Cryptography and Network Security Chapter 19

Fifth Edition

by William Stallings

Lecture slides by Lawrie Brown

Chapter 19 – IP Security

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

—*The Art of War*, Sun Tzu

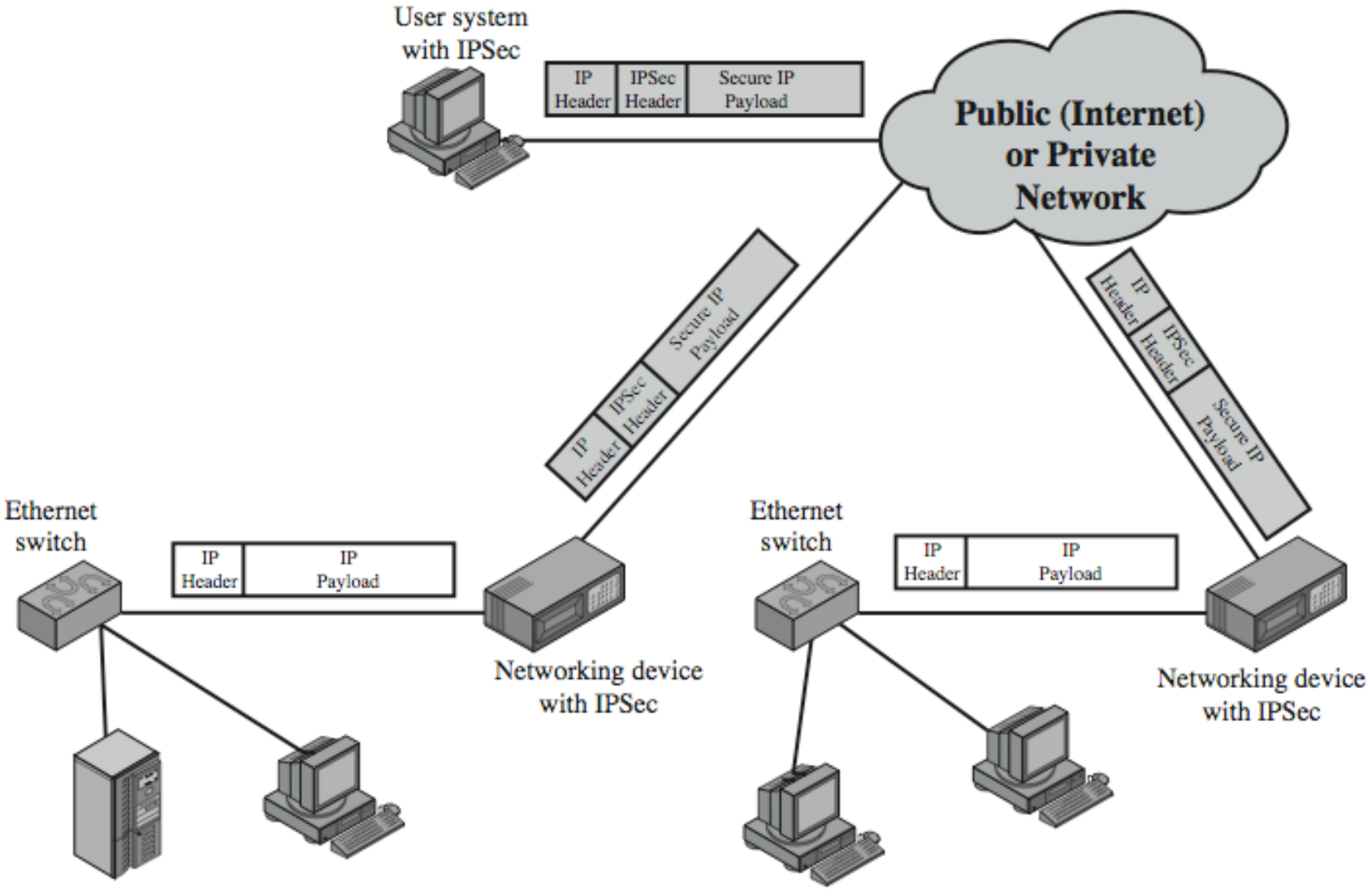
Ασφαλεια του IP
(IP Security)

- Υπαρχει μια μεγαλη γκαμα απο application-specific μηχανισμους ασφαλειας
  - π.χ. S/MIME, PGP, Kerberos, SSL/HTTPS
- Ωστοσο υπαρχουν θεματα ασφαλειας που τεμνουν τα επιπεδα των πρωτοκολλων
- Πρεπει η ασφαλεια να υλοποιηθει απο το δικτυο για ολες τις εφαρμογες

IP Security

- Γενικοι μηχανισμοι ασφαλειας του IP
- Παρεχει:
  - Πιστοποιηση αυθεντικοτητας (authentication)
  - Εμπιστευτικοτητα (confidentiality)
  - Διαχειριση κλειδιων (key management)
- Εφαρμοζεται για χρηση πανω απο LANs, κατα μηκος δημοσιων και ιδιωτικων WANs, και για το Internet
- Η αναγκη αυτη προσδιοριζεται σε ενα report του 1994 (Security in the Interner Architecture, RFC 1636).
  - Χρειαζεται πιστοποιηση αυθεντικοτητας και κρυπτογραφηση

Τυπικο σεναριο χρησης IPSec



Πλεονεκτηματα του IPSec

- Σε ενα firewall/router το IPSec παρεχει ισχυρη ασφαλεια σε ολο το traffic που διερχεται απο αυτον
- Το traffic σε ενα firewall/router δεν μπορει να γινει bypass
- Ειναι κατω απο το transport layer, και αρα ειναι διαφανες για τις εφαρμογες
- Μπορει να ειναι διαφανες για τους τελικους χρηστες
- Μπορει να παρεχει ασφαλεια σε μεμονωμενους χρηστες
- Ασφαλιζει την αρχιτεκτονικη της δρομολογησης (routing)

Αρχιτεκτονικη Ασφαλειας του IP

- Ο ορισμος της ειναι πολυ συνθετος και γνεται κατα ομαδες:
  - Architecture
    - RFC4301 *Security Architecture for Internet Protocol*
  - Authentication Header (AH)
    - RFC4302 *IP Authentication Header*
  - Encapsulating Security Payload (ESP)
    - RFC4303 *IP Encapsulating Security Payload (ESP)*
  - Internet Key Exchange (IKE)
    - RFC4306 *Internet Key Exchange (IKEv2) Protocol*
  - Cryptographic algorithms
  - Other

