Security Protocols: IPSec

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Corso di Sicurezza nelle reti, a.a. 2009/2010

http://www.tlc.unipr.it/veltri

Introduzione ad IPSec

- IPSec rappresenta un'architettura aperta definita (RFC 4301) dall'IPSec Working Group dell'IETF come framework per garantire la sicurezza al network layer e/o ai protocolli di livello superiore dello stack TCP/IP
  - **fornisce una serie di funzionalità (Security Services) orientate a garantire la Sicurezza su traffico di tipo IP**
  - **può essere utilizzato per proteggere uno o più percorsi tra coppie di host, di router o coppie miste host/router, o VPN (Virtual Private Network)**
  - **può essere implementato sia su un host che su un router (security gateway)**
- Il supporto di IPSec è raccomandato per IPv4, mandatorio per IPv6

Introduzione ad IPSec (cont.)

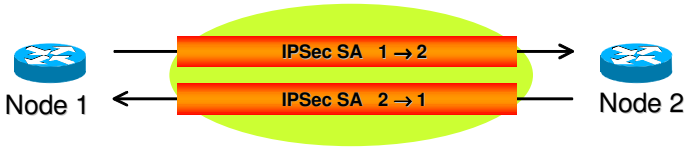
- IPSec permette di offrire sicurezza della comunicazione in modo trasparente
  - **trasparenza rispetto ai nodi intermedi ai nodi IPSec**
  - **trasparenza rispetto alle applicazioni e ai protocolli di trasporto**
    - molto utile in presenza di applicazioni legacy
    - servizio offerto contemporaneamente a tutte le applicazioni
  - **trasparenza rispetto ai nodi terminali, nel caso IPSec sia router-to-router o router-to-host**
    - molto utile in presenza di nodi legacy
    - 1 nodo IPSec può proteggere contemporaneamente più host terminali
- L'implementazione di IPSec può avvenire:
  - **IP stack**
    - mediante modifica del codice sorgente IP
  - **Bump-in-the-stack**
    - strato IP inalterato; IPSec viene implementato nello stack tra il protocollo IP ed il local network driver
  - **Bump-in-the-wire**
    - viene impiegata una scheda con crypto processor separata

Protocolli di IPSec

- IP Authentication Header (AH)
  - **protocollo utilizzato per lo scambio di dati tra sorgente e destinazione che fornisce:**
    - data origin authentication
    - data integrity
    - opzionalmente replay protection
- IP Encapsulating Security Payload (ESP)
  - **protocollo utilizzato per lo scambio di dati tra sorgente e destinazione che fornisce:**
    - data confidentiality
    - opzionalmente data origin authentication, data integrity e replay protection
- Internet Key Exchange (IKE)
  - **basato su Internet Security Association and Key Management Protocol (ISAKMP)**
  - **protocollo di controllo e gestione di una SA tra nodi IPSec che permette di:**
    - instaurare automaticamente connessioni IPSec (SA) tra coppie di nodi
    - negoziare le chiavi di crittografia associate

Security Association (SA)

- Le SA sono essenziali in IPSec, sia con AH che ESP
- Una SA identifica univocamente tutti i parametri necessari per una comunicazione sicura far due parti qualsiasi
  - **identità dei partecipanti, tipo di protocollo (AH, ESP), algoritmi di crittografia ed autenticazione utilizzati, etc.**
- Rappresenta una connessione logica unidirezionale (simplex) tra due sistemi IPSec
  - **nel caso di comunicazione bidirezionale è necessario instaurare almeno due SA**

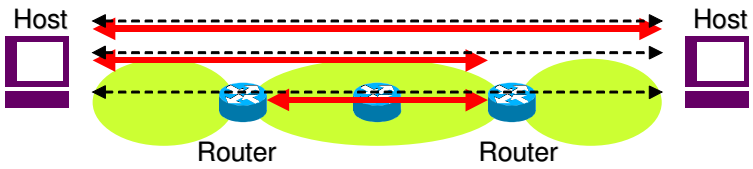


SA (cont.)

