ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ(Θ)

Ενότητα 8: ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

ΔΙΔΑΣΚΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΕΙΛΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

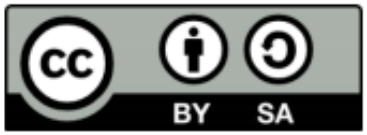
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 8

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Χειλάς Κωνσταντίνος
Διδάκτορας Φυσικής

Περιεχόμενα ενότητας

1. Ασφάλεια επικοινωνιών
    1. Ipsec
2. Security Association (SA)
3. Transport mode
4. Transport mode Ipsec
5. Authentication Header (AH)
6. Tunnel Mode
7. ESP – Encapsulating Security Payload
8. Η επικεφαλίδα του ESP
9. TLS/SSL
    1. Γιατί υπάρχει το SSL
    2. Transport Layer Security (TLS)
    3. TLS διαδικασία χειραψίας
10. Πώς εμπιστεύομαι κάποιον;

Σκοποί ενότητας

Ασφάλεια επικοινωνιών

IPsec

IPsec

- Είναι μια προσπάθεια της IETF να προσθέσει ασφάλεια στη διαδικασία μεταφοράς των πακέτων.
- Συγκεκριμένα, το IPsec τοποθετείται στο 3ο επίπεδο. Με τον τρόπο αυτό η ασφάλεια γίνεται ανεξάρτητη από την εφαρμογή και διάφανη στο χρήστη
- Περιγράφεται κυρίως στα RFCs 2401, 2402 και 2406
- Προσφέρει, κυρίως, μυστικότητα και ακεραιότητα δεδομένων καθώς και προστασία από επανεκπομπές.
- Βασίζεται σε τεχνικές κρυπτογραφίας συμμετρικού κλειδιού (για λόγους ταχύτητας)

Security Association (SA)

- Μια σύνδεση IPsec ονομάζεται *Security Association*.
- Η SA είναι simplex και διαθέτει ένα αναγνωριστικό ασφαλείας που είναι χαρακτηριστικό της συγκεκριμένης SA.
  - Υπό την έννοια αυτή είναι connection-oriented
- Αν θέλω αμφίδρομη επικοινωνία χρειάζομαι 2 παράλληλες SA

Security Association (SA)

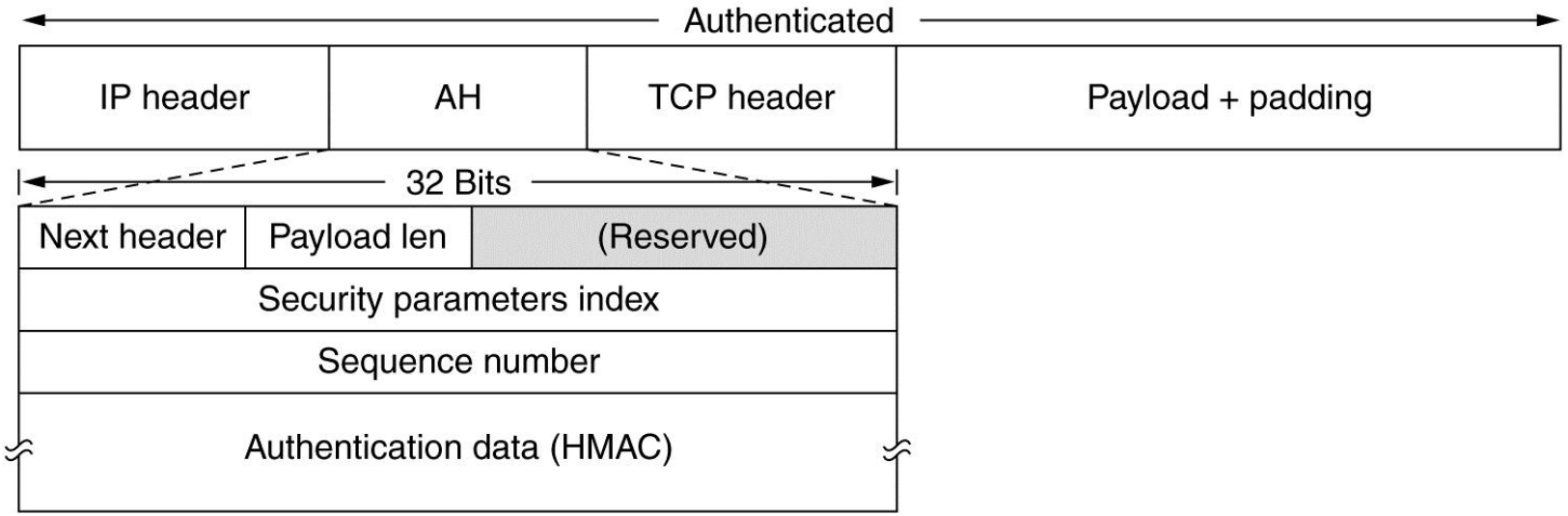
- Απαιτούνται δύο διαδικασίες:
  - η προσθήκη επικεφαλίδων, και
  - η ISAKMP (Internet Security Association and Key Management Protocol) που ασχολείται με την εγκαθίδρυση κλειδιών.

