IPsec

Scienze dell'Informazione - Cesena
Corso di Sicurezza A.A. 2006/2007
Antonio Nardelli

Introduzione

- IPsec (IP SECurity) è una famiglia di protocolli dell'IETF che ha lo scopo di rendere più sicure le comunicazioni che utilizzano il protocollo IP.

- È un estensione del protocollo IP che fornisce sicurezza a livello IP ed ai livelli superiori. È stato sviluppato prima all'interno dello standard IPv6 ed in seguito inserito in Ipv4. L'architettura di IPsec viene descritta nell'RFC2401 (seconda versione, 1998 - http://www.ietf.org/rfc/rfc2401.txt)

- Perché la necessità di una simile architettura? Come ben noto, i protocolli IP sino alla versione 4, sono stati sviluppati senza un grande riferimento alle problematiche di sicurezza. In particolare, le comunicazioni tra due host tramite IP soffrono di alcuni problemi.

Problematiche a livello IP

- **Integrità**: sebbene ogni pacchetto IP abbia un controllo di integrità tramite una checksum (CRC), gli algoritmi utilizzati sono molto deboli e non sufficienti a garantire l'integrità dei pacchetti; pertanto il ricevente non può essere sicuro che il pacchetto che riceve sia identico a quello spedito e che non sia stato modificato, volontariamente o meno, durante il percorso.
- **Autenticità**: chiunque può inviare un pacchetto ponendo come mittente (sorgente) il numero IP di un altro host (questo è di solito chiamato spoofing) pertanto il ricevente (destinatario), utilizzando solo i dati presenti negli header IP, non può essere sicuro di chi sia il mittente del pacchetto.
- **Confidenzialità**: tutto il pacchetto, ed i dati (payload) in esso trasportati, sono in chiaro, pertanto chiunque possa intercettare (detto anche sniffing) il pacchetto può leggerne il contenuto.

IPsec

- **L'architettura IPsec è stata definita allo scopo di dotare lo strato IP di meccanismi standard di sicurezza indipendenti dalle applicazioni**
- Esistono soluzioni che forniscono servizi di sicurezza a diversi livelli della pila OSI, ma tali soluzioni per la loro natura sono limitate alle loro specifiche nicchie (PGP, HTTPS, SSL, ecc.).
- Fornendo questi servizi di sicurezza a livello di network anche i livelli superiori della pila OSI (trasporto, sessione, presentazione e applicazione) ne beneficiano.
- Lo standard IPsec può essere usato tra due host (includendo anche i client), un gateway e un host o tra due gateway.
- Non è necessaria alcuna modifica all'hardware e al software di rete per "ruotare" il protocollo IPsec.
- IPsec consente la realizzazione di reti virtuali private sicure (**Secure VPN**), cioè reti sicure ritagliate su reti pubbliche e/o insicure.

IPsec

- Mutua **Autenticazione** prima e durante le comunicazioni.
- **Confidenzialità** tramite la cifratura del traffico IP.
- **Integrità** del traffico IP: viene rifiutato il traffico modificato.
- Collezione di protocolli formata da:
  - Protocolli che forniscono autenticazione e/o la cifratura del flusso di dati (AH e ESP)
  - Protocolli che implementano lo scambio delle chiavi per realizzare il flusso crittografato. (IKE)

Protocolli IPsec

- **AH** (Authentication Header)
  - Fornisce integrità, autenticazione, protezione da attacchi di tipo “replay”
- **ESP** (Encapsulating Security Payload)
  - Fornisce (in più rispetto ad AH) confidenzialità
- **IKE** (Internet Key Exchange)
  - protocollo per scambio chiavi

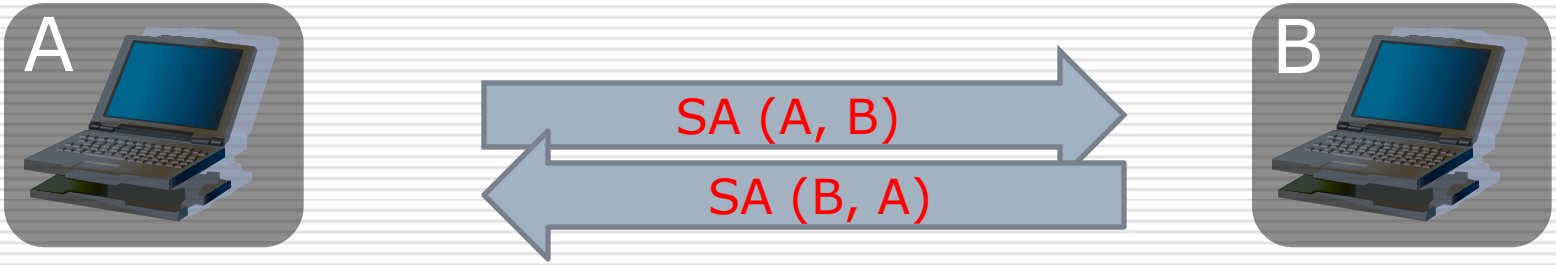
Osservazioni

- IPsec non definisce l'algoritmo di sicurezza (cifratura, ...) specifico da utilizzare ma fornisce un modo per indicare qual è l'algoritmo prescelto, **consentendo l'utilizzo degli algoritmi più consoni alle esigenze del momento**. Ad esempio **l'integrità** viene normalmente controllata facendo uso degli algoritmo **MD5 o SHA**, mentre la **crittografia** è spesso fatta mediante **DES**. Lo standard prevede comunque anche gli algoritmi IDEA, Blowfish e RC4.

