



# Laboratorio di sicurezza dei protocolli di rete - lab\_100

23 Marzo 2007

**Master in progettazione e gestione di  
sistemi di rete - III edizione**



Dipartimento di  
Informatica



# Agenda lab 011

LAB\_100 Sicurezza dei Protocolli



Dipartimento di  
Informatica

# Agenda lab 011

- ❑ Creazione e gestione di VPN
- ❑ OpenBSD ed ISAKMPD



# IP Security?

IPsec 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.



# Protocolli

IPsec usa due differenti protocolli - AH ed ESP - per fornire l'autenticazione, l'integrità e la confidenzialità della comunicazione.

Può proteggere l'intero datagramma IP o solamente i protocolli di alto livello.



# Tunnel mode

I diversi modelli di funzionamento sono detti tunnel mode e transport mode.

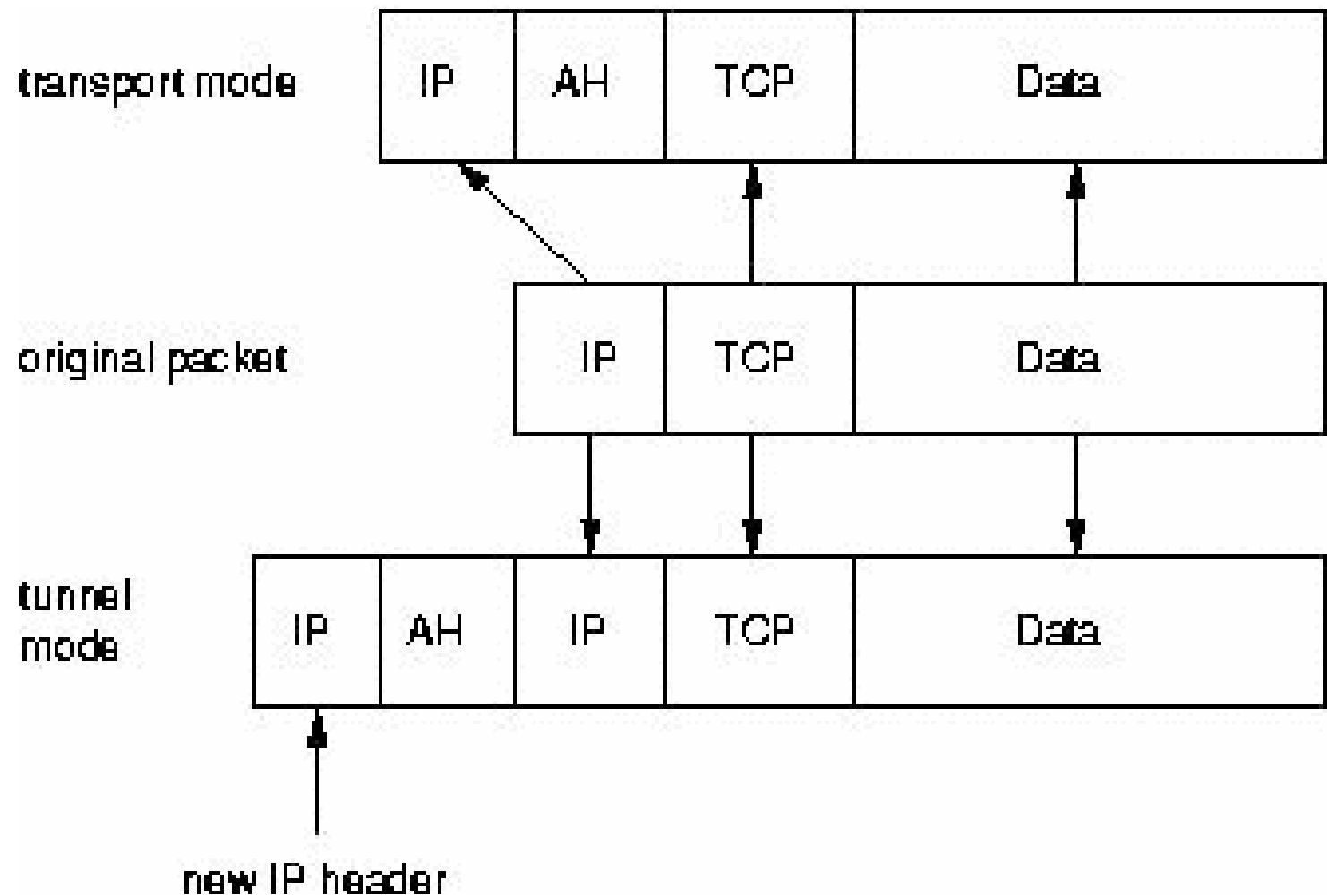
Nel tunnel mode il datagramma IP viene completamente incapsulato in un nuovo datagramma IP utilizzando IPsec.