  Η δεύτερη αυτή διαδικασία είναι ιδιαίτερα πολύπλοκη και το πρωτόκολλο υλοποίησης της Internet Key Exchange – IKE) παρουσιάζει κάποιες αδυναμίες

Transport mode

- Υπάρχουν δύο τεχνικές εφαρμογής του IPsec.
- Η πρώτη ονομάζεται transport mode και με αυτή η επικεφαλίδα του IPsec παρεμβάλλεται μεταξύ της IP επικεφαλίδας και της επικεφαλίδας 4ου επιπέδου.
- Η *Transport Mode* παρέχει ασφαλή σύνδεση μεταξύ δύο ακραίων σημείων καθώς ενθυλακώνει το φορτίο ενός IP πακέτου, ενώ η *Tunnel Mode* ενθυλακώνει ολόκληρο το IP πακέτο και προσφέρει ένα εικονικό «ασφαλές άλμα» μεταξύ δύο πυλών. Έτσι, η δεύτερη χρησιμοποιείται για τη δημιουργία παραδοσιακών VPNs όπου το τούνελ δημιουργεί μια ασφαλή σύνδεση πάνω από το μη-ασφαλές Internet.

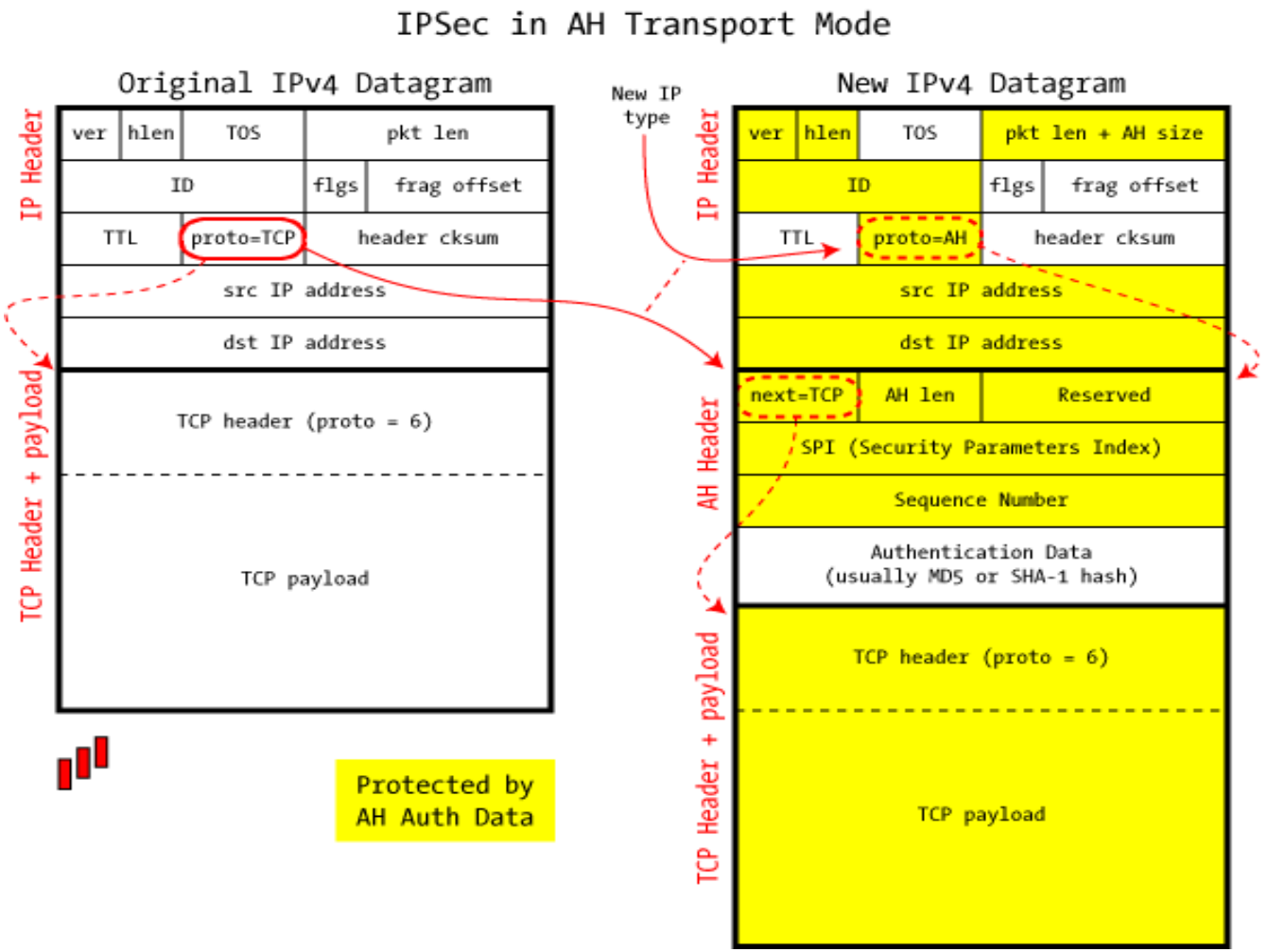
Transport mode IPsec



- Προστίθεται η επικεφαλίδα AH (Authentication Header)
- Το πεδίο Protocol αντικαθίσταται ώστε να δείχνει στο IPsec (port 51) και η αναφορά στο 4ο επίπεδο γίνεται μέσω του IPsec header.