- Stante la diversa complessità computazionale tra gli algoritmi a chiave pubblica e quelli simmetrici, IPsec utilizza i primi solamente nella fase dello scambio delle chiavi (autenticazione della controparte), quindi viene negoziata una chiave di sessione che verrà utilizzata dagli algoritmi tradizionali per la crittografia del canale.

Security Association (SA)

- Connessione logica **unidirezionale** tra due sistemi Ipsec
  - SPI: Security Parameter Index, identifica l'associazione localmente alla sorgente
  - IP destination address
  - Security Protocol Identifier indica la natura dei protocolli collegati all'associazione (SA relativa ad AH o ESP)
- Ad ogni SA sono associabili caratteristiche di sicurezza differenti
- Occorrono **due SA** per avere protezione completa di un canale **bidirezionale**



Database locali IPsec

- **SAD** (SA Database)
  - elenco delle SA attive e delle loro caratteristiche (algoritmi, chiavi, parametri)

- **SPD** (Security Policy Database)
  - contiene le security policy da applicare ai diversi tipi di comunicazione

SAD (SA Database)

- Elenca le SA attive e, per ciascuna SA, ne specifica le caratteristiche
  - Sequence number counter (32 bit)
  - AH information (algoritmi, chiavi, tempo di validità,...)
  - ESP information (algoritmi, chiavi, tempo di validità,...)
  - Lifetime of SA: tempo/num byte dopo il quale la SA deve essere sostituita o terminata
  - Modalità di IPsec: trasporto o tunnel

SPD (Security Policy Database)

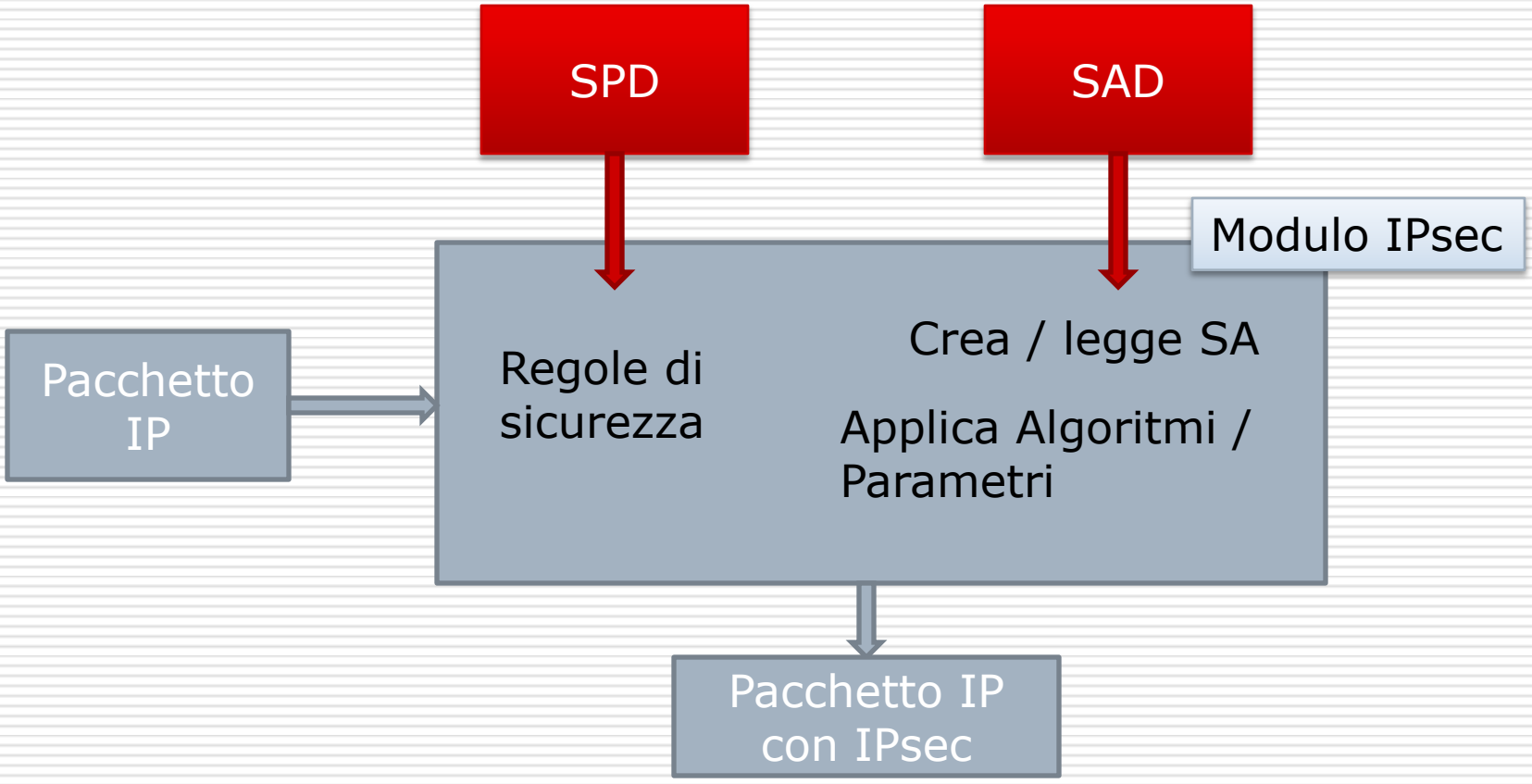
- Il Database delle Politiche di Sicurezza specifica quali servizi devono essere offerti ai diversi tipi di traffico IP
- Esempi
  - Tutto il traffico verso 192.168.2.1 deve protetto da ESP in modalità trasporto usando DES
  - Tutto il traffico FTP (TCP, porta 20) verso 192.168.2.2 deve essere protetto da ESP in modalità tunnel usando 3DES
  - Tutto il traffico verso 192.168.2.3 non deve essere protetto
- SPD è costituito da **policy entry**