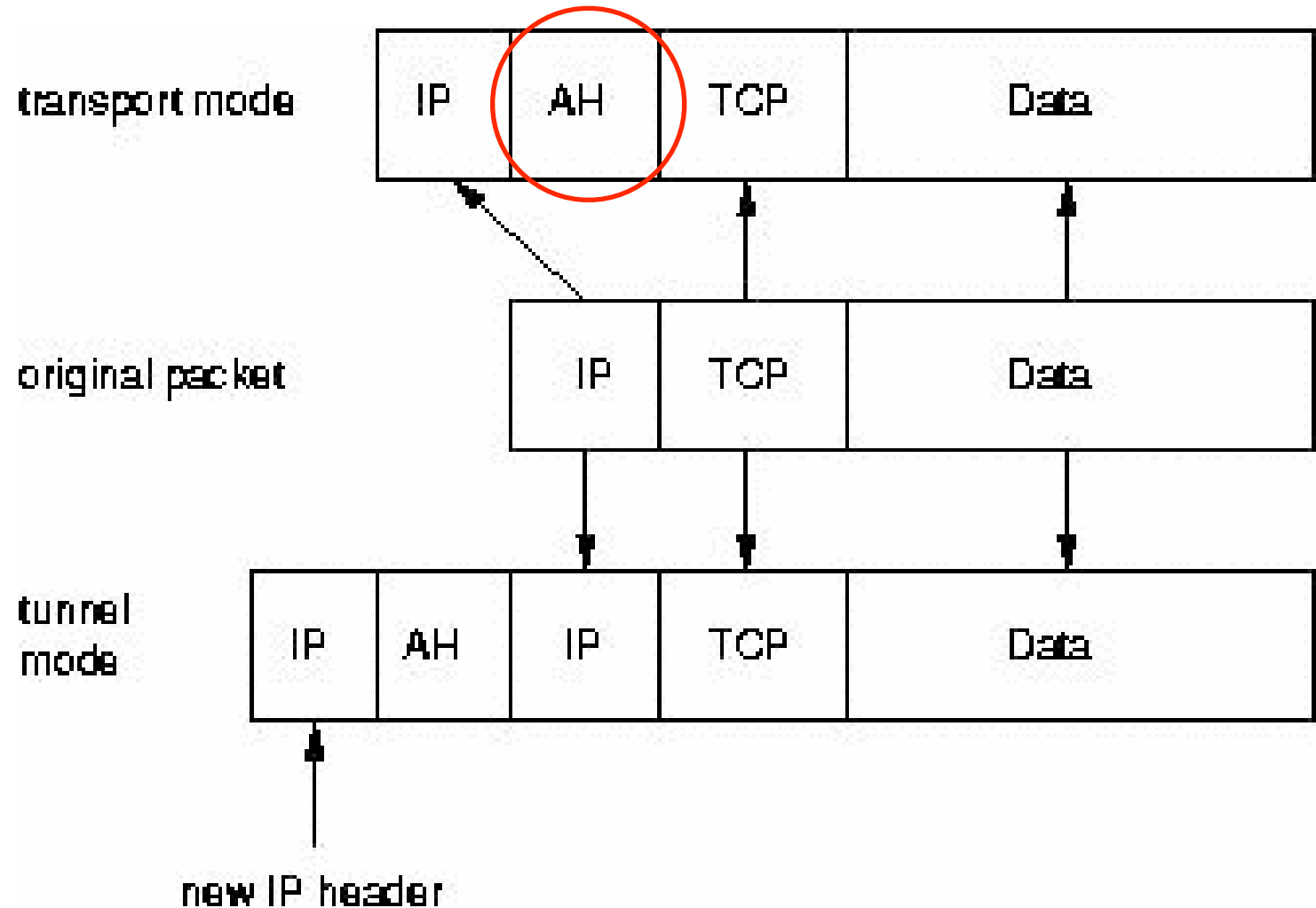


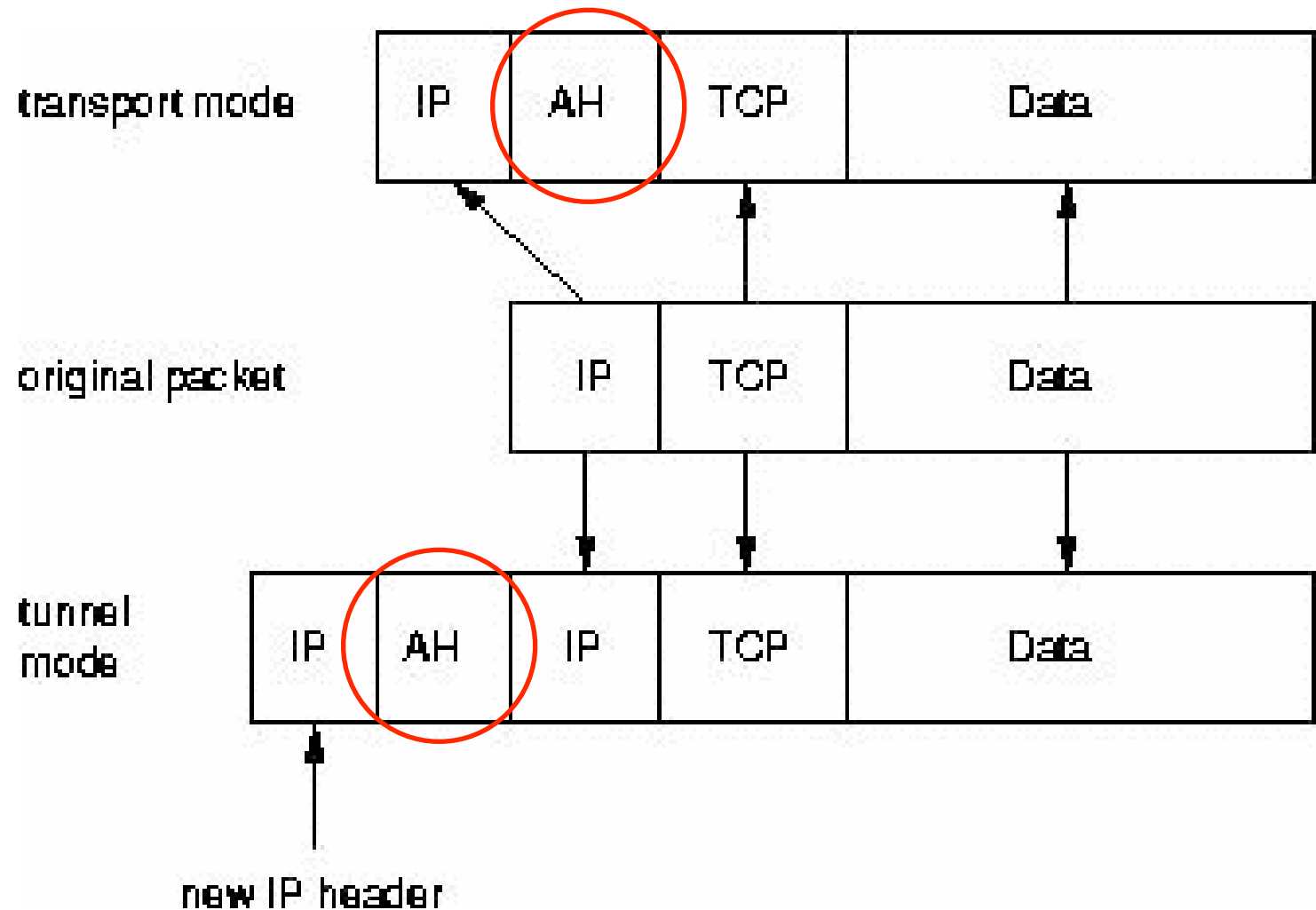
# Transport mode

In transport mode solo il payload del datagramma IP viene trattato da IPsec che inserisce il proprio header tra l'header IP ed i livelli superiori.









# Integrità

Per proteggere l'integrità di un datagramma IP il protocollo IPsec utilizza meccanismi di autenticazione basati su codici hash (HMAC).