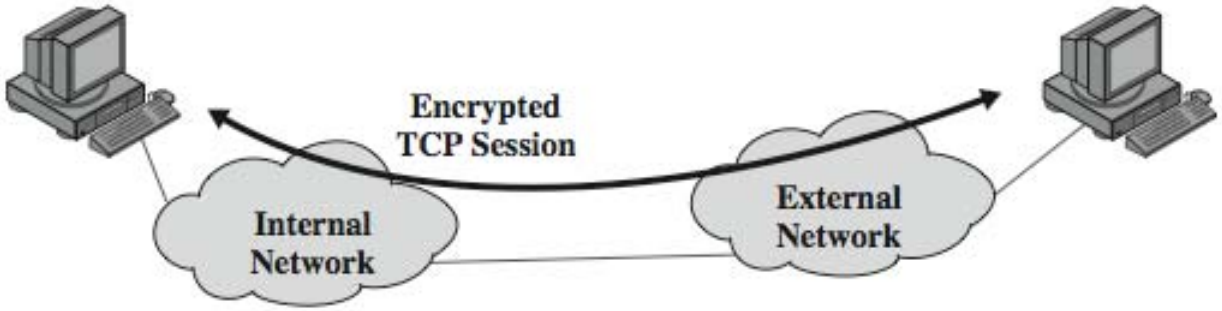
Υπηρεσιες του IPSec

- Ελεγχος Προσβασης (Access control)
- Ακεραιοτητα Χωρις Συνδεση (Connectionless integrity)
- Πιστοποιηση Αυθεντικοτητας Προέλευσης Δεδομενων (Data origin authentication)
- Απορριψη επαναλαμβανομενων πακετων (replayed packets)
  - Μια μορφη μερικης ακεραιοτητας ακολουθιας
- Εμπιστευτικοτητα (Confidentiality, encryption)
- Περιορισμενη Εμπιστευτικοτητα Ροης (Traffic Flow Confidentiality, κρυβει τα στατιστικα χαρακτηριστικα του traffic pattern)

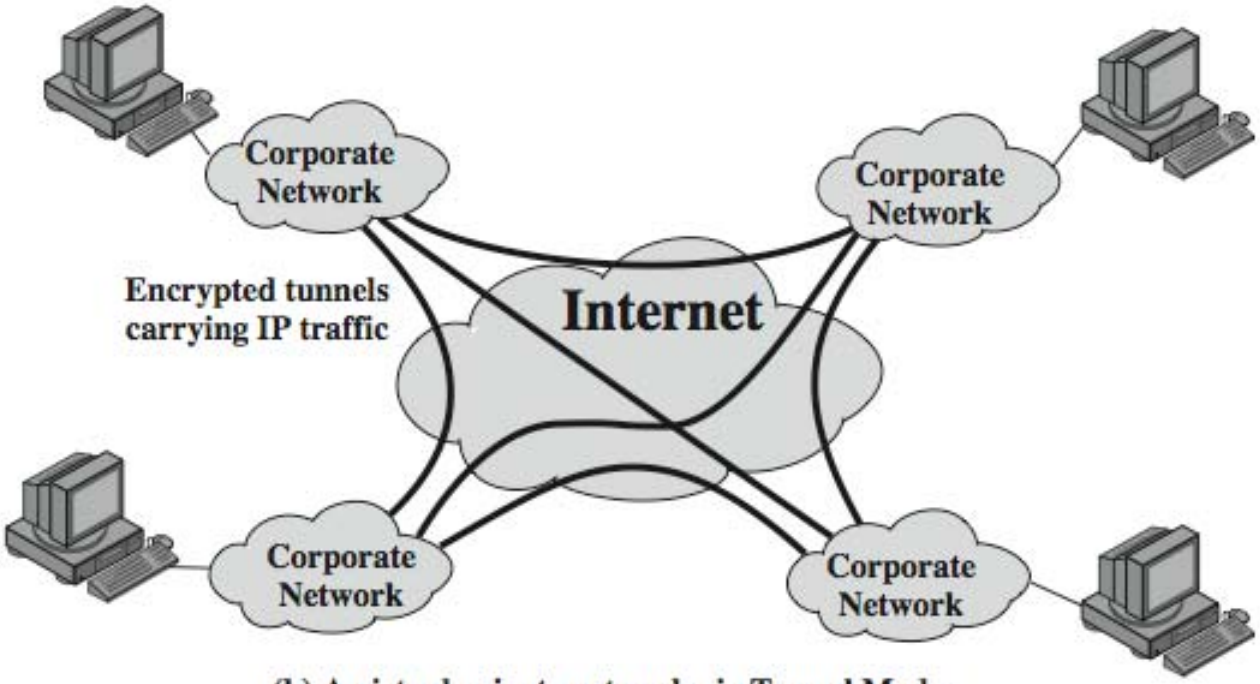
Transport and Tunnel Modes

- **Transport Mode (Κατασταση Μεταφορας)**
  - Παρεχει προστασια κυριως σε πρωτοκολλα ανωτερων επιπεδων. Δηλ. η προστασια εκτεινεται στο payload του πακετου IP.
  - Συνηθως χρησιμοποιειται για end-to-end επικοινωνια μεταξυ hosts.
  - Κρυπτογραφει και προαιρετικα πιστοποιει την αυθεντικοτητα του payload του πακετου IP.
- **Tunnel Mode (Κατασταση Σηραγγας)**
  - Κρυπτογραφει ολοκληρο το πακετο IP
  - Προσθετει νεο header για το επομενο hop
  - Απαγορευει σε ενδιαμεσους routers να εξετασουν τον εσωτερικο IP header
  - Ειναι καταλληλο για VPNs και ασφαλεια gateway-to-gateway