Policy entry di SPD

- Una policy entry è costituita da
  - uno o piú selettori che specificano il traffico IP gestito da questa entry
  - indicazione se il matching traffic deve essere scartato, by-passare IPsec o essere soggetto a IPsec processing
  - specifica di una SA

- Esempi di selettori:
  - Indirizzo IP destinazione / sorgente
  - Livello di trasporto (ricavabile dal campo protocol dell'header IP)
  - Porta sorgente e porta destinazione
  - Tipo di protocollo incapsulato in IP (compreso AH e ESP)

Come funziona IPsec
Spedizione



Modalità trasporto

- Transport Mode
  - L'intestazione AH o ESP viene inserita dopo l'header IP originale

  - Fornisce protezione ai pacchetti del livello trasporto
  - Non protegge i campi variabili dell'header IP
  - Gli indirizzi nell'header IP non sono modificati
  - Sicurezza end-to-end
  - Non coinvolge gateway (eccezione: traffico destinato ai gateway)

Modalità tunnel

- Tunnel Mode
  - Da Wikipedia: *"Nelle reti di calcolatori, il termine tunneling si riferisce a un insieme di tecniche per cui un protocollo viene incapsulato in un protocollo dello stesso livello o di livello superiore per realizzare configurazioni particolari."*
  - Header IPsec inserito subito dopo la nuova intestazione IP. Il datagramma IP originale segue l'intestazione IPsec

  - Sempre quando almeno uno degli host è un gateway
  - Fornisce protezione all'intero pacchetto IP
  - Protegge i campi variabili (del pacchetto originale)
  - Gli indirizzi nell'header IP tunnel possono essere diversi da quelli nell'header IP originale

Transport vs Tunnel

Transport

- Pro: basso overhead (pochi bytes aggiunti), QoS minimale
- Contro: le informazioni mandate in chiaro permettono di scoprire, ad esempio, che un utente A sta inviando dati ad un utente B. Nonostante non sia possibile determinare il contenuto della comunicazione, in certi casi può essere l'indicazione di una certa azione (es. collegamento a banca)

Tunnel

- Pro: decisamente più sicuro (lo sniffing è praticamente inutile in quanto non c'è modo di risalire ai veri mittente e destinatario del pacchetto) e offre la possibilità ad una entità intermedia (ad esempio un router) di attivare IPsec sui pacchetti in transito per conto del client (facile da configurare)
- Contro: alto overhead

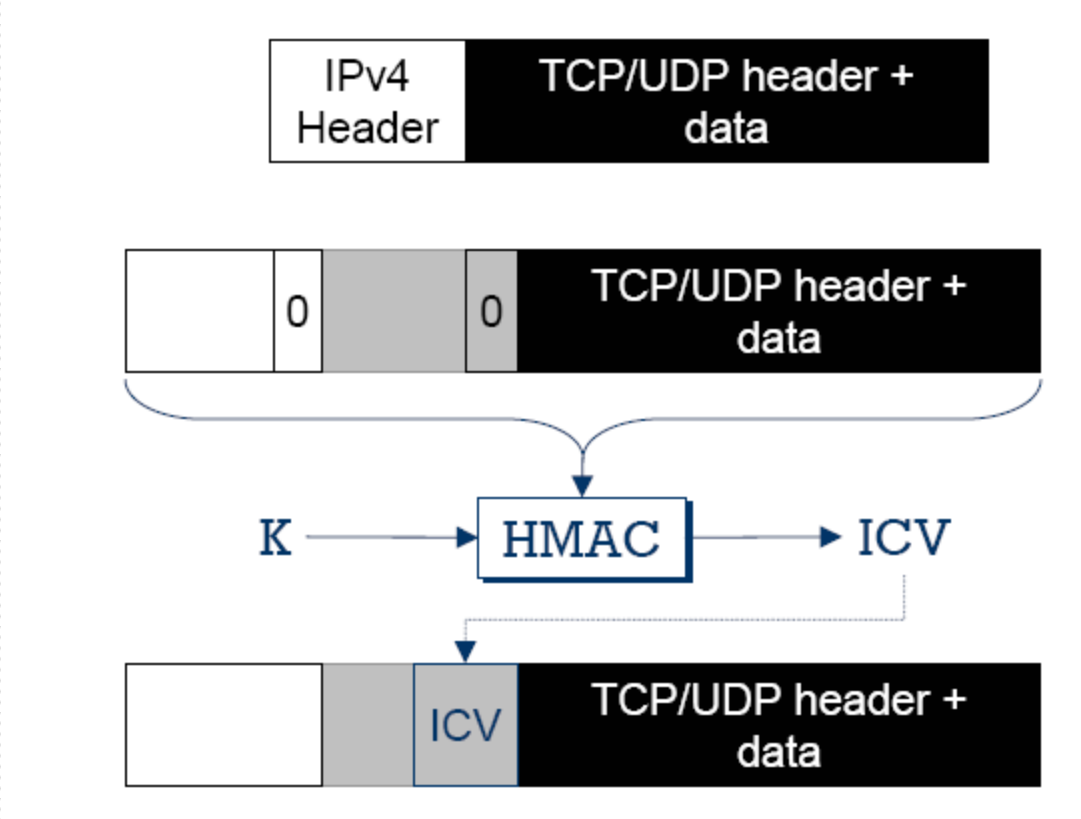
Protocollo AH

- Integrità dei dati, autenticazione del mittente e protezione da replay attack

Next Header	Length	Riservato
Security Parameters Index (SPI)		
Sequence number		
Dati per l'autenticazione (ICV)		

- SPI: identifica i parametri di sicurezza in combinazione con l'indirizzo IP. In genere è un numero pseudo-casuale che identica la security association cui fa parte questo pacchetto.
- Sequence Number: una successione di numeri monotonicamente crescenti che serve ad impedire i replay-attack.