- Una SA è identificata da 3 parametri:
  - **SPI (Security Parameter Index)**
  - **IP address di destinazione**
  - **Sec protocol (AH, ESP)**
- Una SA è caratterizzata dai seguenti parametri:
  - **AH info (algo, IV, keys)**
  - **ESP info (algos, IV, keys)**
  - **IPSec mode**
  - **sequence number**
  - **anti-replay window**
  - **lifetime**
  - **max MTU**
- E' stato standardizzato un protocollo di creazione e gestione delle SA detto Internet Security Association and Key Management Protocol (ISAKMP)

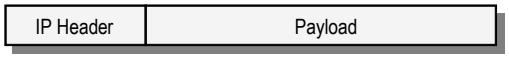
Configurazioni di IPSec

- IPSec (AH ed ESP) può essere impiegato per creare comunicazioni "sicure" di tipo
  - **host-to-host**
    - scenario end-to-end, in alternativa a soluzioni a livello applicativo/trasporto
  - **host-to-router**
    - scenario host-to-network, spesso riferito come "road-warrior"
  - **router-to-router**
    - scenario network-to-network, spesso riferito come VPN/IPSec

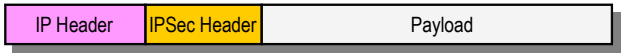


Transport & Tunnel Mode

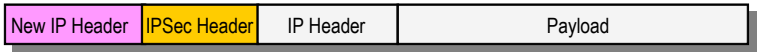
- Pacchetto originale (no IPSec)



- Transport Mode
  - **viene mantenuto l'header del datagramma IP originale, seguito dall'header IPSec e dal payload originale**
  - **è impiegato tra i due end point di una comunicazione fornendo quindi una protezione da estremo a estremo lungo l'intero percorso**

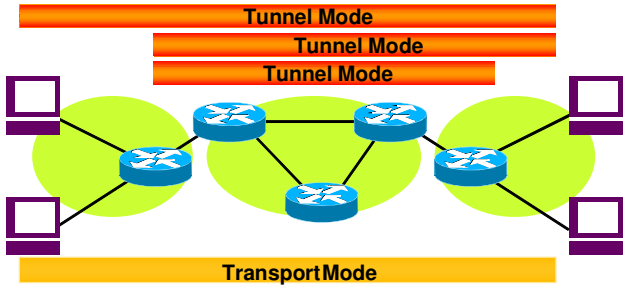


- Tunnel Mode
  - **viene utilizzato un nuovo header IP con Source e Destination address in genere differenti da quelli originari (tipicamente gli indirizzi dei security gateway)**
  - **il nuovo header è seguito dall'AH header e dall'intero datagramma IP originale**
  - **è normalmente impiegato tra due macchine di cui almeno una non rappresenta l'end point della connessione (firewall to firewall, client to firewall) fornendo quindi una protezione su di un singolo segmento del percorso**



Transport & Tunnel Mode (cont.)

- Il transport mode può essere impiegato soltanto quando sia la sorgente che la destinazione implementano IPSec



- E' possibile combinare le due modalità utilizzando ricorsivamente più istanze del medesimo protocollo (AH o ESP) o combinazioni dei due
  - **adiacenze di trasporto**
  - **tunnel iterato**

Transport & Tunnel Mode (cont.)

- E' possibile combinare le due modalità utilizzando ricorsivamente più istanze del medesimo protocollo (AH o ESP) o combinazioni dei due
  - **adiacenze di trasporto**
  - **tunnel iterato**
- Tramite combinazioni delle due modalità e dei due protocolli (AH e ESP) è possibile selezionare maggiormente il livello di granularità offerto dai Security Services
- Esempi:
  - **adiacenze di trasporto AH e ESP:**
    - (end-to-end) per autenticare anche header IP
  - **transport-tunnel:**
    - singolo tunnel AH per trasportare il traffico tra una coppia di security gateway
    - ESP transport per crittare il traffico di ciascuna connessione TCP tra coppie di host separati dai security gateway

Authentication Header (AH)

Authentication Header

- IP Authentication Header (RFC 4302)
- AH fornisce l'integrità e l'autenticazione dei datagrammi IP
  - **Si ottiene calcolando una funzione hash sul datagramma IP ed usando una chiave segreta di autenticazione**
- Le informazioni di autenticazione sono calcolate utilizzando tutti i campi del datagramma IP che non cambiano durante il trasporto (o che cambino in maniera prevedibile)
- Due modalità di impiego: Transport Mode e Tunnel Mode
  - **La modalità "Tunnel" protegge l'IP header originale mascherando gli indirizzi IP di sorgente e di destinazione**

