH, ESP, or ESP with the authentication option
    - Nested tunnels are not required because the IPSec services apply to the entire inner packet



Combinations of SA

SAPIENZA
UNIVERSITÀ DI ROMA

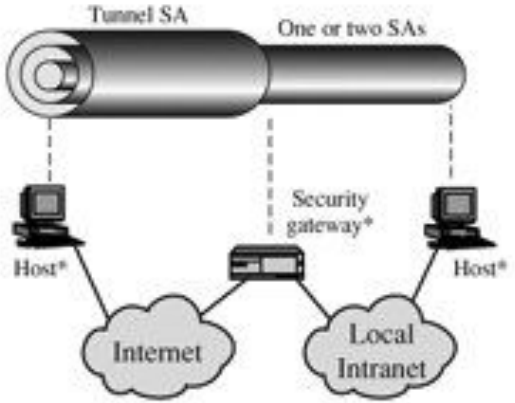
- The gateway-to-gateway tunnel provides either authentication or confidentiality or both for all traffic between end systems
- When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality
- Individual hosts can implement any additional IPSec services required for given applications or given users by means of end-to-end SAs



Combinations of SA

SAPIENZA
UNIVERSITÀ DI ROMA

- Provide support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall
- Only tunnel mode is required between the remote host and the firewall
- One or two SAs may be used between the remote host and the local host



Outline

SAPIENZA
UNIVERSITÀ DI ROMA

- Background on Communication Security
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combining Security Associations
- Key Management

Key Management

SAPIENZA
UNIVERSITÀ DI ROMA

- The key management portion of IPSec involves the determination and distribution of secret keys
- A typical requirement is four keys for communication between two applications: transmit and receive pairs for both AH and ESP
- The IPSec Architecture document mandates support for two types of key management:
  - **Manual**
    - A system administrator manually configures each system with its own keys and with the keys of other communicating systems
    - practical for small, relatively static environments
  - **Automated**
    - An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration

Key Management

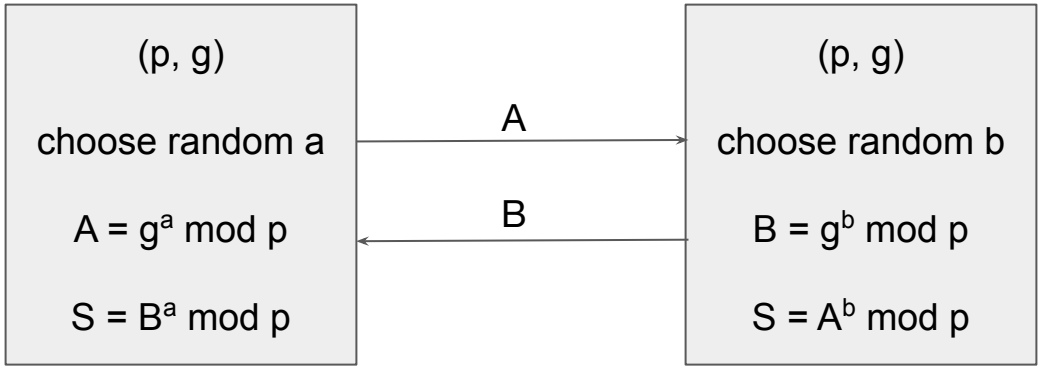
SAPIENZA
UNIVERSITÀ DI ROMA

- The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley
- It consists of the following elements:
  - **Oakley Key Determination Protocol**
    - Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security
  - **Internet Security Association and Key Management Protocol** (ISAKMP)
    - ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes

Oakley Key Determination Protocol

SAPIENZA UNIVERSITÀ DI ROMA

- Oakley is a refinement of the Diffie-Hellman key exchange algorithm
  - Diffie-Hellman
    - prior agreement on global parameters:
      - **p** - a large prime number, **p**
      - **g** - a primitive root of **p**



Oakley Key Determination Protocol

SAPIENZA
UNIVERSITÀ DI ROMA

- **attractive features:**
  - Secret keys are created only when needed
    - no need to store secret keys for a long period of time, exposing them to increased vulnerability
    - no pre existing infrastructure is required other than an agreement on the global parameters
- **weaknesses**
  - it does not provide any information about the identities of the parties
  - subject to man-in-the-middle attacks
  - It is computationally intensive
    - it is vulnerable to a clogging attack, in which an opponent requests a high number of keys

Features of Oakley

SAPIENZA
UNIVERSITÀ DI ROMA

- Oakley is designed to retain the advantages of Diffie-Hellman while countering its weaknesses
- The Oakley algorithm is characterized by **five important features**
  1. It employs a mechanism known as cookies to thwart clogging attacks
  2. It enables the two parties to negotiate a group (DH parameters)
  3. It uses nonces to ensure against replay attacks
  4. It enables the exchange of Diffie-Hellman public key values
  5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks

Cookies

SAPIENZA
UNIVERSITÀ DI ROMA

- **Clogging attack**
  - an opponent forges the source address of a legitimate user and sends a public Diffie-Hellman key to the victim
  - The victim then performs a modular exponentiation to compute the secret key
  - Repeated messages of this type can clog the victim's system with useless work
- **Cookie exchange**
  - each side send a pseudorandom number (cookie) in the initial message
  - the other side acknowledges the cookie
  - this acknowledgment must be repeated in the first message of the DH key exchange
- If the source address was forged, the opponent gets no answer
  - it can only force a user to generate acknowledgments (not to perform the DH calculation)