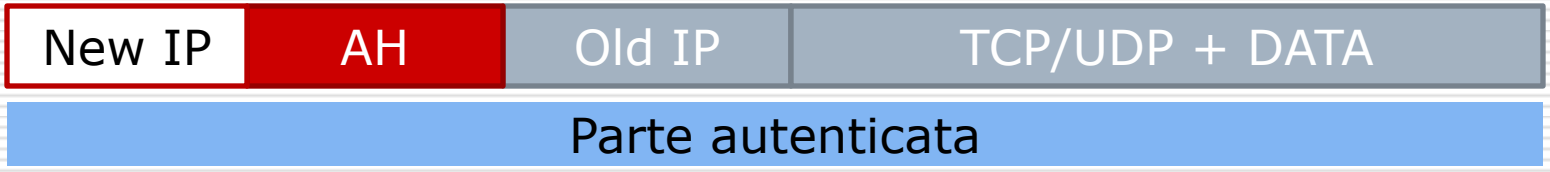
Creazione pacchetto AH



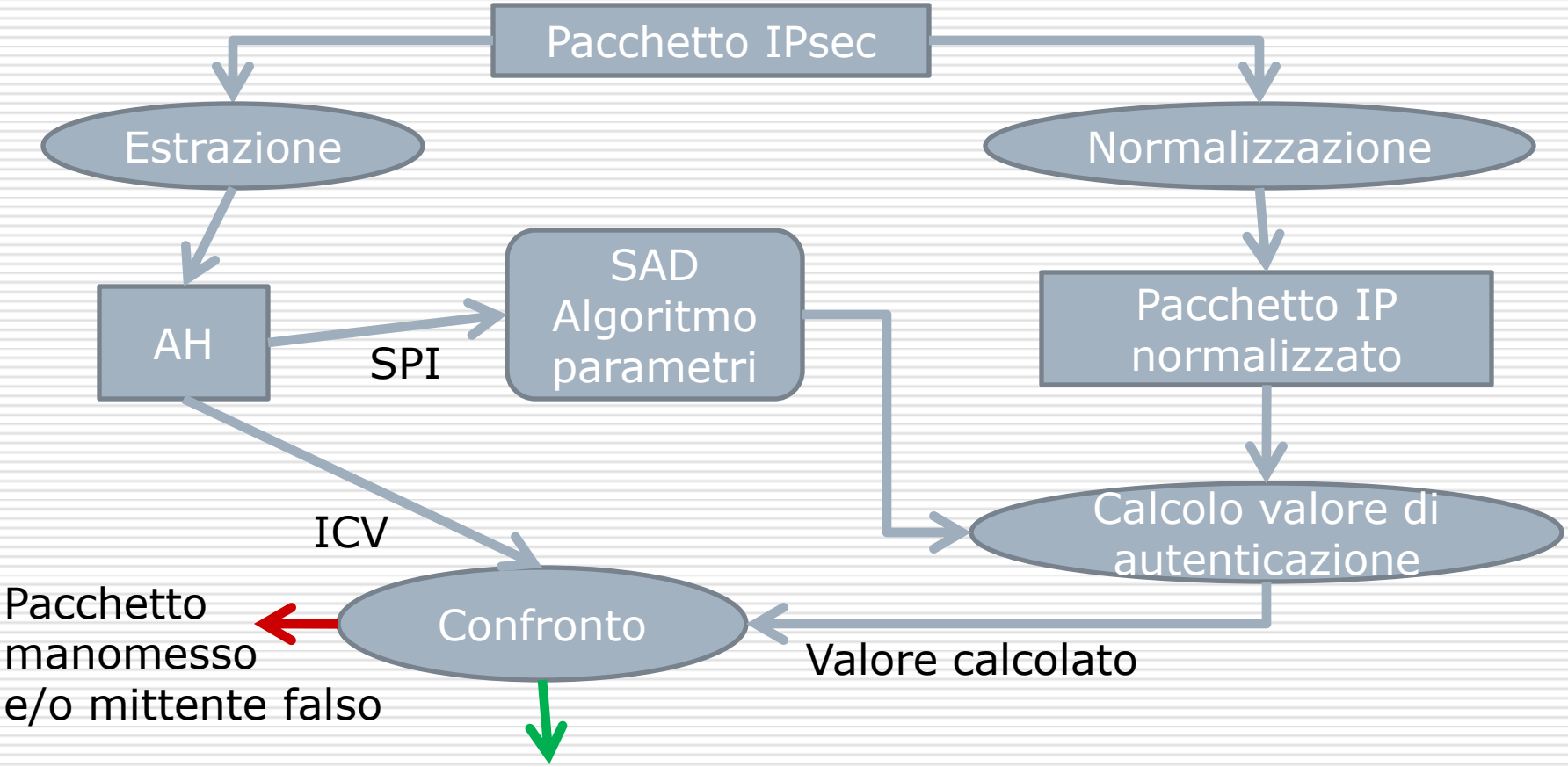
AH

- AH – Transport Mode

- AH – Tunnel Mode



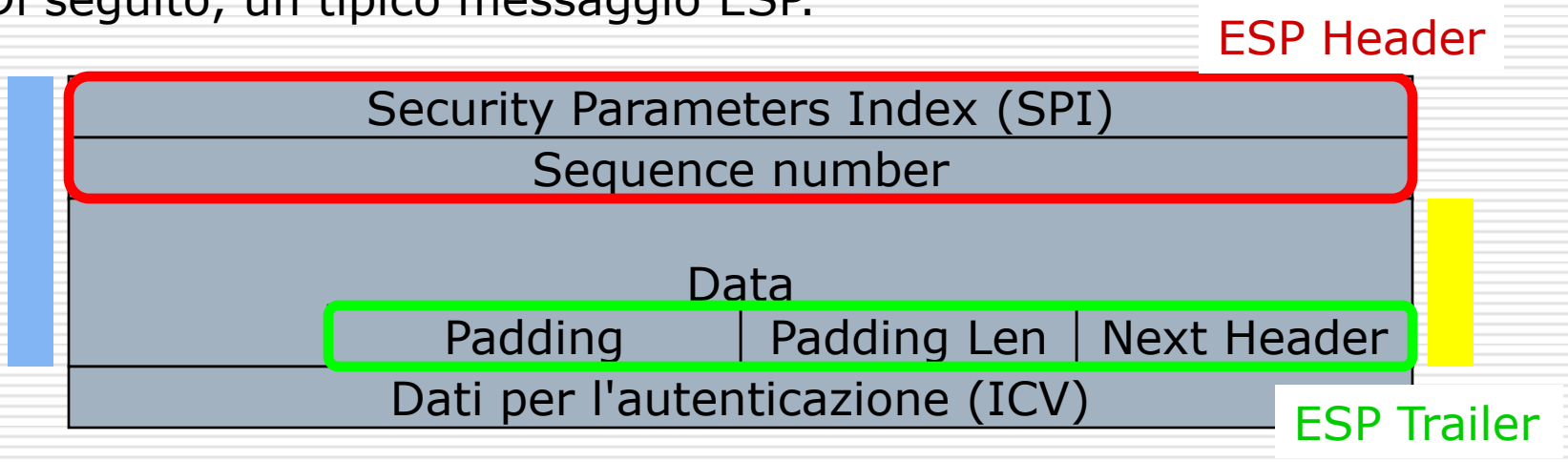
Esempio Ricezione con AH