Transport & Tunnel Modes

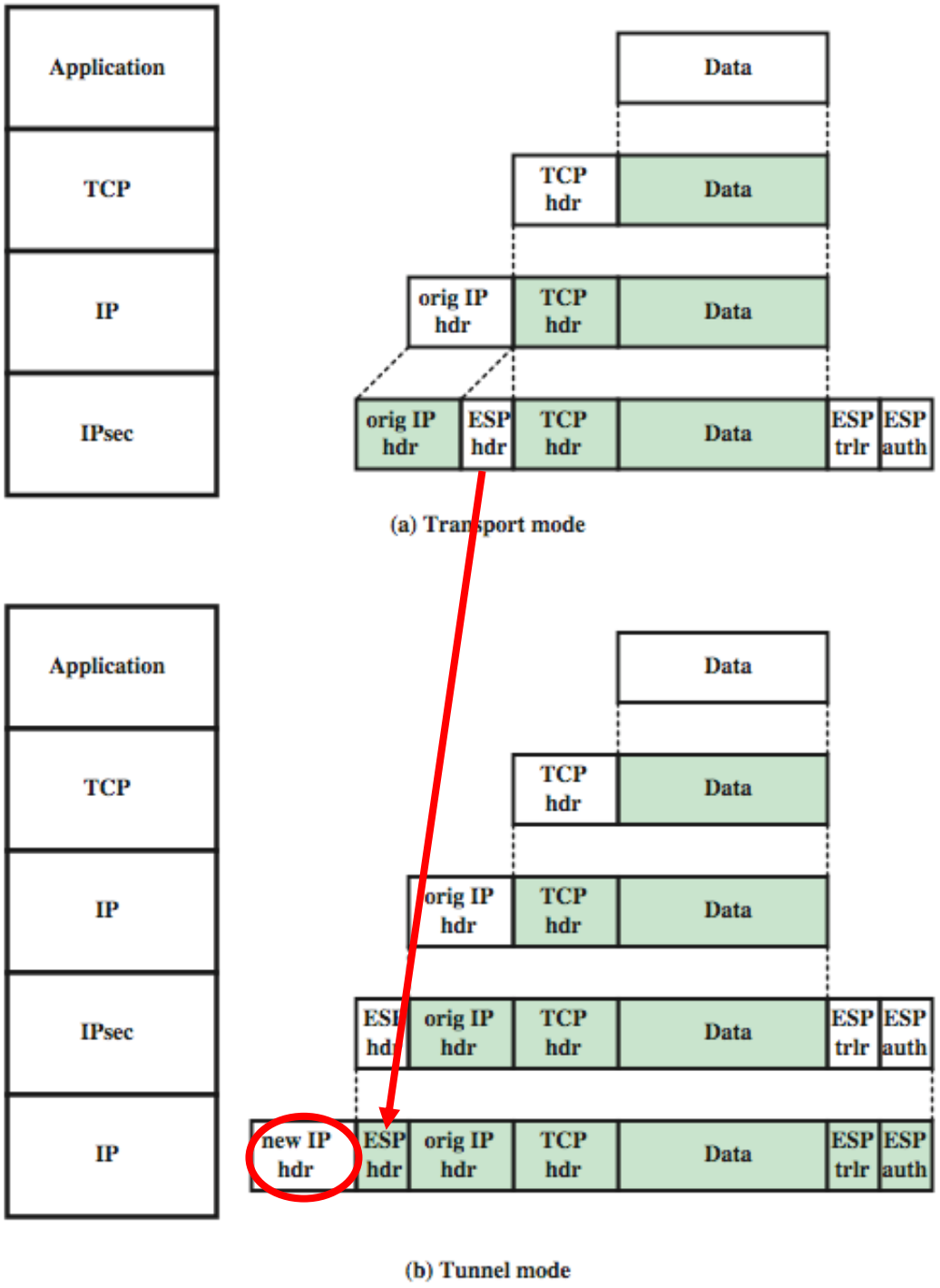


(a) Transport-level security



(b) A virtual private network via Tunnel Mode

Πρωτοκολλα Transport & Tunnel Mode



Συσχετισεις Ασφαλειας (Security Associations)

- Συσχετιση Ασφαλειας (SA) ειναι μια μονοδρομη σχεση μεταξυ αποστολεα και παραληπτη που παρεχει υπηρεσιες ασφαλειας στην κυκλοφορια που διεξαγεται πανω σε αυτη.
- Αναγνωριζεται με μοναδικο τροπο απο τρεις παραμετρους:
  - Δεικτης παραμετρων ασφαλειας (Security Parameters Index, SPI)
  - Διευθυνση IP προορισμου (IP Destination Address)
  - Αναγνωριστκο Πρωτοκολλου Ασφαλειας (Security Protocol Identifier)
- Εχει και εναν αριθμο απο αλλες παραμέτρους
  - seq no, AH & EH info, lifetime, etc
- Το μεσο με το οποιο η κυκλοφορια IP συσχετιζεται με μια συγκεκριμενη SA ειναι η βαση δεδομενων πολιτικης ασφαλειας (Security Policy Database, SPD)

Security Policy Database

- Συσχετιζει την κινηση IP με συγκεκριμενες SAs
  - Ταιριαζει ενα υποσυνολο της κινησης IP με την SA που αυτο αντιστοιχει.
  - Καθε καταχωρηση στη βαση SPD προσδιοριζεται απο ενα συνολο τιμων πεδιων του IP και πρωτοκολλων υψηλοτερου επιπεδου που ονομαζονται επιλογεις (selectors).
  - Οι επιλογεις χρησιμοποιουνται για το φιλτραρισμα της εξερχομενης κινησης, με σκοπο την κετευθυνση της σε συγκεκριμενη SA.
  - Επιλογεις: Διευθυνση IP πηγης και προορισμου, θυρες πηγης και προορισμου, Πρωτοκολλο του Transport Layer.