Cookies

SAPIENZA
UNIVERSITÀ DI ROMA

- cookie generation must satisfy three basic requirements
  - The cookie must depend on the specific parties
  - It must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity
  - The cookie generation and verification methods must be fast to thwart attacks intended to sabotage processor resources
- The recommended method for creating the cookie is to perform a **fast hash** (e.g., MD5) over the **IP Source** and **Destination** addresses, the UDP Source and Destination **ports**, and a locally generated **secret value**

Other Security Mechanisms

SAPIENZA
UNIVERSITÀ DI ROMA

- Oakley supports the use of different groups for the Diffie-Hellman key exchange
  - each group includes the definition of the two global parameters and the identity of the algorithm
- Oakley employs nonces to ensure against replay attacks
  - each nonce is a locally generated pseudorandom number
- Three different authentication methods:
  - **digital signatures:** the exchange is authenticated by signing a mutually obtainable hash generated over important parameters, such as user IDs and nonces
  - **public-key encryption:** the exchange is authenticated by encrypting parameters such as IDs and nonces with the sender's private key
  - **symmetric-key encryption:** a key derived by some out-of-band mechanism can be used to authenticate the exchange by symmetric encryption of exchange parameters

An Aggressive Example

SAPIENZA
UNIVERSITÀ DI ROMA

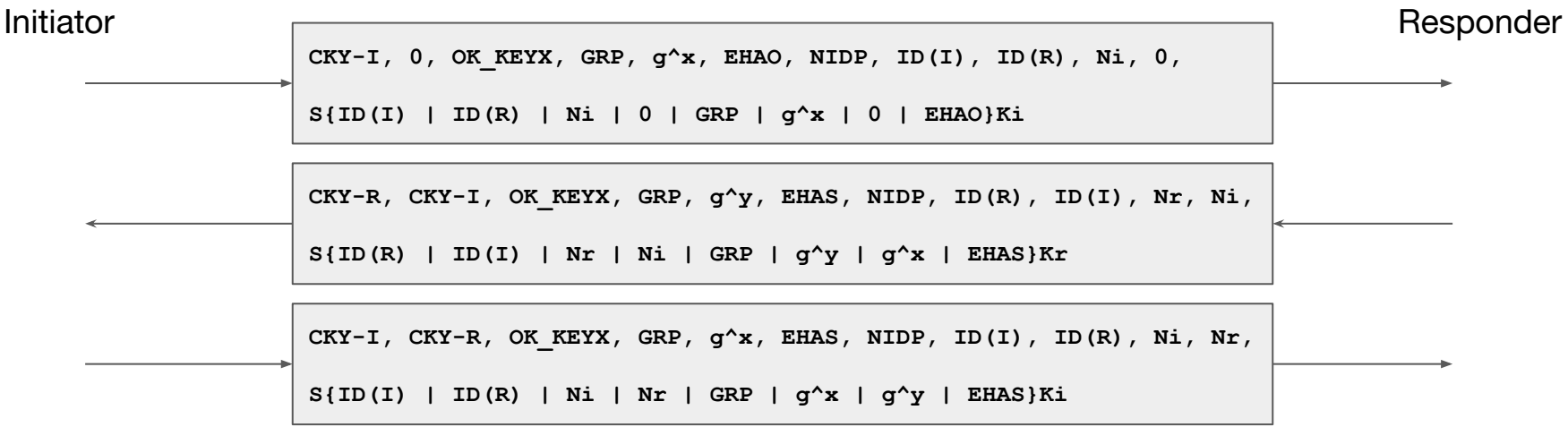
RFC 2412

- CKY-I originator cookie.
- CKY-R responder cookie.
- MSGTYPE message type
- GRP the name of the Diffie-Hellman group used for the exchange
- g^x (or g^y) variable length integer representing a power of group generator
- EHAO or EHAS encryption, hash, authentication functions, offered and selected, respectively
- IDP an indicator as to whether or not encryption with g^xy follows (perfect forward secrecy for ID's)
- ID(I) the identity for the Initiator
- ID(R) the identity for the Responder
- Ni nonce supplied by the Initiator
- Nr nonce supplied by the Responder

An Aggressive Example

SAPIENZA UNIVERSITÀ DI ROMA

- The following example indicates how two parties can complete a key exchange in three messages