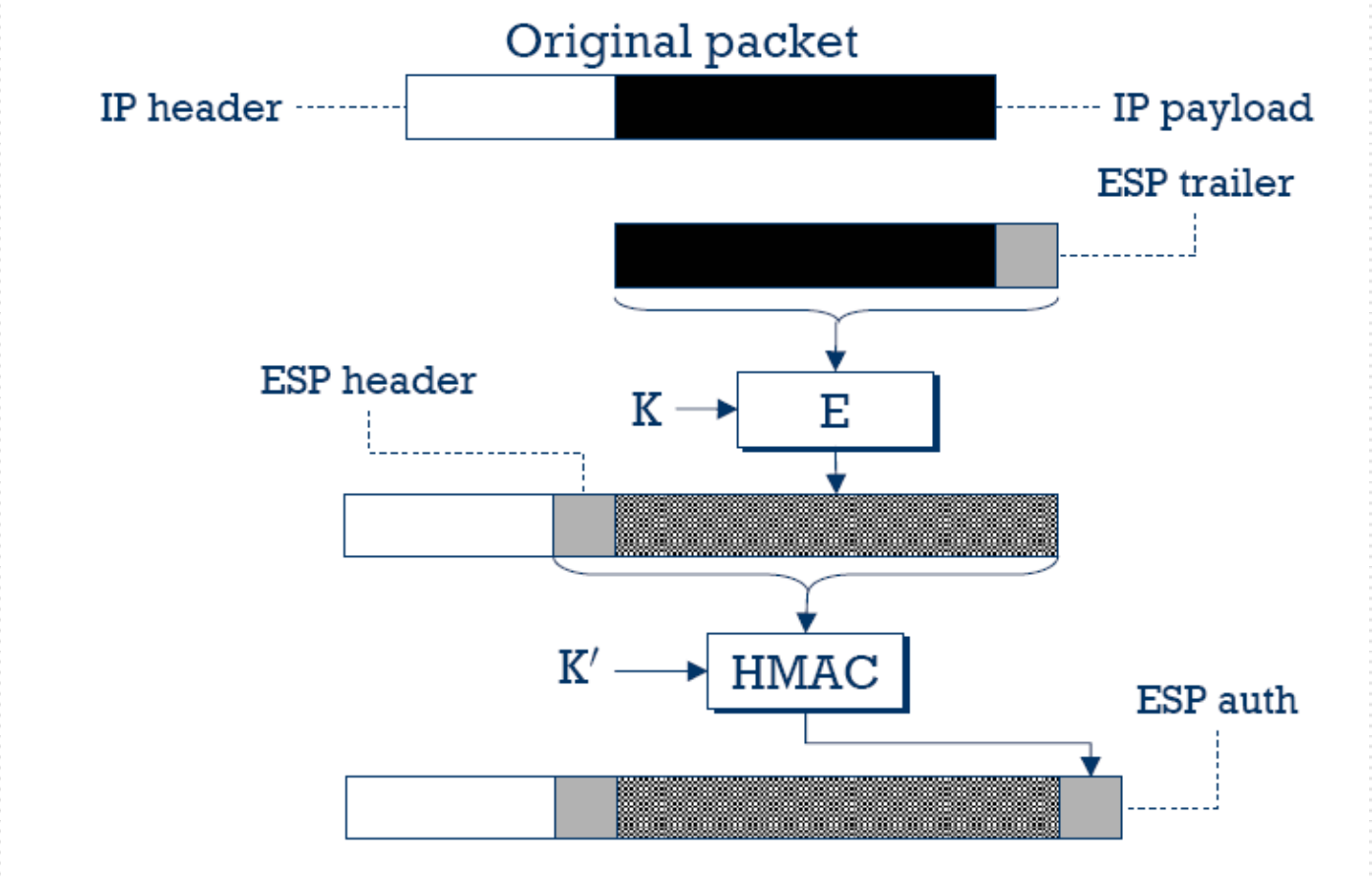
Protocollo ESP

Fornisce confidenzialità, integrità e autenticazione.
Quest'ultima differisce da quella fornita dal protocollo AH in quanto non copre l'header IP esterno.