Per ottenere questo HMAC vengono usati algoritmi come MD5 o SHA per calcolare un hash basato su una chiave segreta e sul contenuto di un datagramma IP.



# Simmetria

L'HMAC viene quindi inserito nell'header IPsec ed il destinatario del pacchetto ne può verificare l'esattezza soltanto avendo accesso alla chiave segreta.



# Confidenzialità

Per proteggere la confidenzialità di un datagramma IP il protocollo IPsec utilizza degli algoritmi di cifratura simmetrici.

L'IPsec richiede l'implementazione di NULL (nessuna cifratura) e del DES.

Attualmente vengono utilizzati algoritmi più robusti come 3DES, AES ed il Blowfish.



# DoS

Per proteggersi contro un attacco di tipo denial of service, il protocollo IPsec utilizza un meccanismo di sliding window.

Ciascun pacchetto possiede un numero di sequenza e viene accettato solo se tale numero rientra nella finestra o è più recente.

# Replay Attack

I pacchetti più vecchi vengono immediatamente scartati.

Questo protegge da attacchi di tipo replay, nei quali pacchetti originali vengono conservati e rispediti in seguito.



# Gestione delle informazioni

Perchè le due parti siano in grado di effettuare l'incapsulamento ed il recupero dei pacchetti IPsec è necessario che vi sia un luogo nel quale conservare le chiavi, gli algoritmi e gli indirizzi IP coinvolti nella comunicazione.



# Security Association

Tutti questi parametri necessari per la protezione del datagramma IP, sono inseriti in una security association (SA).

Le security association vengono conservate a turno in un database detto SAD (security association database).



# SA

Ciascuna SA definisce i seguenti parametri:

- IP sorgente e destinazione
- Il protocollo IPsec (AH o ESP), l'eventuale supporto per la compressione (IPCOMP).
- Gli algoritmi e le chiavi utilizzate.
- Security Parameter Index (SPI).
- Un numero di 32 bit che identifica la SA.



# Implementazioni

Alcune implementazioni di SAD permettono inoltre di immagazzinare:

- IPsec mode (tunnel o transport)
- Le dimensioni per la sliding window
- La durata della SA.



# Duplex

Poiché la security association contiene l'IP sorgente e destinazione, può proteggere una sola direzione in una connessione full duplex.

Per proteggere entrambe le direzioni sono necessarie due security association.



# Security Policy

Una security association specifica solo come proteggere il traffico. Sono necessarie ulteriori informazioni per definire quale tipo di traffico proteggere. Queste informazioni sono contenute in una security policy (SP) e immagazzinate a turno in un security policy database (SPD).



Una SP specifica normalmente i seguenti parametri:

- Sorgente e destinazione del pacchetto da proteggere. In transport mode sono i medesimi della corrispondente SA.
- Il protocollo (e la porta) da proteggere. Alcune implementazioni non permettono di definire un protocollo in particolare. In questo caso tutto il traffico tra i due IP specificati viene protetto.
- La security association da utilizzare per la protezione dei pacchetti.





# Le chiavi

La chiave segreta e gli algoritmi di crittografia devono essere condivisi dalle due parti di una virtual private network.

Come scambiarle in modo sicuro?

# Phase 1

Per risolvere questo problema è stato sviluppato l'internet key exchange protocol (IKE).

Nella prima fase quest'ultimo autentica le due parti.



# Metodi

L'autenticazione delle parti nella prima fase può di solito essere basata su pre-shared keys (PSK), RSA keys e certificati X.509.



# Phase 2

Nella seconda la security association viene negoziata e le chiavi simmetriche vengono scambiate attraverso il metodo Diffie Hellmann.



# IKE

Il protocollo IKE rinegozia periodicamente le chiavi per garantire la confidenzialità.

Crea inoltre le security association e popola il SAD.

IKE utilizza la porta 500/udp per la comunicazione tra le parti.





La famiglia di protocolli IPsec è composta da:

- Authentication Header (AH)
- Encapsulated Security Payload (ESP).

Entrambi sono indipendenti dai protocolli IP.

AH è il protocollo IP 51 ed ESP è il 50.