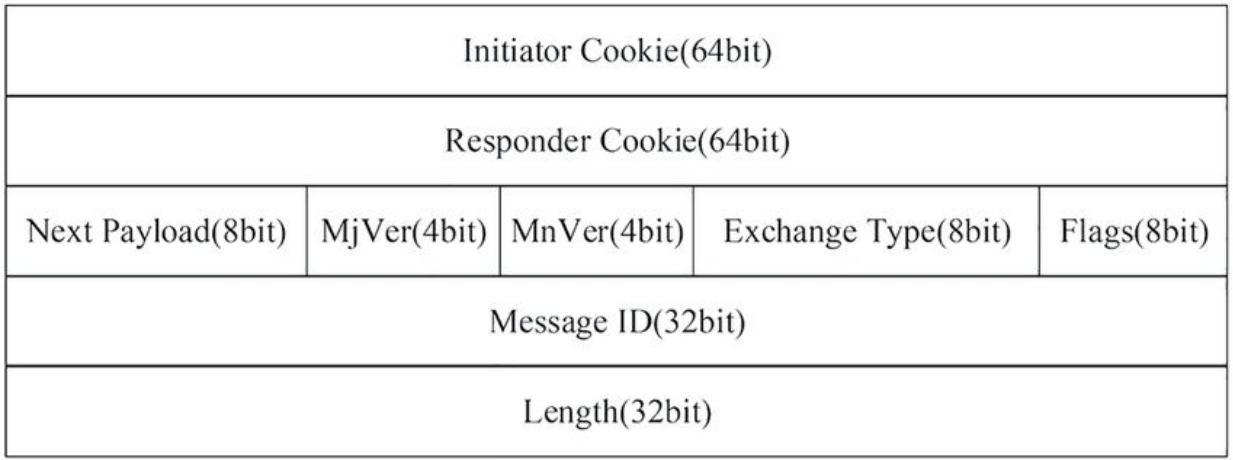
ISAKMP

- ISAKMP defines procedures and packet formats to **establish**, **negotiate**, **modify**, and **delete** security associations
- As part of SA establishment, ISAKMP defines payloads for exchanging key generation and authentication data
- These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm, and authentication mechanism

ISAKMP Header Format

SAPIENZA UNIVERSITÀ DI ROMA

- An ISAKMP message consists of an ISAKMP header followed by one or more payloads
  - messages are encapsulated in **UDP segments**



ISAKMP Header Format

SAPIENZA
UNIVERSITÀ DI ROMA

- **Initiator Cookie:** cookie of entity that initiated SA establishment
- **Responder Cookie:** cookie of responding entity (null in first message from initiator)
- **Next Payload:** indicates the type of the first payload in the message
- **Major Version:** indicates major version of ISAKMP in use
- **Minor Version:** indicates minor version in use
- **Exchange Type:** indicates the type of exchange
- **Flags:** indicates specific options set for this ISAKMP exchange
  - the Encryption bit is set if all payloads following the header are encrypted using the encryption algorithm for this SA
  - the Commit bit is used to ensure that encrypted material is not received prior to completion of SA establishment
- **Message ID:** unique ID for this message
- **Length:** length of total message (header plus all payloads) in octets

ISAKMP Payload Types

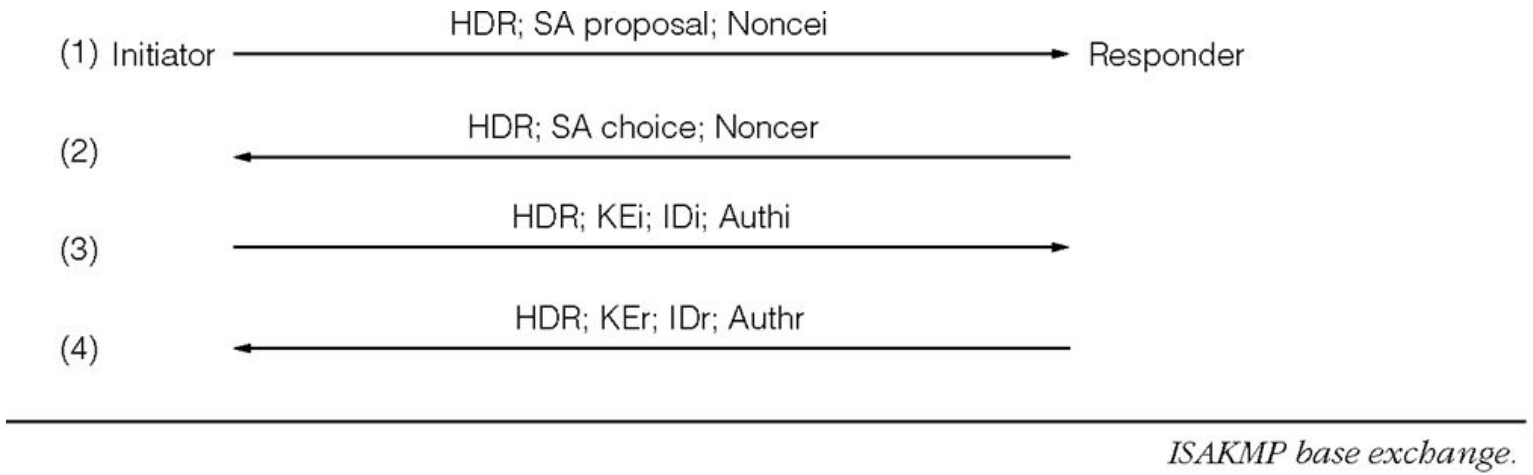
SAPIENZA
UNIVERSITÀ DI ROMA

- **Security Association payload**
  - used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place
- **Proposal payload**
  - proposal #, Protocol-ID, SPI Size, # of Transforms, SPI
- **Transform payload**
  - Transform #, Transform-ID, SA Attributes
- **Key Exchange payload**
  - Key Exchange Data
- **Identification payload**
  - ID Type, ID Data
- **Certificate payload**
  - Cert Encoding, Certificate Data
- **Certificate Request payload**
  - # Cert Types, Certificate Types, # Cert Auths, Certificate Authorities
- **Hash payload**
  - Hash data
- **Signature payload**
  - Signature data
- **Nonce payload**
  - Nonce data
- **Notification payload**
  - DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
- **Delete payload**
  - DOI, Protocol-ID, SPI Size, #of SPIs, SPI (one or more)

ISAKMP Exchange Type

SAPIENZA
UNIVERSITÀ DI ROMA

Base Exchange: allows key exchange and authentication material to be transmitted together