Di seguito, un tipico messaggio ESP.

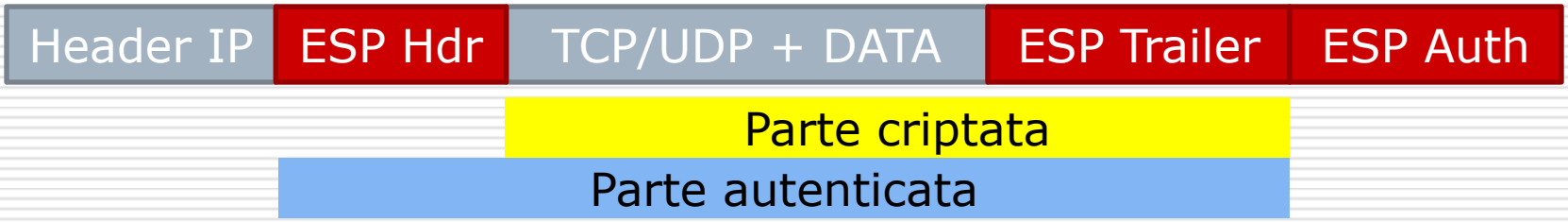


Creazione pacchetto ESP

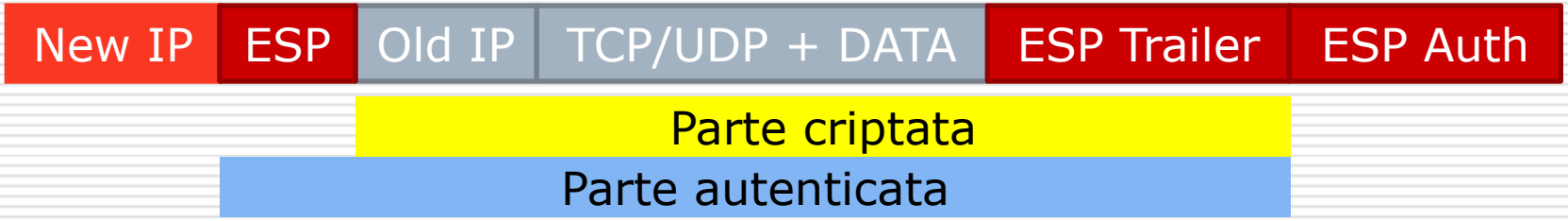


ESP

- ESP – Transport Mode

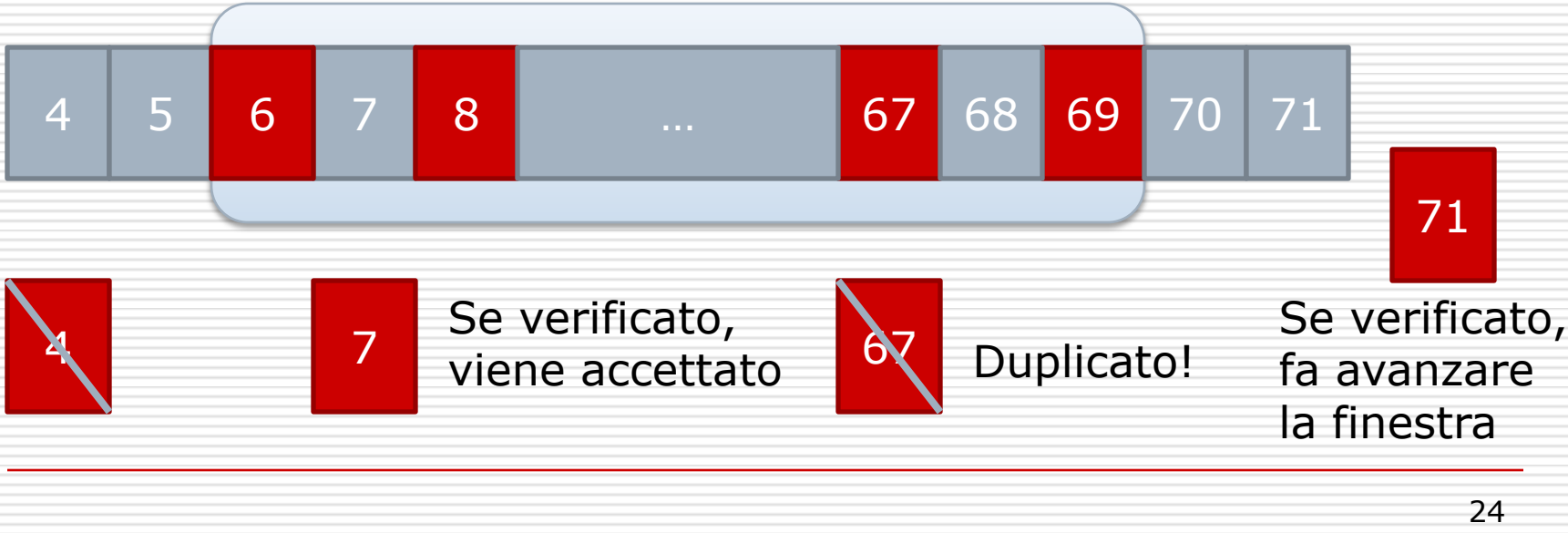


- ESP Tunnel Mode



Anti Replay Window

- Consente alla destinazione di stabilire se i datagrammi ricevuti posseggono numeri seriali validi.
- Finestra mobile larga 64 unità. Essa avanza ogni volta che si riceve un nuovo pacchetto **valido**.
- Un datagramma è accettato se possiede un numero seriale compreso all'interno della finestra.