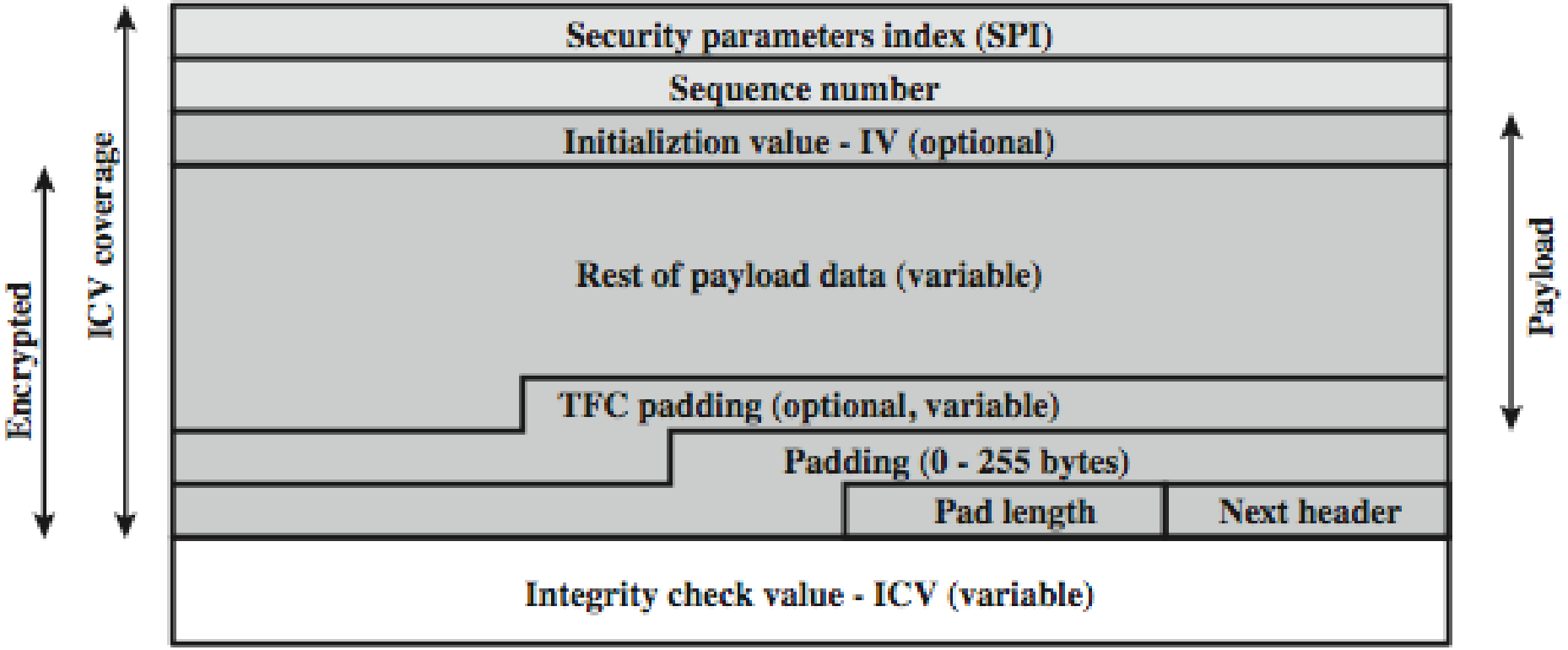
Παραδειγμα SPD

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Πρωτοκολλο Ασφαλους Ενθυλακωσης Πακετου (Encapsulating Security Payload, ESP)

- Παρεχει εμπιστευτικοτητα περιεχομενου του μηνυματος, πιστοποιηση αυθεντικοτητας πηγης, connectionless ακεραιοτητα, υπηρεσια αποτροπης της επιθεση επαναληψης (replay attack), περιορισμενη εμπιστευτικοτητα ροης κινησης
- Οι υπηρεσιες εξαρτωνται απο τις options που θα επιλεγουν κατα την εγκατασταση της SA
- Μπορουν να χρησιμοποιηθουν μια ποικιλια αλγοριθμων κρυπτογραφησης και πιστοποιησης αυθεντικοτητας

Format Πακέτου ESP



Αλγοριθμοι Κρυπτογραφησης και Πιστοποιησης Αυθεντικοτητας

- Το ESP μπορει να κρυπτογραφησει τα πεδια: payload data, padding, pad length, next header
  - Αν απαιτειται απο τον αλγοριθμο κρυπτογραφησης μπορει να υπαρχει ενα προαιρετικο πεδιο IV (Initialization Value) στην αρχη των payload data
- Το ESP μπορει να εχει ενα προαιρετικο και μεταβλητου μηκους πεδιο ICV (integrity check value) που εξασφαλιζει την ακεραιοτητα του πακετου
  - Υπολογιζεται μετα την κρυπτογραφηση

Padding

- Το πρωτοκολλο ESP χρησμοποιει padding
  - Για να επεκτεινει το plaintext ωστε να φτασει στο απαιτουμενο μηκος
  - Για να ευθυγραμμισει τα πεδια **pad length** και **next header**
  - Για να συνεισφερει στην εμπιστευτικοτητα της ροης κινησης κρυβοντας το πραγματικο μηκος του payload.

Υπηρεσια αποτροπης της επιθεσης επαναληψης (Anti-Replay Service)

- Η επιθεση επαναληψης συνισταται στη επανεκπομπη ενος αντιγραφου καποιου πιστοποιημενου πακετου.
- Για να αντιμετωπιστει πρεπει να χρησιμοποιουνται ακολουθιακοι αριθμοι (sequence numbers)
- Οταν εγκαθισταται μια νεα SA, ο αποστολεας αρχικοποιει τον ακολουθιακο αριθμο σε 0.
  - Αυξανεται κατα 1 για καθε πακετο
  - Δεν πρεπει να υπερβαινει το οριο $2^{32} – 1$
  - Αν φτασει το οριο αυτο, τοτε τερματιζεται η συγκεκριμενη SA και διαπραγματευεται η δημιουργια νεας SA με νεο κλειδι.