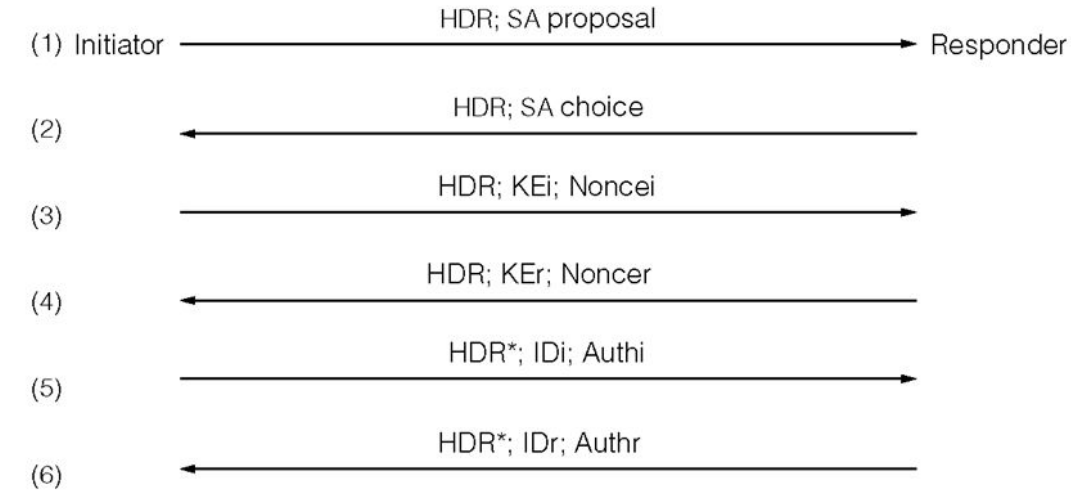


ISAKMP base exchange.

ISAKMP Exchange Type

SAPIENZA
UNIVERSITÀ DI ROMA

Identity Protection Exchange: expands the Base Exchange to protect the users' identities

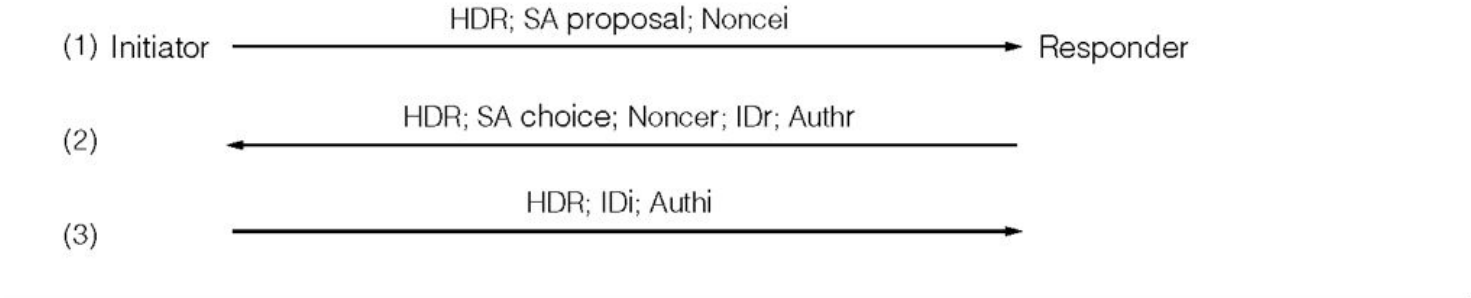


ISAKMP identity protection exchange.

ISAKMP Exchange Type

SAPIENZA
UNIVERSITÀ DI ROMA

Authentication Only Exchange: is used to perform mutual authentication

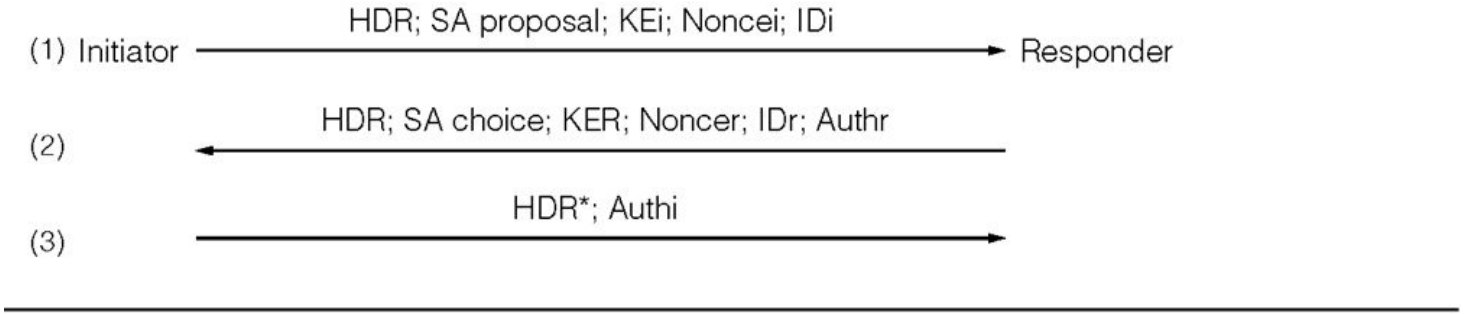


ISAKMP authentication only exchange.