Scambio delle chiavi

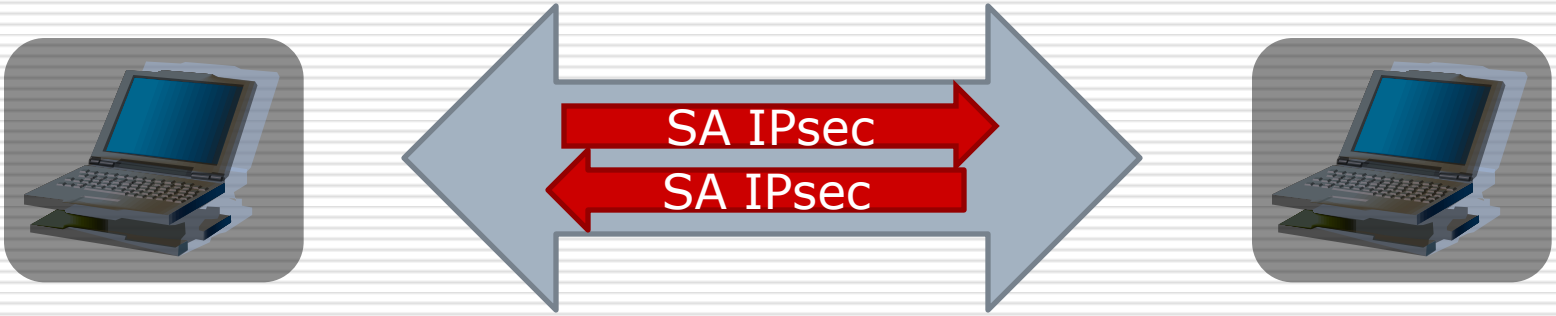
- AH ed ESP non si preoccupano della gestione delle SA.
- Le SA possono essere costruite manualmente (possibile in contesti limitati) o automaticamente
- Il protocollo ISAKMP (Internet Security Association and Key Management Protocol) definisce le procedure e il formato dei pacchetti per la gestione delle security association e per lo scambio e l'autenticazione delle chiavi, indipendentemente dallo schema adottato per lo scambio delle chiavi.
- ISAKMP non è un vero e proprio protocollo ma una struttura di riferimento

Scambio delle chiavi

- OAKLEY (RFC-2412): protocollo che realizza lo scambio autenticato delle chiavi simmetriche tra sistemi IPsec.
- Di tutti gli schemi compatibili con ISAKMP quello che ha raggiunto lo status di standard ufficiale per Internet (RFC-2409) è una variante dello schema OAKLEY, chiamato schema IKE.
- Il protocollo IKE (Internet Key Exchange) permette la creazione, negoziazione, modifica e cancellazione delle associazioni in modo automatico

IKE

Fase 1 - Negoziazione di una SA ISAKMP bidirezionale:
"main mode" o "aggressive mode"



Fase 2 - Negoziazione della SA IPsec: "quick mode"

IKE

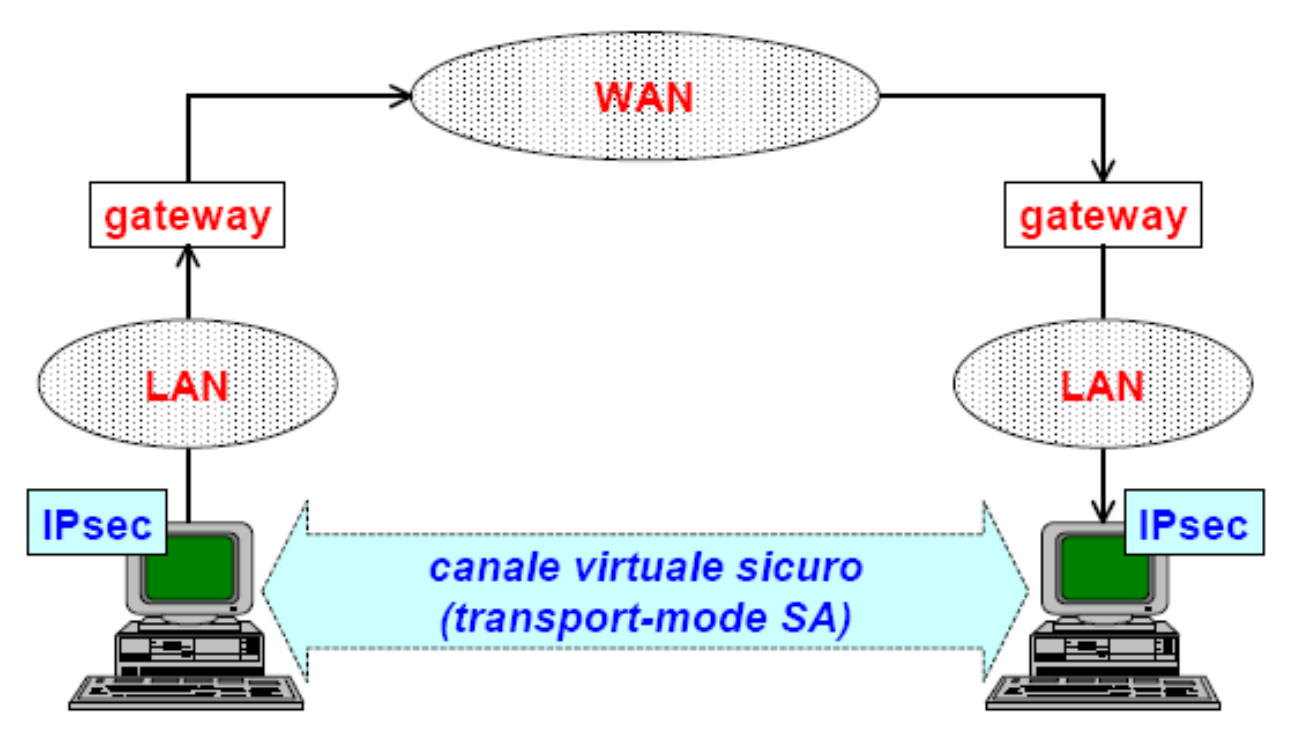
- Creazione di una SA per proteggere lo scambio ISAKMP
- Con questa SA protegge la negoziazione della SA richiesta da IPsec
- La stessa SA ISAKMP può essere riusata più volte per negoziare altre SA IPsec
- Fase 1
  - Aggressive Mode: 3 messaggi scambiati – Protegge solo il materiale relativo alla mutua autenticazione
  - Main Mode: 6 messaggi scambiati – Protegge anche identità dei partecipanti
- Fase 2
  - Quick Mode: 3 messaggi scambiati – Il materiale per l'autenticazione è protetto grazie alla SA ISAKMP stabilita nella fase precedente.