Μηχανισμος Anti-Replay

Αν N ειναι ο μεγαλύτερος ακολουθιακος αριθμος που εχει ληφθει μεχρι στιγμης και W το μεγεθος του παραθυρου, τοτε το δεξι ακρο του παραθυρου τοποθετειται στο N και αποδεκτης δεχεται μονο πακετα με ακολουθιακο αριθμο μεσα στο παραθυρο [*N –W+1, N*]

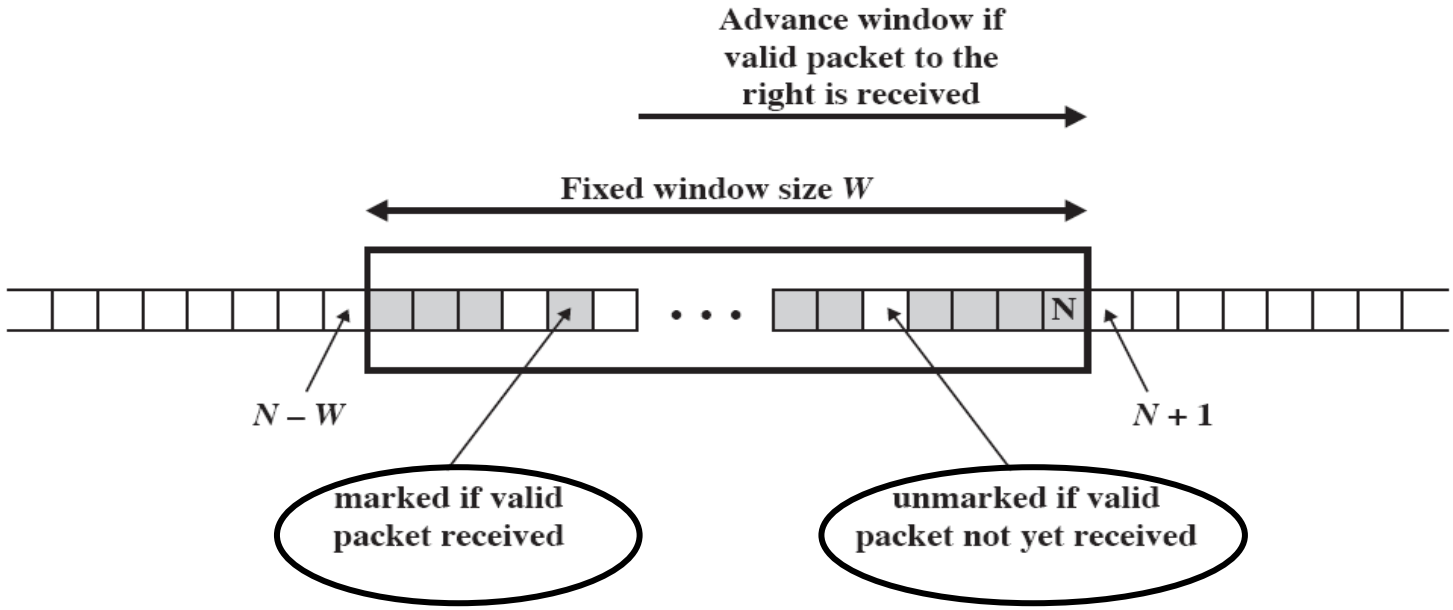


Figure 19.6 Anti-Replay Mechanism

Συνδιαζοντας Συσχετισεις Ασφαλειας (Combining Security Associations)

- Καποια στιγμη καποια ροη μπορει να ζητησει υπηρεσιες που για να ικανοποιηθουν χρειαζεται και το ESP και το AH. Οι SA μπορουν να υλοποιησουν ειτε ESP, ειτε AH. Αλλα οχι και τα δυο μαζι.
- Σε τετοιες περιπτωσεις θα πρεπει να χρησιμοποιηθουν περισσοτερες απο μια SAs (δεσμη SAs) για την ιδια ροη πληροφοριας, ετσι ωστε να επιτευχθουν ολες οι επιθυμητες υπηρεσιες IPSec.
- Αυτο μπορει να γινει με τους εξης δυο τροπους:
  - **Γειτνιαση μεταφορων (transport adjacency):** Εφαρμογη περισσοτερων απο ενα πρωτοκολλων ασφαλειας στο ιδιο πακετο IP, χωρις τη χρηση σηραγγας.
  - **Επαναλαμβανομενη σηραγγα (iterated tunnel):** Εφαρμογη πολλαπλων επιπεδων πρωτοκολλων ασφαλειας μεσα απο σηραγγες IP. Επιτρεπει την ενθεση πολλων επιπεδων, καθως η καθε σηραγγα μπορει να ξεκιναει και να τερματιζεται σε διαφορετικα σημεια IPSec της διαδρομης.

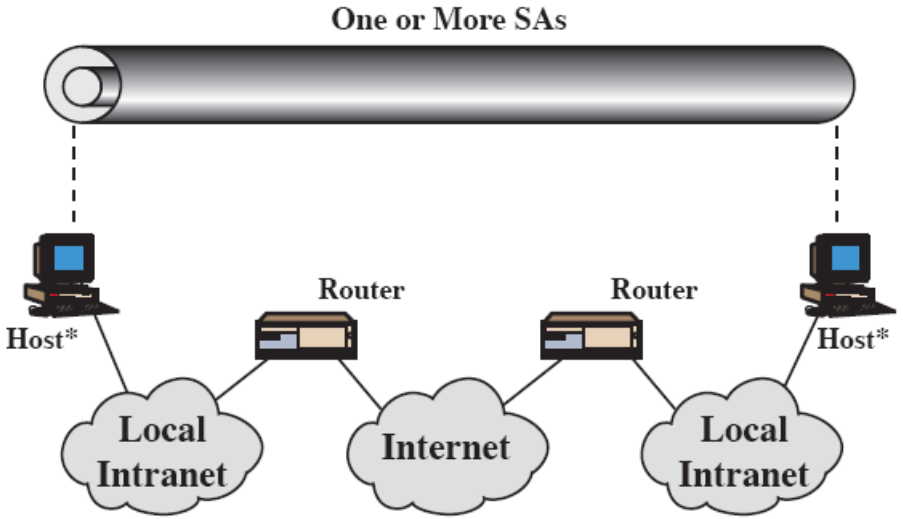
Πιστοποιηση Αυθεντικοτητας και Εμπιστευτικοτητα

Για να επιτευχθει και πιστοποιηση αυθεντικοτητας και εμπιστευτικοτητα κατα τη μεταδοση ενος πακετου IP μεταξυ δυο υπολογιστων υπαρχουν διαφορες εναλλακτικες προσεγγισεις.