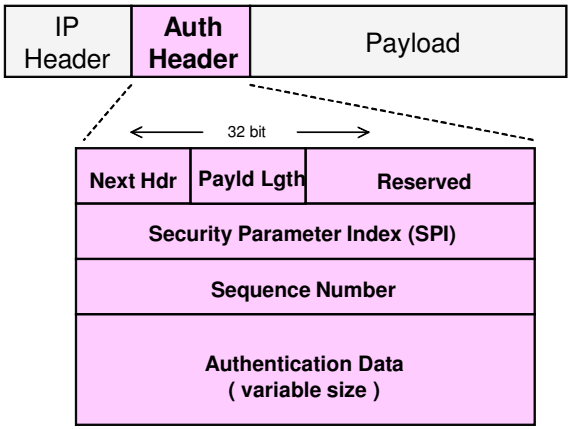
AH: Security Services offerti

- Data integrity
  - **viene assicurata in maniera connectionless (pacchetto per pacchetto) generando un Integrity Check Value che protegge l'intero datagramma IP eccetto alcuni campi mutevoli dell'header**
- Data origin authentication
  - **viene garantita firmando in maniera digitale l'Integrity Check Value**
- Replay protection
  - **è opzionale ed è realizzata impiegando un campo sequence number nell'header del pacchetto AH**
- Nella terminologia IPSec le tre distinte funzioni vengono comunemente riferite con il termine "Authentication"
- Osservazione:
  - **la mancanza di confidenzialità consente anche l'uso di IPSec su Internet anche nei paesi dove l'esportazione, l'importazione o l'uso della crittografia è regolato da leggi restrittive**

Informazione protetta da AH

- AH protegge anche tutti i campi dell'intestazione IP immutabili o mutabili in maniera prevedibile
- Immutable IP header fields (IPv4):
  - **Version**
  - **Internet Header Length**
  - **Total Length**
  - **Identification**
  - **Protocol (This should be the value for AH.)**
  - **Source Address**
  - **Destination Address (without loose or strict source routing)**
- Mutable but predictable IP header fields (IPv4):
  - **Destination Address (with loose or strict source routing)**
- Mutable IP header fields (IPv4) - zeroed prior to ICV calculation of AH:
  - **Type of Service (TOS)**
  - **Flags**
  - **Fragment Offset**
  - **Time to Live (TTL)**
  - **Header Checksum**

Authentication Header

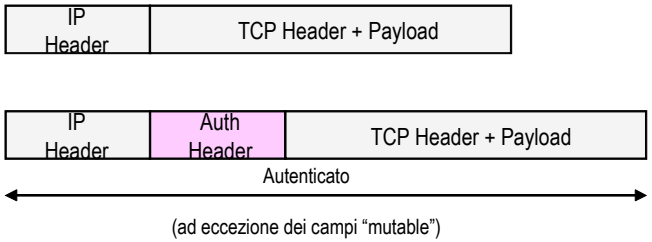


Descrizione del AH

- Next header
  - **indica il tipo di protocollo trasportato nel campo payload**
- Payload length
  - **campo di 8 bit che specifica la lunghezza del pacchetto AH in 32 bit word, meno due (compatibilità vecchia specifica di AH)**
    e.g. se authentication data = HMAC-md5-96, allora PL= 3+3-2=4
- Reserved
  - **campo riservato per scopi futuri ed attualmente riempito di zeri**
- Security Parameter Index (SPI)
  - **identificativo numerico a 32 bit che identifica una SA e tutti i suoi attributi (security protocol, algoritmi utilizzati, le chiavi e la durata di validità delle chiavi)**
- Sequence number
  - **contatore che viene incrementato ogni volta che un pacchetto viene spedito alla medesima destinazione usando la stessa SA**
- Authenication data
  - **contiene un Integrity Check Value (ICV) calcolato sulla parte rimanente del pacchetto e sulla parte fissa dell'header del datagramma IP (header originale/transport mode o nuovo header/tunnel mode)**
  - **può includere un padding per riportare la lunghezza dell'header del pacchetto AH ad un multiplo intero di 32 bit (IPv4) o 64 bit (IPv6)**

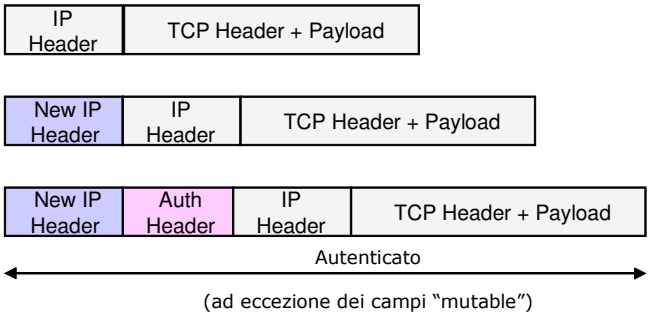
AH - Transport Mode

- Viene mantenuto l'header del datagramma IP originale, seguito dall'AH header e dal payload originale
- L'intero datagramma IP, eccetto alcuni campi dell'header, viene autenticato
- Qualsiasi modifica al contenuto del datagramma, eccetto quelle che avvengono nei campi mutevoli dell'header IP, viene rilevata
- Tutti i dati sono trasportati dal datagramma in chiaro