IPsec vs SSL

- Il protocollo TCP non è a conoscenza del livello SSL soprastante e **i due livelli chiaramente non si parlano**. E' quindi possibile, per un attaccante, spedire un pacchetto TCP fasullo che verrà ricevuto dalla macchina attaccata e riconosciuto come valido. Il risultato è che il TCP passerà questo paccetto al livello SSL, il quale si renderà conto dell'attacco e scarterà questi dati. Il problema è che **non ha modo di informare che quel pacchetto dati era fasullo**, quindi il vero pacchetto del flusso, con quel Sequence Number, verrà scartato in quanto il TCP crede di aver già ricevuto questi dati.
- IPsec, posizionandosi sotto il TCP, **evita questo problema**. Inoltre, come SSL, non richiede alcuna modifica sulla rete core in quanto i pacchetti IPsec sono ancora pacchetti IP.

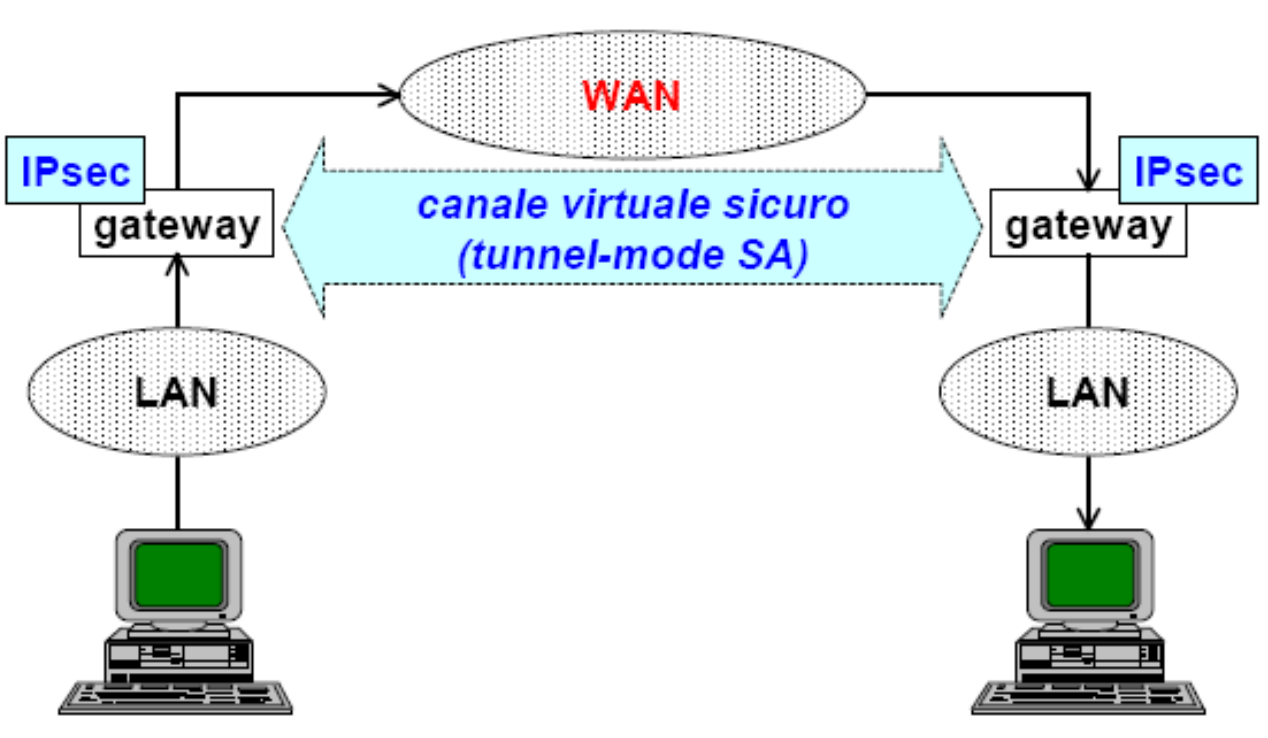
IPsec e canali sicuri

- End-to-end security



IPsec e canali sicuri

- Basic VPN



Breve bibliografia e link

- Maurizio Cinotti. *Internet Security*. Milano, Hoepli Informatica, 2002
- http://www.ietf.org
- http://en.wikipedia.org/wiki/IPsec
- http://www.ipsec-howto.org
- http://www.freeswan.org (una delle implementazioni IPsec per Linux più diffuse)