1. **ESP με επιλογη πιστοποιησης.** Ο χρηστης εφαρμοζει πρωτα το μηχανισμο ESP στα δεδομενα ωστα να τα προστατευσει και στη συνεχεια επισυναπτει το πεδιο Authentication Data.
   - ESP σε κατασταση μεταφορας
   - ESP σε κατασταση σηραγγας
2. **Γειτνιαση μεταφορων.** Χρησιμοποιειται μια δεσμη απο δυο SAs. Μια εσωτερικη με ESP (χωρις την επιλογη πιστοποιησης) και μια εξωτερικη με AH. Το πλεονεκτημα εναντι της χρησης μιας ESP με επιλογη πιστοποιησης ειναι οτι καλυπτονται περισσοτερα πεδια συμπεριλαμβανομενων των διευθυνσεων IP πηγης και προορισμου. Μειονεκτημα το μεγαλυτερο κοστος υλοποιησης δυο SAs αντι για μια.
3. **Δεσμη μεταφορας σε σηραγγα.** Χρηση πιστοποιησης πριν απο την κρυπτογραφηση. Ετσι ειναι αδυνατο να υποκλεψει καποιος το μηνυμα και να τροποποιησει τις πληροφοριες πιστοποιησης χωρις να ανιχνευθει. Επισης μπορει να θελουμε να αποθηκευσουμε τις πληροφοριες πιστοποιησης μαζι με το μηνυμα για μελλοντικη χρηση.

Βασικοι συνδιασμοι SAs

- Περιπτωση 1: Ολη η ασφαλεια παρεχεται μεταξυ των τελικων συστηματων που υλοποιουν το IPSec. Καθε δυο τελικα συστηματα που επικοινωνουν μεσω μιας SA πρεπει να μοιραζονται μυστικα κλειδια.



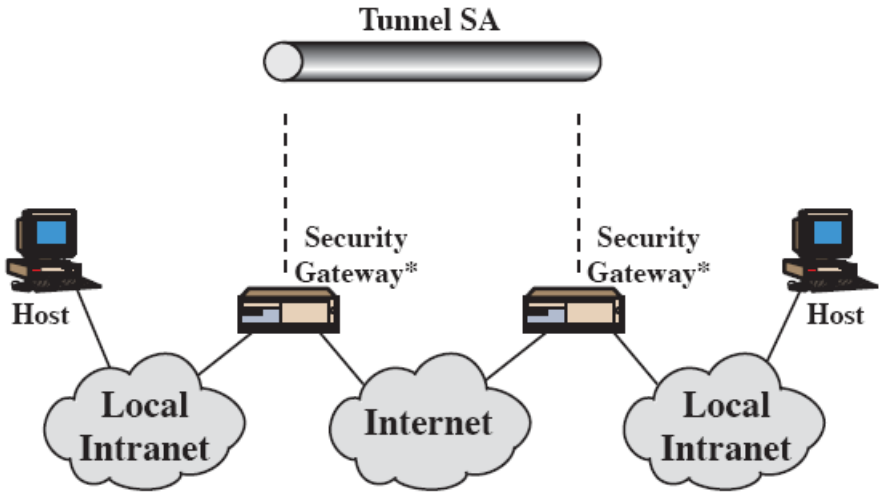
(a) Case 1

Λογικη διασυνδεση

Φυσικη διασυνδεση

Βασικοι συνδιασμοι SAs

- **Περιπτωση 2:** Παρεχεται ασφαλεια μονο μεταξυ των security gateways και κανενα host δεν υλοποιει το IPSec. Αυτος ειναι ενας καλος τροπος υλοποιησης VPNs. Απαιτειται μονο μια SA σε κατασταση σηραγγας.

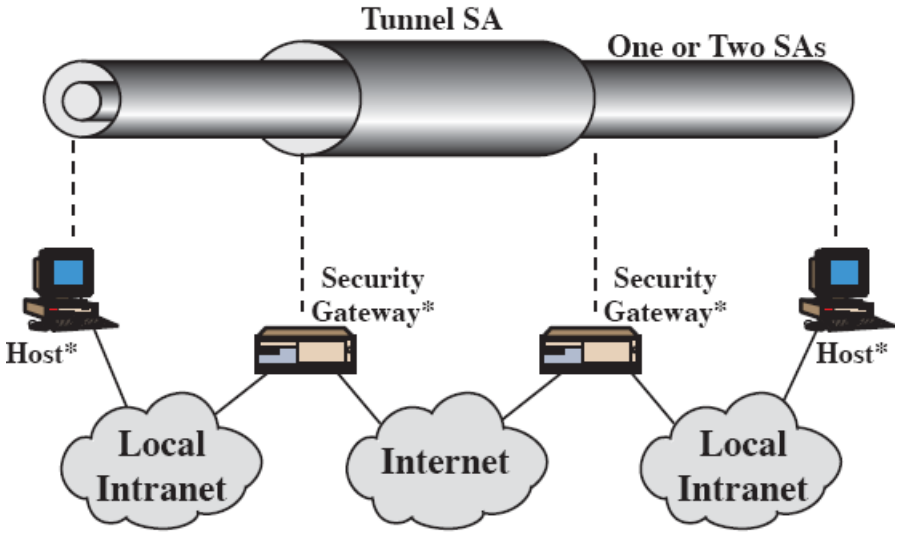


Λογικη διασυνδεση

Φυσικη διασυνδεση

Βασικοι συνδιασμοι SAs

- **Περιπτωση 3:** Ιδια με την περιπτωση 2, αλλα με προσθηκη ασφαλειας απο ακρο σε ακρο. Η σηραγγα απο gateway σε gateway παρεχει σε ολη την κυκλοφορια μεταξυ των τελικων συστηματων πιστοποιηση αυθεντικοτητας, εξασφαλιση απορρητου, ή και τα δυο μαζι.