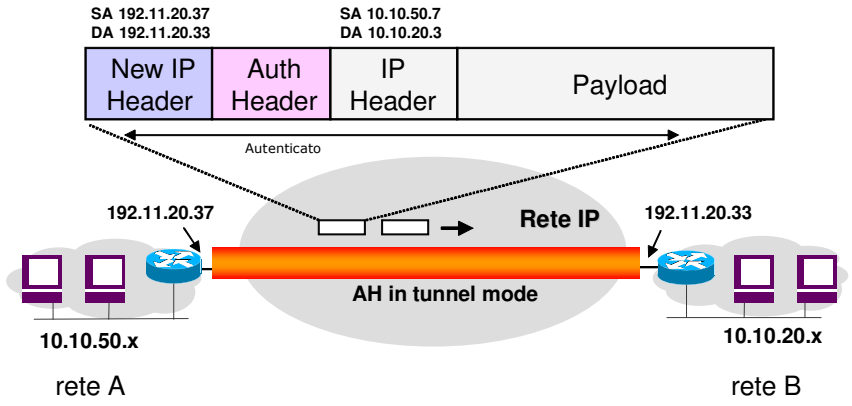
AH - Tunnel Mode

- Aggiunto un nuovo header con src e dest address in genere differenti da quelli originari (tipicamente l'indirizzo di un security gateway)
- Il nuovo header è seguito dall'AH header e dal datagramma IP originale
- viene autenticato l'intero nuovo datagramma IP, eccetto alcuni campi mutevoli del nuovo header
- Tutti i dati sono trasportati dal datagramma in chiaro



AH- Tunnel Mode: Esempio

- AH in tunnel mode
- Due gateway autenticano tutto il traffico trasportato



Encapsulating Security Paylod (ESP)

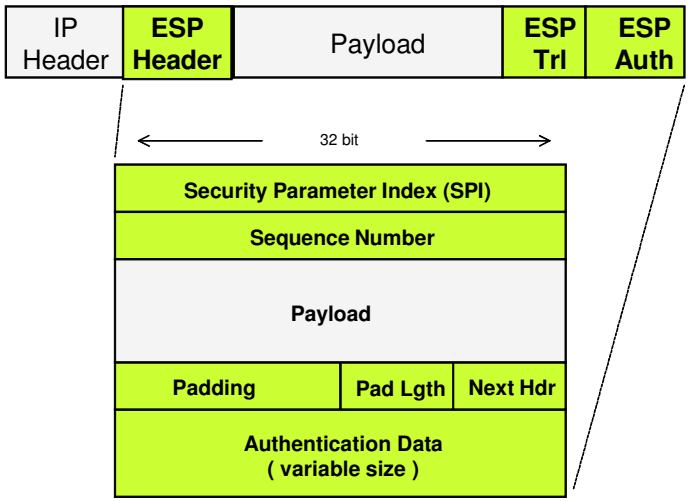
Encapsulating Security Paylod

- IP Encapsulating Security Payload (RFC 4303)
- ESP fornisce vari servizi di sicurezza tra cui la confidenzialità
- Non è specificato un particolare algoritmo di cifratura
- Due modalità di impiego: Transport mode e Tunnel Mode
- La modalità "Tunnel" protegge l'IP header originale mascherando gli indirizzi IP di sorgente e di destinazione

ESP: Security Services offerti

- Data confidentiality
  - **viene assicurata mediante meccanismi di encryption/decryption dei dati trasmessi, avvalendosi dell'impiego di una chiave simmetrica utilizzata da entrambi gli attori della comunicazione**
- Data integrity
  - **è opzionale, come in AH viene assicurata in maniera connectionless (pacchetto per pacchetto) generando un Integrity Check Value, ma copre una porzione differente del datagramma IP**
- Data origin authentication
  - **è opzionale, come in AH viene garantita firmando in maniera digitale l'Integrity Check Value**
- Replay protection
  - **è opzionale ed utilizza un sequence number**