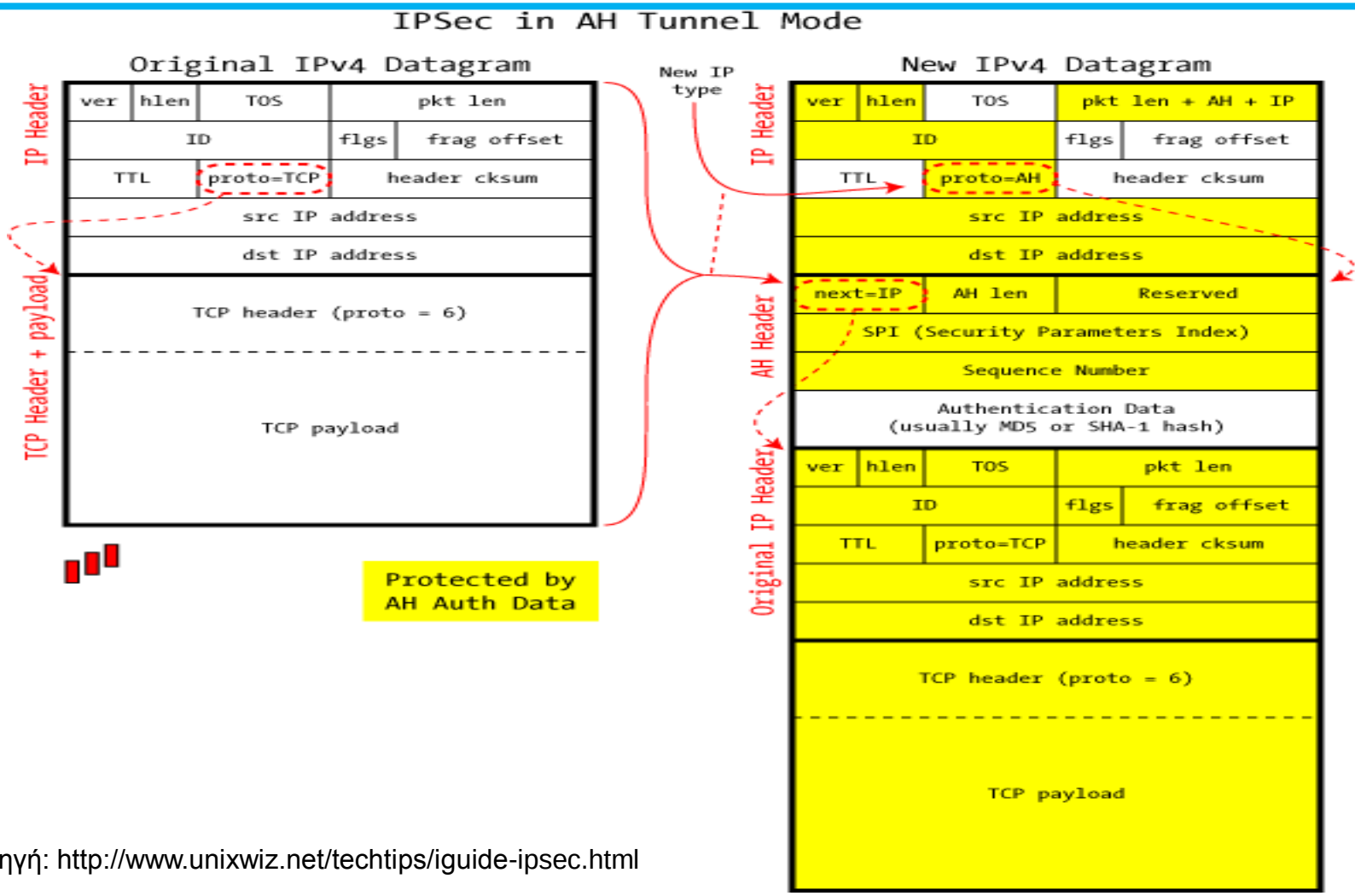
Authentication Header (AH)

- Next Header (π.χ. TCP (06))
- Payload length: αριθμός των 32-bit λέξεων στον AH μείον 2.
- Security Parameters Index: ο αριθμός του εικονικού κυκλώματος ή του SA. Είναι δείκτης που δείχνει σε μια βάση δεδομένων του δέκτη όπου φυλάσσεται το κλειδί της επικοινωνίας μαζί με άλλες παραμέτρους της σύνδεσης.
- Sequence Number: αρίθμηση των πακέτων. Διαφορετική ακόμη και για τις επανεκπομπές. Προστατεύει από replay attacks. Αν τα 2^{32} νούμερα τελειώσουν πρέπει να υλοποιηθεί νέα SA.
- Authentication Data: ψηφιακή υπογραφή του payload. Ενεργείται πάνω στο: payload+κλειδί+(κάποια πεδία του IP header (SA)). Έτσι καλύπτει και την ταυτότητα του αποστολέα. HMAC= Hashed Message Authentication Code