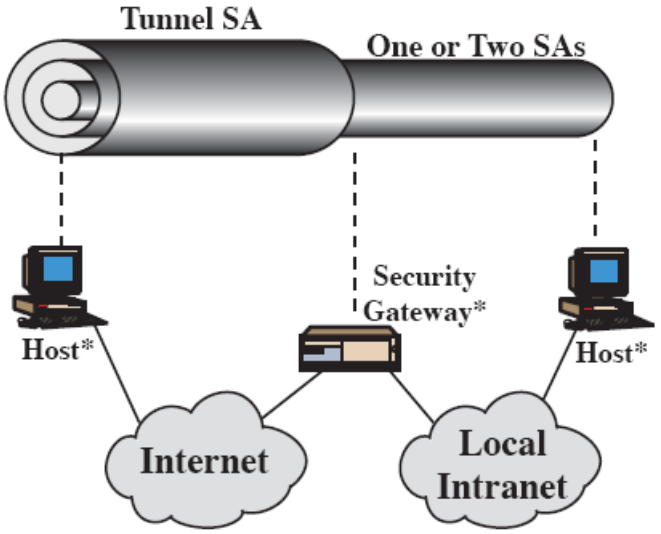


Λογικη διασυνδεση

Φυσικη διασυνδεση

Βασικοι συνδυασμοι SAs

- **Περιπτωση 4:** Υποστηριζει απομακρυσμενους υπολογιστες που χρησιμοποιουν το Internet για να συνδεθουν με ενα firewall ενος οργανισμου και να αποκτησουν προσβαση σε καποιο server ή workstation που βρισκεται πισω απο το firewall.



Λογικη διασυνδεση

Φυσικη διασυνδεση

Διαχειριση κλειδιου στο IPSec

- Φροντιζει για τη δημιουργια και τη διανομη κλειδιου
- Συνηθως χρειαζονται 2 ζευγη κλειδιων
  - 2 ανα κατευθυνση για AH & ESP
- Υποστηριζονται δυο τροποι διαχειρισης κλειδιων
- Χειροκινητη (manual)
  - Ο διαχειριστης διαμορφωνει χειροκινητα το καθε συστημα με τα κλειδια του και τα κλειδια των αλλων συστηματων που επκοινωνουν με αυτο. Εφαρμοζεται σε μικρα και στατικα περιβαλλοντα.
- Αυτοματη (automated)
  - Ενα αυτοματο συστημα επιτρεπει την κατοπιν αιτησης δημιουργια κλειδιων για τις SA. Εφαρμοζεται σε μεγαλα κατανεμημενα συστηματα με μη στατικη διαμορφωση.
  - Το πρωτοκολλο αυτοματης διαχειρισης κλειδιων ονομαζεται Oakley/ISAKMP και αποτελειται απο τα δυο στοιχεια τα ονοματα των οποιων φερει (Oakley και ISAKMP).

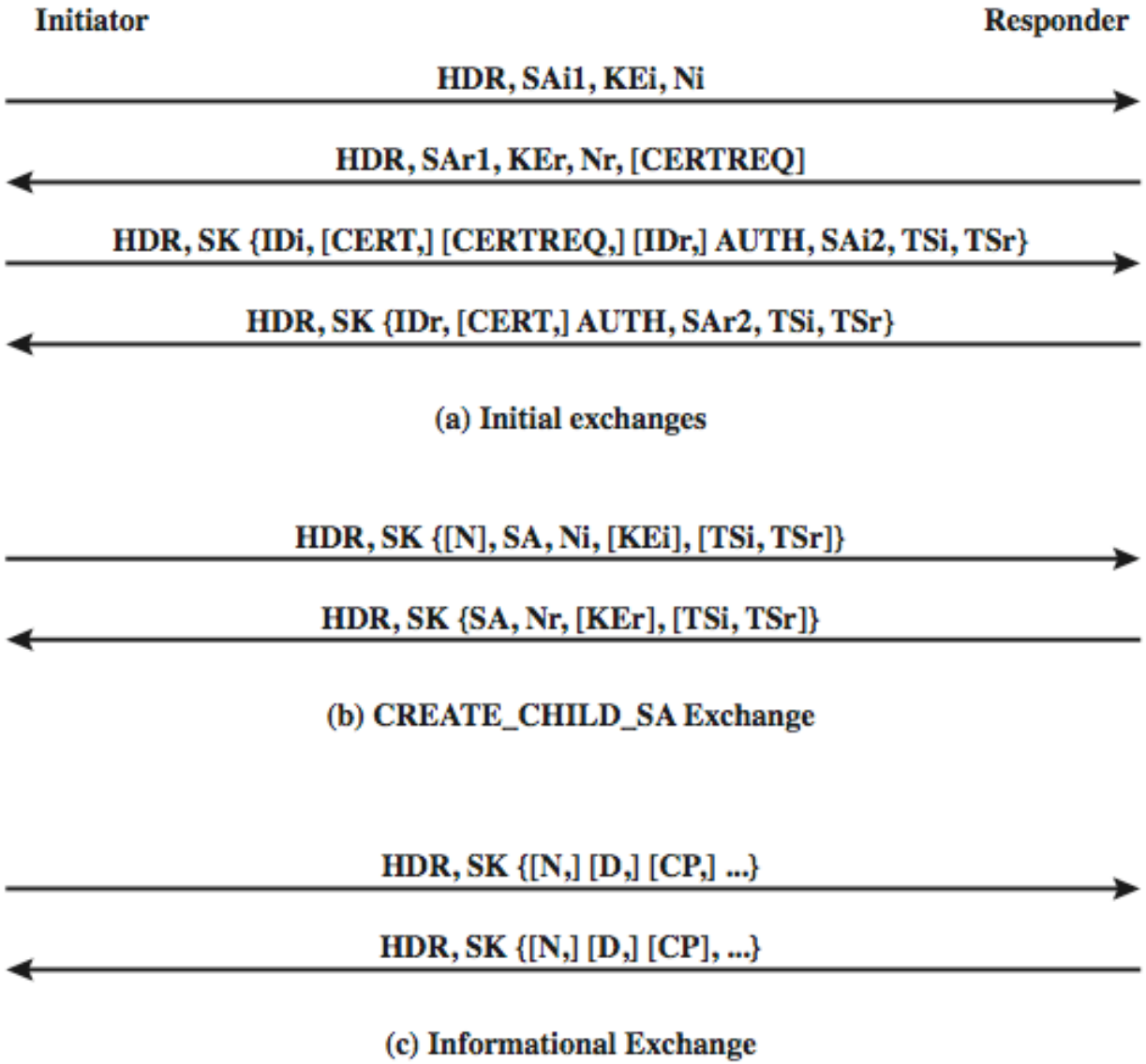
Oakley

- Ειναι ενα πρωτοκολλο προσδιορισμου κλειδιων
- Βασιζεται στην ανταλλαγη κλειδιου Diffie-Hellman αλλα με προσθετη ασφαλεια
- Ειναι γενικο και δεν υπαγορευει καποια συγκεκριμενη διαμορφωση