Encapsulating Security Paylod

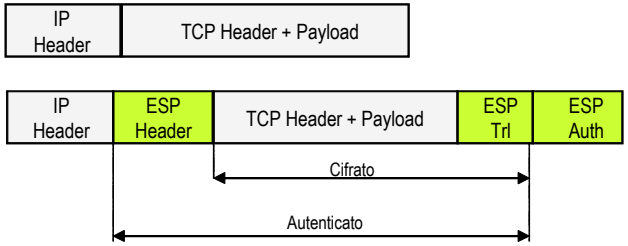


Formato del pacchetto ESP

- Security Parameter Index (SPI)
  - **identificativo numerico a 32 bit che identifica una SA e tutti i suoi attributi (security protocol, algoritmi utilizzati, le chiavi e la durata di validità delle chiavi)**
- Sequence number
  - **contatore che viene incrementato ogni volta che un pacchetto viene spedito alla medesima destinazione usando la stessa SA**
- Payload data
  - **rappresenta l'area destinata al trasporto dei dati (protocollo di livello superiore/transport mode o datagramma IP/tunnel mode)**
- Padding
  - **(0-255 bytes) riempimento di lunghezza variabile necessario ad alcuni algoritmi che richiedono che i dati da criptare abbiano una lunghezza multipla di un valore fissato**
- Pad lenght
  - **indica la lunghezza del campo riempimento**
- Next header
  - **indica il tipo di protocollo trasportato nel campo payload**
- Authentication data
  - **campo opzionale che contiene un Integrity Check Value (ICV) calcolato sulla rimanente parte del pacchetto ESP dopo che lo stesso è stato criptato**
  - **la lunghezza varia a seconda dell'algoritmo di autenticazione utilizzato**

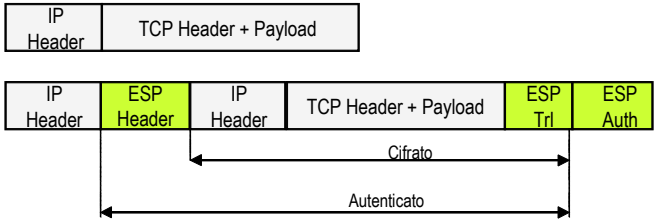
ESP - Transport Mode

- viene mantenuto l'header del datagramma IP originale, seguito dall'ESP Header, dal Payload originale, l'ESP Trailer e l'ESP Auth
- vengono crittati esclusivamente il Payload del datagramma IP originale e l'ESP Trailer
- vengono autenticati l'ESP Header, l'IP Payload e l'ESP Trailer
- l'header IP non viene né crittato né autenticato, gli indirizzi IP sorgente e destinazione originali restano in chiaro nel transito e visibili da un eventuale hacker

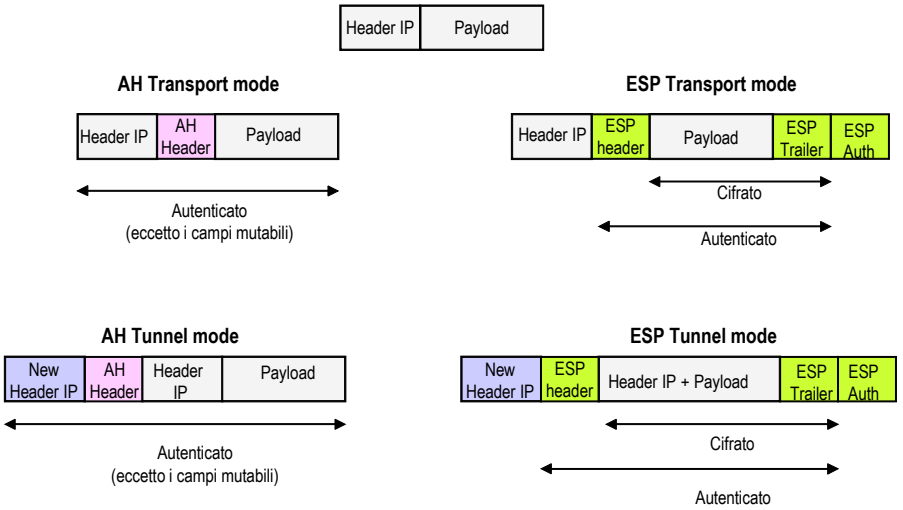


ESP - Tunnel Mode

- viene utilizzato un nuovo Header IP con Source e Destination address in genere differenti da quelli originali
- l'intero datagramma IP originale (IP Header ed IP Payload) e l'ESP Trailer vengono crittati
- l'autenticazione viene applicata all'ESP Header, all'intero datagramma IP originale e all'ESP Trailer
- Un tipico impiego di ESP in tunnel mode è quello di nascondere gli indirizzi IP sorgente e destinazione originali realizzando un tunnel tra una coppia di security gateway (firewall/router)