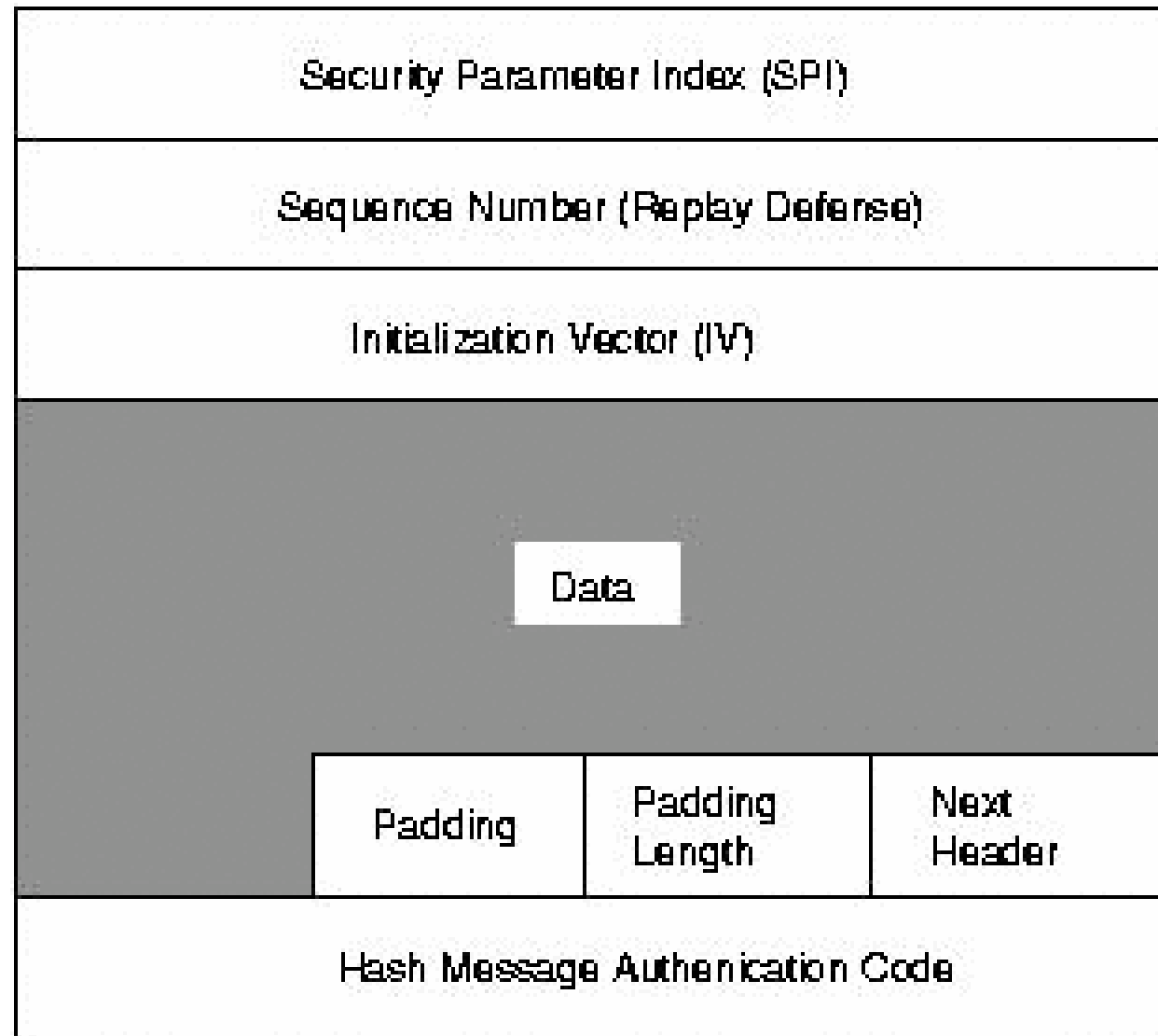
Poichè il protocollo AH calcola l'HMAC in base ad alcune parti non mutabili del datagramma IP, tra le quali gli indirizzi, il NAT non si sposa bene con IPsec.