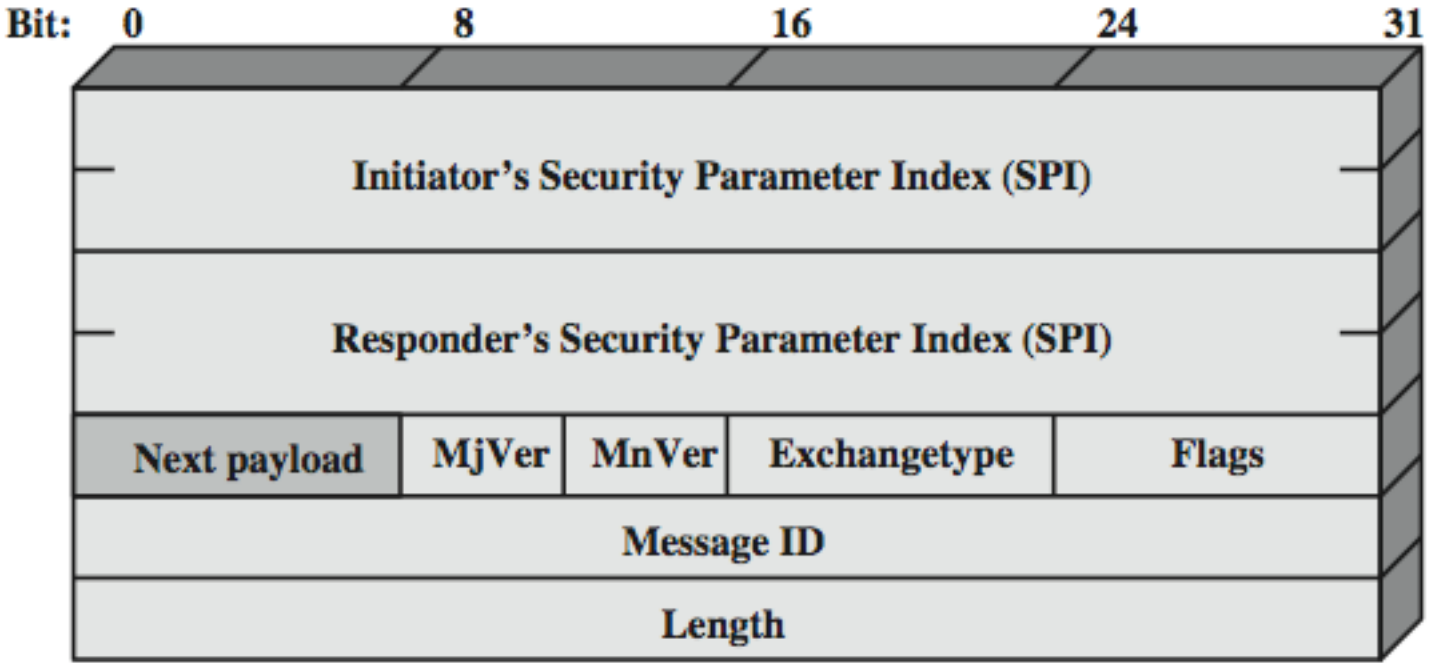
ISAKMP

- Internet Security Association and Key Management Protocol
- Παρεχει το πλαισιο για διαχειριση κλειδιων
- Οριζει διαδικασιες και format πακετων για τη αποκατασταση, διαπραγματευση,τροποποιηση και διαγραφη των SAs
- Ειναι ανεξαρτητο απο τοπρωτοκολλο ανταλλαγης κλειδιων, απο τον αλγοριθμο κρυπτογραφησης και τη μεθοδο πιστοποιησης αυθεντικοτητας

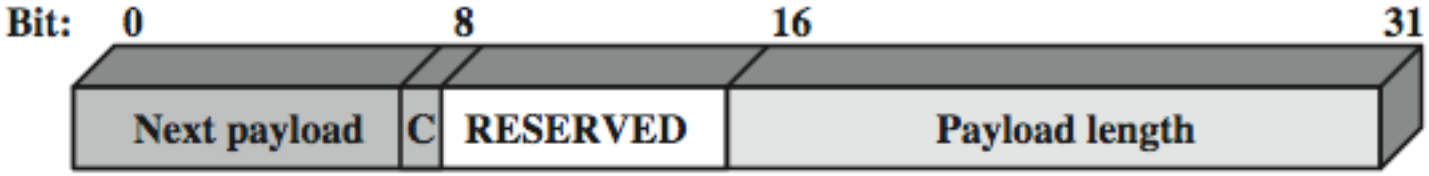
Internet Key Exchange (IKE): IKEV2 Exchanges



ISAKMP



(a) IKE Header



(b) Generic Payload Header

IKE Payloads & Exchanges

- Εχει εναν αριθμο τυπων payload ISAKMP:
  - Security Association, Key Exchange, Identification, Certificate, Certificate Request, Authentication, Nonce, Notify, Delete, Vendor ID, Traffic Selector, Encrypted, Configuration, Extensible Authentication Protocol
- Το payload εχει συνθετη ιεραρχικη δομη
- Μπορει να περιεχει πολλες προτασεις, με πολλα πρωτοκολλα και πολλους μετασχηματισμους

Κρυπτογραφικες Σουιτες (Cryptographic Suites)

- Ποικιλια τυπων κρυπτογραφικων αλγοριθμων
- Για να προαγει τη διαλειτουργικοτητα:
  - Το RFC4308 οριζει τις κρυπτογραφικες σουιτες των VPN
    - VPN-A matches common corporate VPN security using 3DES & HMAC
    - VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 οριζει 4 κρυπτογραφικες σουιτες συμβατες με τις προδιαγραφες της NSA
    - Παρεχει επιλογες για ESP & IKE
    - AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA

Συνοψη

- Εξετασαμε:
  - Το πλαιδιο ασφαλειας IPSec
  - Την πολιτικη ασφαλειας IPSec
  - Το πρωτοκολλο ESP
  - Το πως συνδιαζονται Συσχετισεις Ασφαλειας (SA)
  - Το IKE
  - Τις χρησιμοποιουμενες κρυπτογραφικες σουιτες