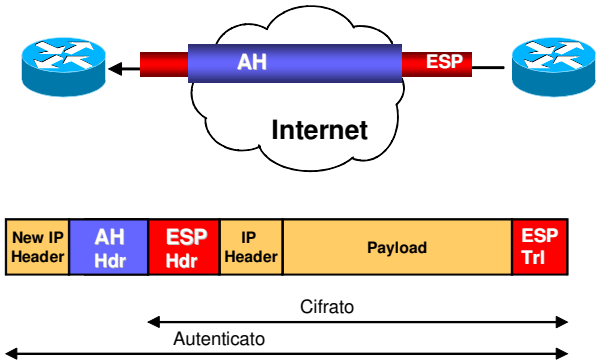


Confronto tra AH e ESP



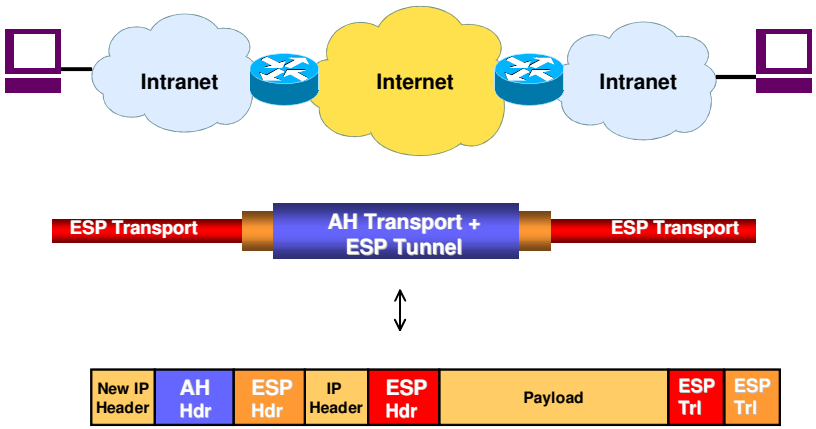
Transport & Tunnel Mode: esempio

- AH ed ESP possono essere combinati in vari modi
  - **Es: ESP in Tunnel Mode + AH in Transport mode**



Transport & Tunnel Mode: esempio

- Esempio End-to-End



IPSec e la crittografia

- IPSec implementa lo stato dell'arte della crittografia avvalendosi dei comuni algoritmi standard
- Rimane aperto a futuri sviluppi
- Ciascun algoritmo è impiegato nell'ambito più opportuno
  - **Cifratura simmetrica a chiave segreta per il data bulk**
  - **Cifratura a chiave pubblica (RSA) per lo scambio della chiave di sessione**
  - **Diffie-Helmann per la generazione di chiavi di sessione**
  - **Trasformazioni Hash**

Problemi con IPSec

- L'impiego di funzionalità di NAT (Network Address Translation) è incompatibile con l'utilizzo del protocollo AH in quanto sostituendo l'indirizzo IP il datagramma non verrebbe più autenticato
- L'impiego di firewall di tipo packet filtering tradizionali (stateless/stateful inspection) è incompatibile con l'utilizzo del protocollo ESP:
  - **ESP nella modalità transport mode critta il payload del datagramma IP rendendo impossibile un controllo di tipo stateful**
  - **ESP nella modalità tunnel mode critta l'intero datagramma IP rendendo impossibile un controllo di tipo stateful o stateless**

Distribuzione delle chiavi

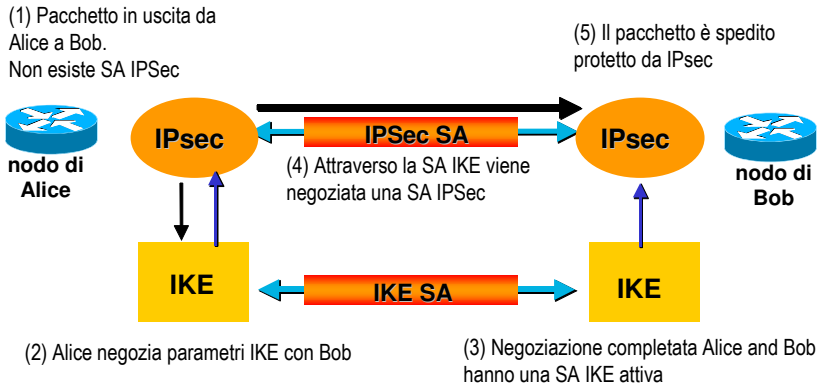
- In generale per una comunicazione bidirezionale tra due nodi sono necessarie 4 chiavi segrete
  - **AH e ESP in entrambe le direzioni**
- La negoziazione e la distribuzione delle chiavi può essere effettuata attraverso due modalità:
  - **distribuzione manuale delle chiavi**
    - soluzione non scalabile
  - **distribuzione automatica delle chiavi**
    - tramite protocollo ISAKMP/IKE

IKEv2

Internet Key Exchange (IKE)