# NAT-T

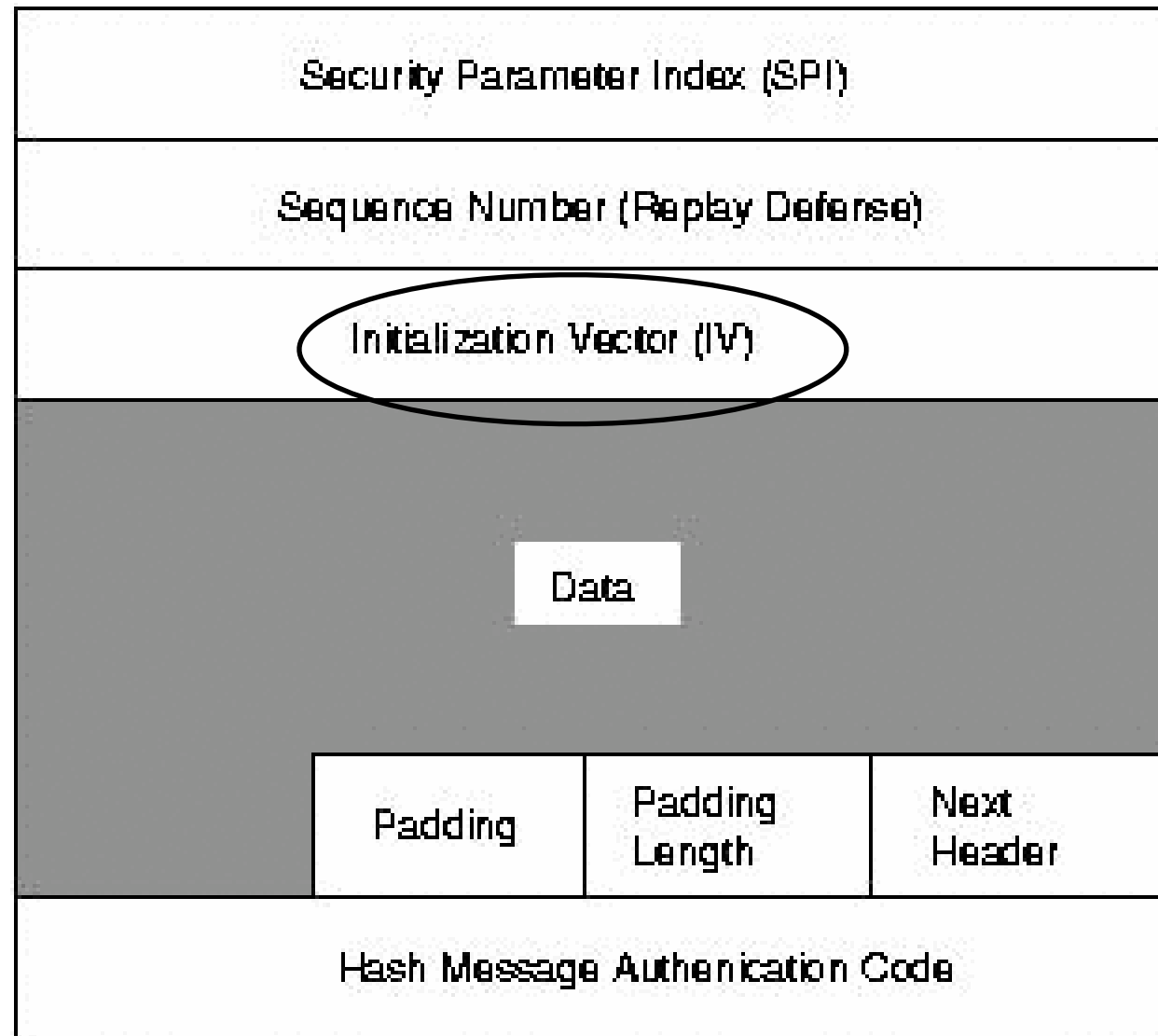
Un'estensione al protocollo detta NAT-Traversal extension riesce però a superare questa limitazione incapsulando il traffico in un flow UDP.



# Header ESP



# Header ESP



# Initialization Vector

Gli algoritmi di crittografia simmetrica sono vulnerabili ad attacchi statistici se non viene utilizzato un IV.

Quest'ultimo infatti assicura che due payload in chiaro identici producano due versioni cifrate differenti.



# NAT ed ESP

L'utilizzo del NAT non rende inutilizzabile il protocollo ESP.