ISAKMP Exchange Type

SAPIENZA
UNIVERSITÀ DI ROMA

Aggressive Exchange: minimizes the number of exchanges at the expense of not providing identity protection



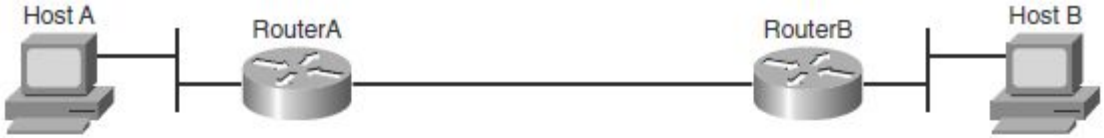
ISAKMP aggressive mode exchange.

IKE Protocol

SAPIENZA
UNIVERSITÀ DI ROMA

- The Internet Key Exchange (IKE) protocol is a hybrid implementation of the Oakley key exchanges, which is designed according to the ISAKMP framework
- IKE negotiates and establishes both the **ISAKMP SA** and the **IPsec SAs**
- It works in two phases
  - **IKE Phase I negotiation**
    - establishes an ISAKMP SA through either the Identity Protection exchange (referred to as main mode) or the Aggressive Mode Exchange
    - three shared keys are established
      - two keys are used to authenticate and encrypt last two messages of the phase 1 (and messages of phase 2)
      - the third shared key is used for deriving keys for IPSEC security associations
  - **IKE Phase II negotiation (quick mode)**
    - establishes IPsec SAs

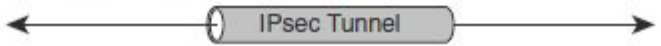
IKE Protocol



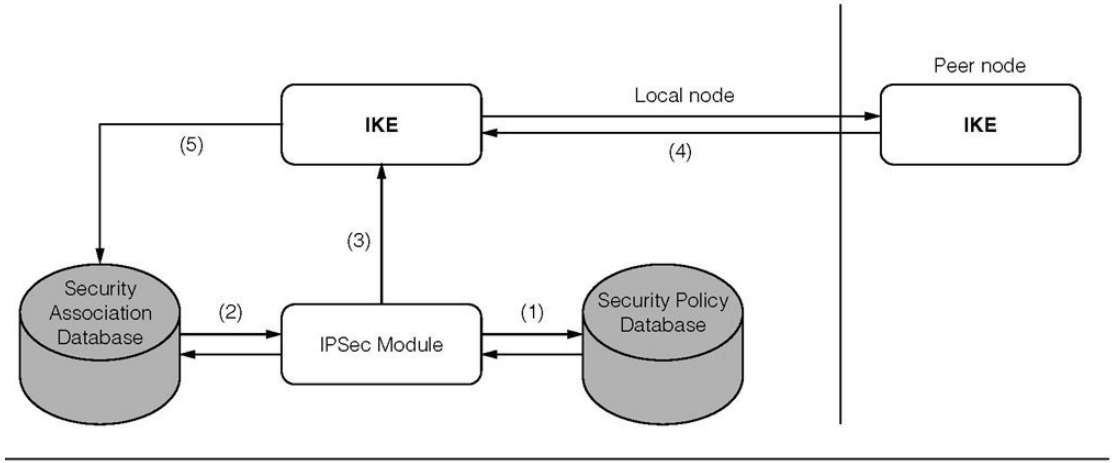
1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE Phase 1 session.

3. Routers A and B negotiate an IKE Phase 2 session.

4. Information is exchanged via IPsec tunnel.



IKE Protocol



The relationship between IP security-related modules.

(1) the IPsec module examines the SPD to determine if IPsec processing is enabled on the outgoing traffic. (2) For IPsec processing enabled traffic that does not have a corresponding entry in the SAD, (3) the IPsec module requests the IKE module to establish the necessary SA. (4) The IKE module negotiates and performs the necessary exchange with the peer IKE module to establish the SA. (5) Then the IKE module inserts this new SA into the SAD.

IKE in Action

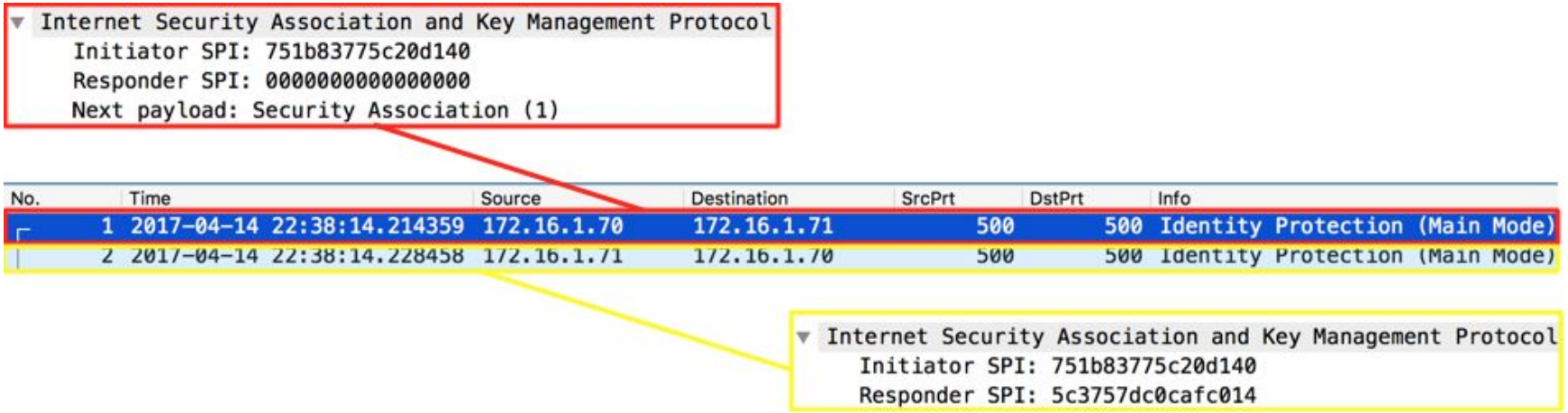
SAPIENZA
UNIVERSITÀ DI ROMA

https://devcentral.f5.com/s/articles/understanding-ikev1-negotiation-on-wireshark-34187