- IPSec necessita la realizzazione tra gli end-point di una Security Association (SA):
  - **una SA contiene tutte le informazioni per l'elaborazione del traffico IPSec:**
    - l'algoritmo di cifratura
    - l'algoritmo di autenticazione
    - chiavi
    - etc.
- IKEv2 (RFC 4306) è un meccanismo per la negoziazione negoziazione/creazione automatica di una SA tra 2 nodi IPsec
  - **permette la creazione delle chiavi e di altro materiale di crittografico in modo protetto**
  - **definisce le modalità di utilizzo e gestione delle stesse**

IKE: modello



- Periodicamente le SA vengono rinegoziate per modificare le chiavi
  - **prima che scadano le SA attualmente attive**
- La IPSec SA in IKE viene anche riferita come CHILD SA

IKEv1 Phase 1 and Phase 2

- IKE coinvolge due o più end point system di una SA in fase di instaurazione secondo un approccio strutturato in due fasi:
  - **Phase 1**
    - avviene la negoziazione di una "master secret" dalla quale dovranno successivamente essere derivate le chiavi per proteggere il traffico IP
    - vengono stabilite una IKE_SA e le chiavi per proteggere i messaggi IKE scambiati nella Phase 2
    - poiché la comunicazione in questa fase avviene su connessioni ancora insicure, per lo scambio di messaggi si fa utilizzo di crittografia a chiave pubblica (DH)
    - richiede il computo di un maggior numero di operazioni crittografiche rispetto alla Phase 2
    - supporta successive e multiple istanze della Phase 2 e quindi viene eseguita non di frequente
    - viene anche negoziata la prima CHILD_SA (per AH o ESP)

IKEv1 Phase 1 and Phase 2 (cont.)

(cont.)

- **Phase 2**
  - avviene la negoziazione di CHILD_SA e delle chiavi necessarie alla protezione del traffico di dati (AH o ESP)
  - La negoziazione avviene per mezzo di messaggi IKE protetti dalla IKE_SA generata nella Phase 1
  - entrambe le parti possono iniziare la negoziazione
  - richiede uno sforzo computazionale inferiore rispetto alla Phase 1
  - può essere eseguita di frequente (ogni due/tre minuti) per effettuare il refresh delle chiavi crittografiche

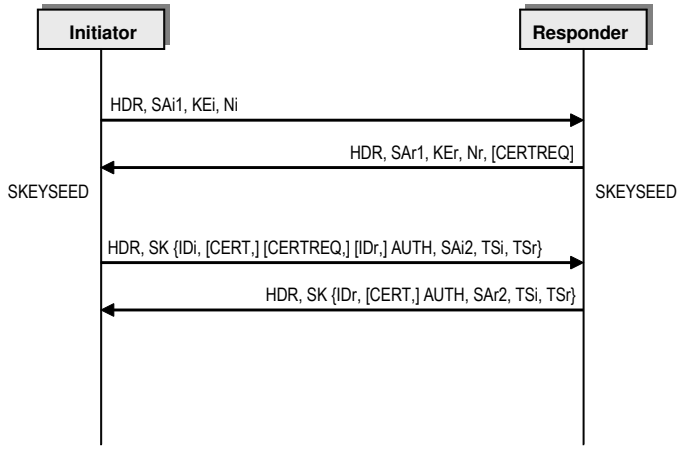
IKE Exchanges

- All IKE communications consist of pairs of messages
  - **a request and a response (with retransmission)**
  - **the pair is called an "exchange"**
- The first exchange is IKE_SA_INIT
  - **negotiates security parameters for the IKE_SA, sends nonces, and sends Diffie-Hellman values**
- The second exchange is IKE_AUTH
  - **transmits identities, proves knowledge of the secrets corresponding to the two identities, and sets up an SA for the first AH and/or ESP CHILD_SA**
  - **parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange**
- In IKEv1 these 2 exchanges (4 messages) are known as Phase1
- Subsequent exchanges are CREATE_CHILD_SA
  - **creates a CHILD_SA**
  - **MAY be initiated by either end of the IKE_SA**
- In IKEv1 this exchange was referred to as a Phase2

IKE Exchanges (cont.)