LAB\_100 Sicurezza dei Protocolli

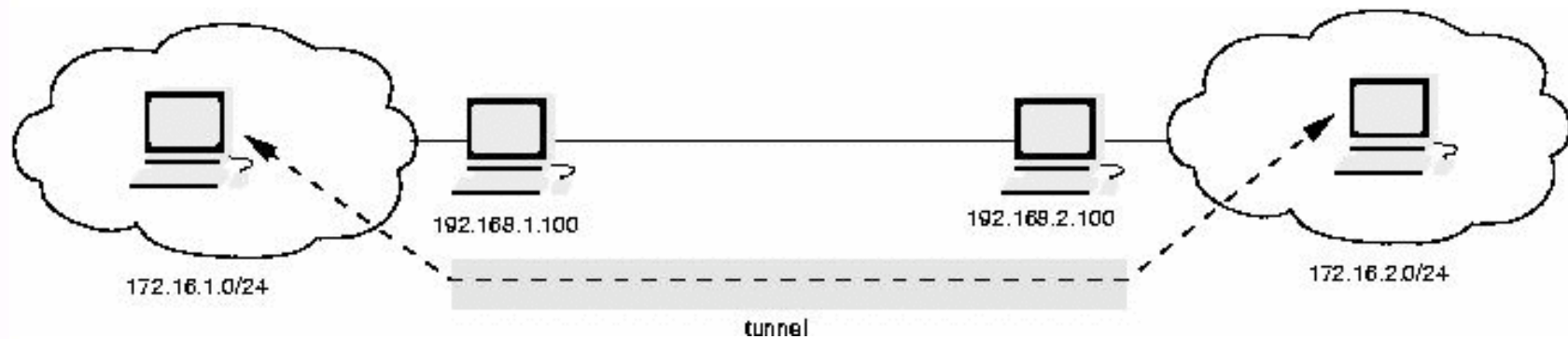


Dipartimento di  
Informatica

# Laboratorio

# Network Schema

LAB\_100 Sicurezza dei Protocolli



Dipartimento di  
Informatica

# /etc/isakmpd/isakmpd.conf

```
[General]
Listen-on= 192.168.1.100

[Phase 1]
192.168.2.100= ISAKMP-peer-west

[Phase 2]
Connections= IPsec-east-west

[ ISAKMP-peer-west ]
Phase= 1
Local-address= 192.168.1.100
Address= 192.168.2.100
Authentication= ThisIsThePassphrase
```





# /etc/isakmpd/isakmpd.conf

```
[ IPsec-east-west ]
Phase=                2
ISAKMP-peer=         ISAKMP-peer-west
Configuration=       Default-quick-mode
Local-ID=             Net-east
Remote-ID=           Net-west

[ Net-west ]
ID-type=              IPV4_ADDR_SUBNET
Network=              172.16.2.0
Netmask=              255.255.255.0

[ Net-east ]
ID-type=              IPV4_ADDR_SUBNET
Network=              172.16.1.0
Netmask=              255.255.255.0

[ Default-quick-mode ]
DOI=                  IPSEC
EXCHANGE_TYPE=       QUICK_MODE
Suites=               QM-ESP-3DES-MD5-PFS-SUITE
```



```
KeyNote-Version: 2
Authorizer: "POLICY"
Licensees: "passphrase:ThisIsThePassphrase"
Conditions: app_domain == "IPsec policy" &&
             esp_present == "yes" &&
             esp_enc_alg == "3des" &&
             esp_auth_alg == "hmac-md5" -> "true";
```

Per provare la connessione si avvia  
isakmpd:

```
isakmpd -d -4 -DA=90
```

isakmpd partirà in foreground (-d) utilizzando  
ipv4 (-4) e un debug level pari a 90.

# Thanks to:

Reyk Floeter @ OpenBSD.org

*for his code, speeches and all the beers and chats @OpenCON ;P*

Ralf Spenneberg

*for the IPsec How-To*

ginox @ autistici.org

*for the Italian translation of the IPsec How-To*



# Bibliografia

<http://www.ipsec-howto.org/>

<http://www.openbsd.org/>

<http://undeadly.org/>

<http://www.openbeer.it/>

<http://www.recursiva.org/>



# Grazie!

Queste slide sono disponibili su

<http://www.scienze.univr.it/fol/main?ent=avvisoin&cs=105>

Per domande od approfondimenti:

[alessio@alba.st](mailto:alessio@alba.st)



Dipartimento di  
Informatica

These slides written by  
Alessio L.R. Pennasilico  
aka mayhem. They are  
subjected to Creative  
Commons Attribution-  
ShareAlike 2.5 version;  
you can copy, modify,  
sell. "Please" cite your  
source and use the same  
licence :)