No.	Time	Source	Destination	SrcPrt	DstPrt	Info
1	2017-04-14 22:38:14.214359	172.16.1.70	172.16.1.71	500	500	Identity Protection (Main Mode)
2	2017-04-14 22:38:14.228458	172.16.1.71	172.16.1.70	500	500	Identity Protection (Main Mode)
3	2017-04-14 22:38:14.246521	172.16.1.70	172.16.1.71	500	500	Identity Protection (Main Mode)
4	2017-04-14 22:38:14.250607	172.16.1.71	172.16.1.70	500	500	Identity Protection (Main Mode)
5	2017-04-14 22:38:14.263722	172.16.1.70	172.16.1.71	500	500	Identity Protection (Main Mode)
6	2017-04-14 22:38:14.264785	172.16.1.71	172.16.1.70	500	500	Identity Protection (Main Mode)
7	2017-04-14 22:38:14.281969	172.16.1.70	172.16.1.71	500	500	Quick Mode
8	2017-04-14 22:38:14.282573	172.16.1.71	172.16.1.70	500	500	Quick Mode
9	2017-04-14 22:38:14.445523	172.16.1.70	172.16.1.71	500	500	Quick Mode

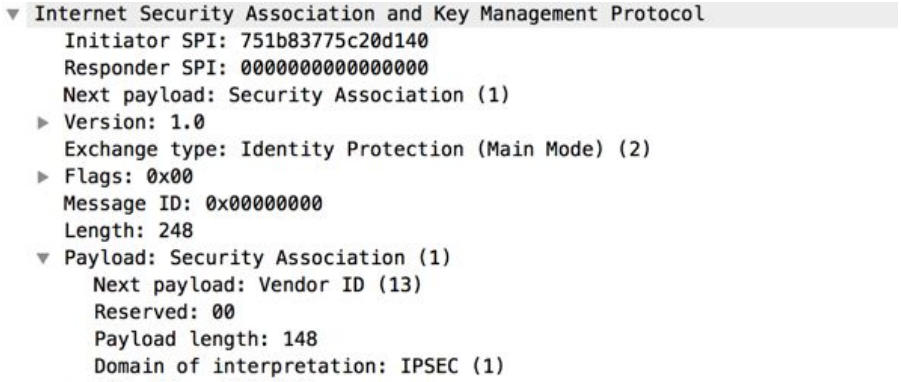
IKE in Action

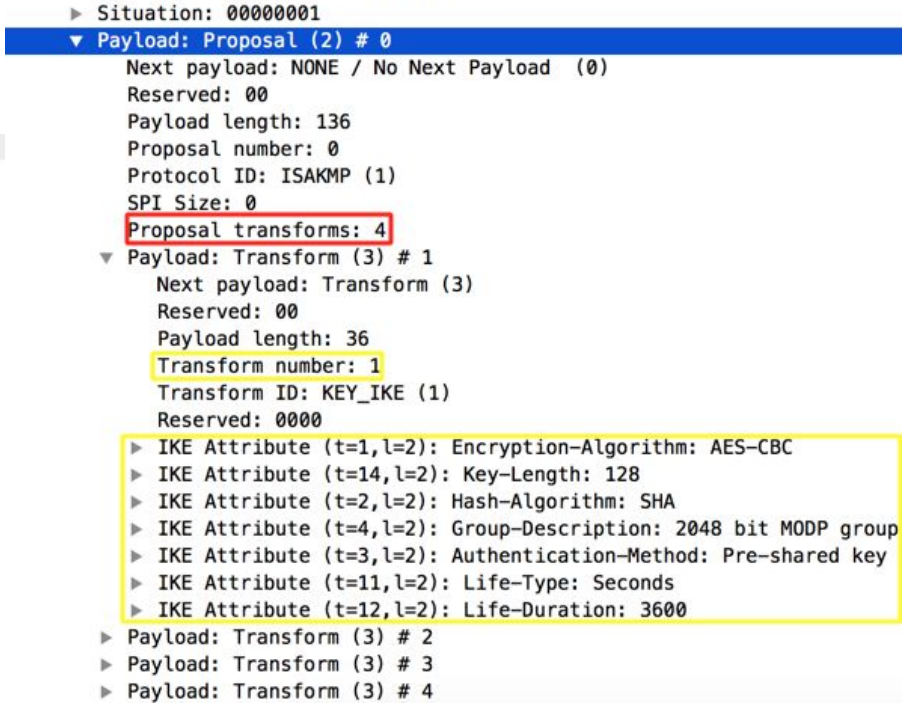
SAPIENZA
UNIVERSITÀ DI ROMA



IKE in Action

SAPIENZA
UNIVERSITÀ DI ROMA





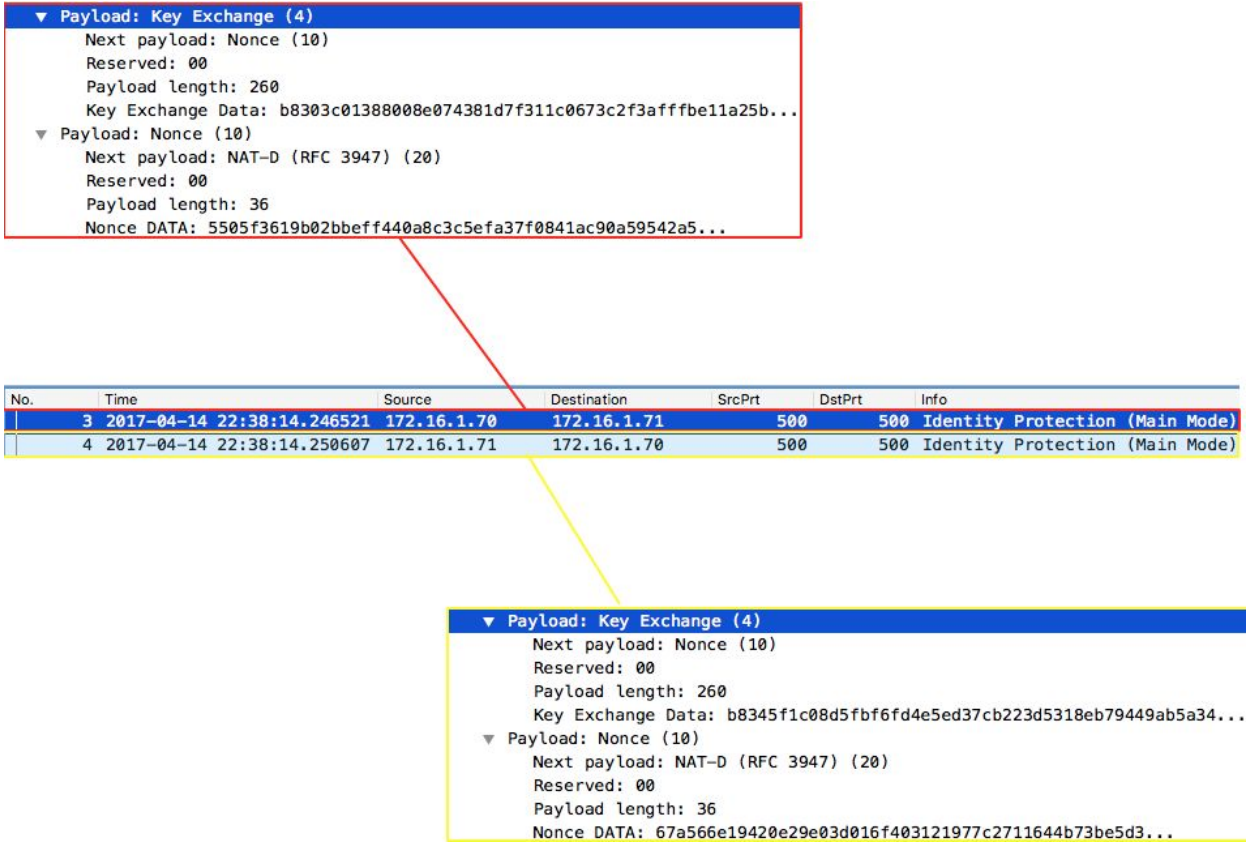
IKE in Action

SAPIENZA
UNIVERSITÀ DI ROMA

```
▼ Payload: Security Association (1)
    Next payload: Vendor ID (13)
    Reserved: 00
    Payload length: 56
    Domain of interpretation: IPSEC (1)
  ▶ Situation: 00000001
  ▼ Payload: Proposal (2) # 0
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 44
      Proposal number: 0
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 1
    ▼ Payload: Transform (3) # 1
        Next payload: NONE / No Next Payload  (0)
        Reserved: 00
        Payload length: 36
        Transform number: 1
        Transform ID: KEY_IKE (1)
        Reserved: 0000
      ▶ IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
      ▶ IKE Attribute (t=14,l=2): Key-Length: 128
      ▶ IKE Attribute (t=2,l=2): Hash-Algorithm: SHA
      ▶ IKE Attribute (t=4,l=2): Group-Description: 2048 bit MODP group
      ▶ IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
      ▶ IKE Attribute (t=11,l=2): Life-Type: Seconds
      ▶ IKE Attribute (t=12,l=2): Life-Duration: 3600
```