- Other exchanges are INFORMATIONAL
  - **deletes an SA, reports errors, etc.**

Initial Exchanges (IKE_SA_INIT and IKE_AUTH)



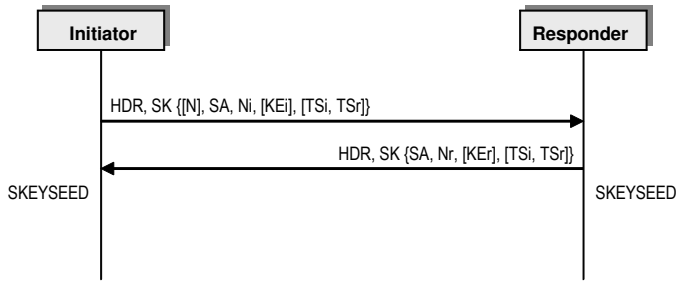
Initial Exchanges

- Communication using IKE always begins with IKE_SA_INIT and IKE_AUTH exchanges (known in IKEv1 as Phase 1)
  - **HDR contains the SPIs, version numbers, and flags**
  - **SA states the cryptographic algorithms for the IKE_SA**
  - **The KE contains the Diffie-Hellman value**
  - **Ni and Nr are nonce values**
  - **SKEYSEED is the DH secret from which all keys are derived for that IKE_SA**
    - all but the headers of all the messages that follow are encrypted SK{·} and integrity protected
    - the keys used for the encryption and integrity protection are derived from SKEYSEED and are known as SK_e (encryption) and SK_a
    - a separate SK_e and SK_a is computed for each direction
    - another quantity SK_d is derived and used for derivation of further keying material for CHILD_SAs

Initial Exchanges (cont.)

- **The initiator and responder assert their identities with the ID payload**
- **AUTH payload is the proof of knowledge of the secret corresponding to ID and is used to integrity protect the contents of the message**
- **Optionally, messages 3 and 4 MAY include a certificate, or certificate chain providing evidence that the key used to compute a digital signature belongs to the name in the ID payload**
- **The optional payloads IDr (for initiator) and IDi (for responder) enable both entities to specify which peer's identities they wants to talk to**
- **The optional payloads TSi and TSr report the proposed traffic selectors**
  - IP packet "protect" selectors are stored in a Security Policy Database (SPD)
- **The N payload identifies the SA being rekeyed (only in case the exchange is rekeying an existing SA)**

CREATE_CHILD_SA Exchange



CREATE_CHILD_SA Exchange

- This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKEv1
- Either endpoint may initiate a CREATE_CHILD_SA exchange
  - **the term "initiator" refers to the endpoint initiating this exchange**
- Request MAY optionally contain a KE payload for an additional Diffie-Hellman exchange to enable stronger guarantees of forward secrecy for the CHILD_SA

Generating Keying Material

- In the context of the IKE_SA, four cryptographic algorithms are negotiated
  - **an encryption algorithm**
  - **an integrity protection algorithm**
  - **a Diffie-Hellman group**
  - **a pseudo-random function (prf)**
- The pseudo-random function is used for the construction of keying material for all of the cryptographic algorithms used in both the IKE_SA and the CHILD_Sas
- prf(K,S) generates fixed length bit string
- prf+(K,S) = p1 | p2 | .. | pi | ..
  - **p1 = prf(K,S|0x01)**
  - **..**
  - **p_i = prf(K,p_{i-1}|S|0x0i)**

Generating Keying Material (cont.)

- SKEYSEED is calculated from the nonces exchanged during the IKE_SA_INIT exchange and the Diffie-Hellman shared secret
- SKEYSEED is used to calculate seven other secrets
  - **SK_d used for deriving new keys for the CHILD_SAs established with this IKE_SA**
  - **SK_ai and SK_ar used as a key to the integrity protection algorithm for authenticating the component messages of subsequent exchanges**
  - **SK_ei and SK_er used for encrypting (and of course decrypting) all subsequent exchanges**
  - **SK_pi and SK_pr, which are used when generating an AUTH payload**
- As follows:
  - **SKEYSEED = prf(Ni | Nr, g^ir)**
  - **{SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr } = prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr)**

Authentication of the IKE_SA

- The signature or MAC will be computed using algorithms dictated by the type of key used by the signer, and specified by the Auth Method field in the Authentication payload
- Data to be signed start with the first octet of the first SPI in the header and end with the last octet of the last payload
  - **for the responder, appended to this are the initiator's nonce Ni and the value prf(SK_pr,IDr') where IDr' is the responder's ID payload excluding the fixed header**
  - **for the initiator, appended to this are the responder's nonce Nr, and the value prf(SK_pi,IDi')**
- In case of shared secret
  - **AUTH = prf(prf(Shared Secret,"Key Pad for IKEv2"), <data>)**
    - the pad string is added so that if the shared secret is derived from a password, the IKE implementation can store the value prf(Shared Secret,"Key Pad for IKEv2")

EAP Methods

- In addition to authentication using public key signatures and shared secrets, IKE supports authentication using EAP (RFC 3748)
  - **typically, these methods are asymmetric (designed for a user authenticating to a server), and they may not be mutual**
  - **for this reason, these protocols are typically used to authenticate the initiator to the responder and MUST be used in conjunction with a public key signature based authentication of the responder to the initiator**