IKE in Action

SAPIENZA
UNIVERSITÀ DI ROMA



IKE in Action

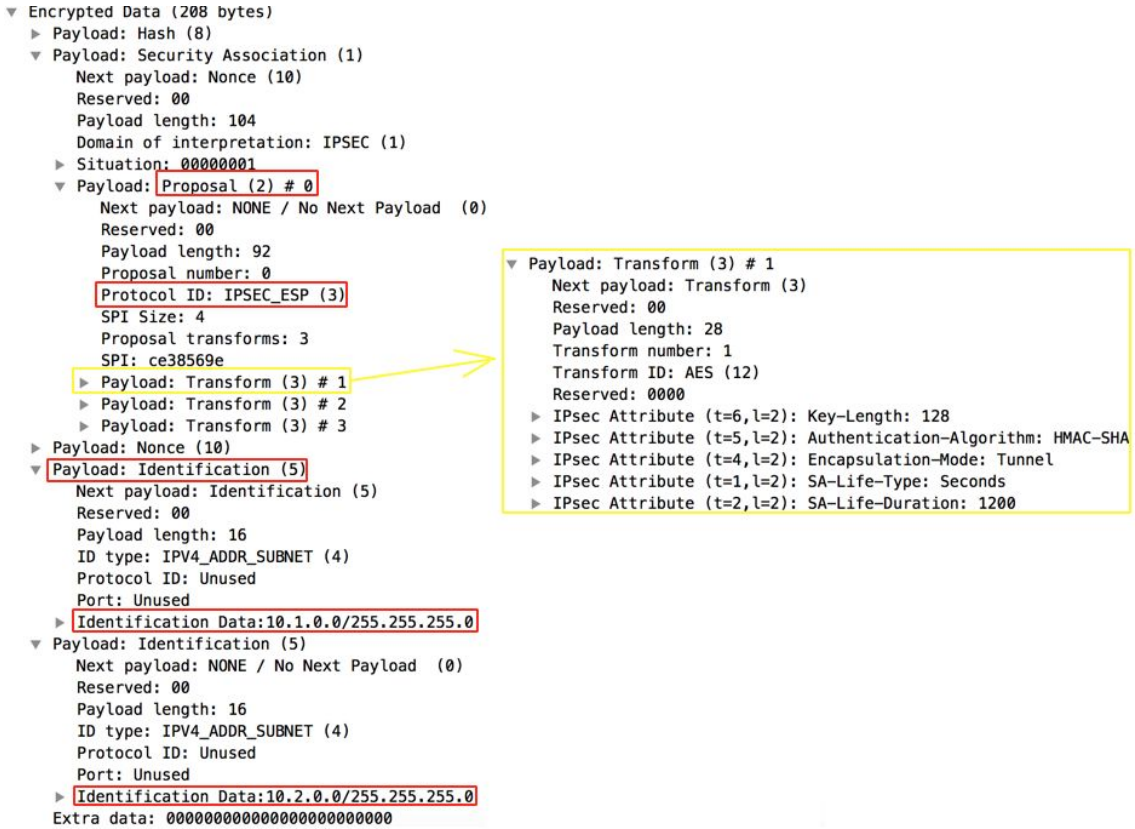
SAPIENZA
UNIVERSITÀ DI ROMA

```
▼ Internet Security Association and Key Management Protocol
    Initiator SPI: 751b83775c20d140
    Responder SPI: 5c3757dc0cafc014
    Next payload: Identification (5)
  ▶ Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ▼ Flags: 0x01
      .... ...1 = Encryption: Encrypted
      .... ..0. = Commit: No commit
      .... .0.. = Authentication: No authentication
    Message ID: 0x00000000
    Length: 108
```

```
▼ Encrypted Data (80 bytes)
  ▼ Payload: Identification (5)
      Next payload: Hash (8)
      Reserved: 00
      Payload length: 27
      ID type: FQDN (2)
      Protocol ID: Unused
      Port: Unused
    ▶ Identification Data:moon.strongswan.org
  ▼ Payload: Hash (8)
      Next payload: Notification (11)
      Reserved: 00
      Payload length: 24
      Hash DATA: 14ff218df52306c134b5431bd88e3a2809fee996
  ▼ Payload: Notification (11)
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 28
      Domain of interpretation: IPSEC (1)
      Protocol ID: ISAKMP (1)
      SPI Size: 16
      Notify Message Type: INITIAL-CONTACT (24578)
      SPI: 751b83775c20d1405c3757dc0cafc014
      Notification DATA: <MISSING>
  Extra data: 00
```

IKE in Action

SAPIENZA
UNIVERSITÀ DI ROMA



IKE in Action

SAPIENZA
UNIVERSITÀ DI ROMA

```
▼ Payload: Security Association (1)
    Next payload: Nonce (10)
    Reserved: 00
    Payload length: 52
    Domain of interpretation: IPSEC (1)
  ▶ Situation: 00000001
```

```
▼ Payload: Proposal (2) # 0
    Next payload: NONE / No Next Payload  (0)
    Reserved: 00
    Payload length: 40
    Proposal number: 0
    Protocol ID: IPSEC_ESP (3)
    SPI Size: 4
    Proposal transforms: 1
    SPI: c04af751
  ▼ Payload: Transform (3) # 1
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 28
      Transform number: 1
      Transform ID: AES (12)
      Reserved: 0000
    ▶ IPsec Attribute (t=6,l=2): Key-Length: 128
    ▶ IPsec Attribute (t=5,l=2): Authentication-Algorithm: HMAC-SHA
    ▶ IPsec Attribute (t=4,l=2): Encapsulation-Mode: Tunnel
    ▶ IPsec Attribute (t=1,l=2): SA-Life-Type: Seconds
    ▶ IPsec Attribute (t=2,l=2): SA-Life-Duration: 1200
▶ Payload: Nonce (10)
▼ Payload: Identification (5)
    Next payload: Identification (5)
    Reserved: 00
    Payload length: 16
    ID type: IPV4_ADDR_SUBNET (4)
    Protocol ID: Unused
    Port: Unused
  ▶ Identification Data:10.1.0.0/255.255.255.0
▼ Payload: Identification (5)
    Next payload: NONE / No Next Payload  (0)
    Reserved: 00
    Payload length: 16
    ID type: IPV4_ADDR_SUBNET (4)
    Protocol ID: Unused
    Port: Unused
  ▶ Identification Data:10.2.0.0/255.255.255.0
  Extra data: 00000000000000000000000000000000
```

IKE in Action

SAPIENZA
UNIVERSITÀ DI ROMA