IPSec in AH Transport Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
Protected by
AH Auth Data
New IP
type
New IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len + AH size
ID
flgs
frag offset
TTL
proto=AH
header cksum
src IP address
dst IP address
AH Header
next=TCP
AH len
Reserved
SPI (Security Parameters Index)
Sequence Number
Authentication Data
(usually MD5 or SHA-1 hash)
TCP Header + payload
TCP header (proto = 6)
TCP payload

Tunnel Mode

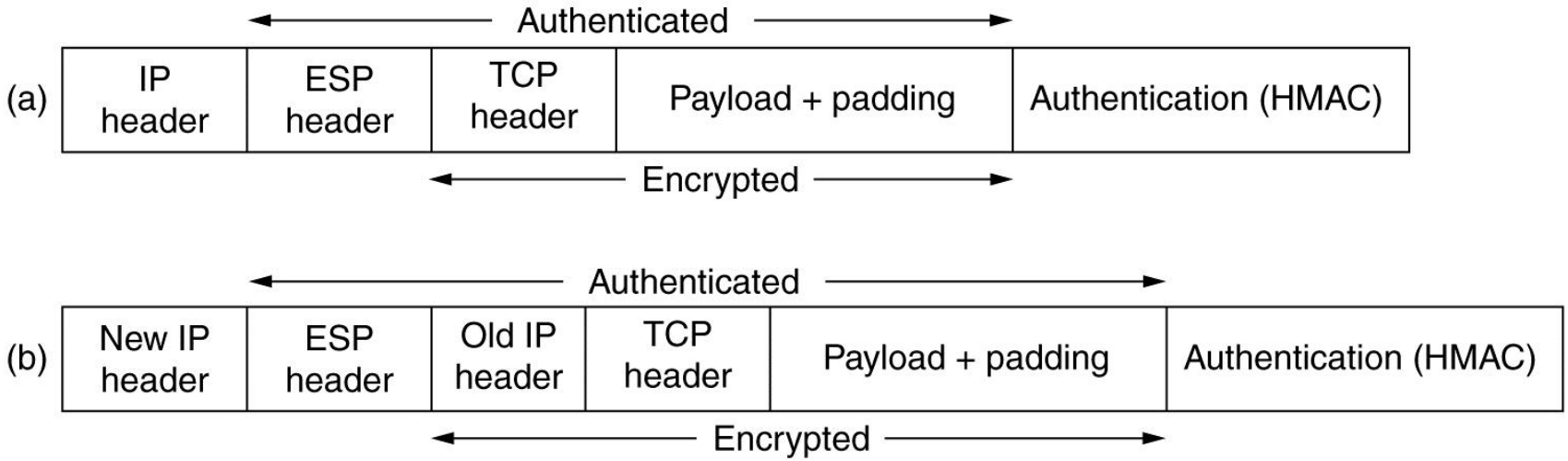
- Γίνεται ενθυλάκωση όλου του IP πακέτου σε ένα νέο IP πακέτο με νέα IP επικεφαλίδα
- Χρησιμοποιείται κυρίως όταν το τούνελ τερματίζει σε μια συσκευή διαφορετική από τον τελικό παραλήπτη του πακέτου
- Η συσκευή αυτή είναι συνήθως ένα firewall και όλα τα δίκτυα που βρίσκονται πίσω από αυτό δε χρειάζεται να γνωρίζουν τίποτα σχετικά με τη χρήση του IPsec
- Η μέθοδος του τούνελ προστατεύει τα δεδομένα και από την περίπτωση της ανάλυσης της κίνησης η οποία σε πολλές περιπτώσεις μπορεί να δώσει αρκετές πληροφορίες σε έναν πιθανό εισβολέα.



Πηγή: http://www.unixwiz.net/techtips/iguide-ipsec.html

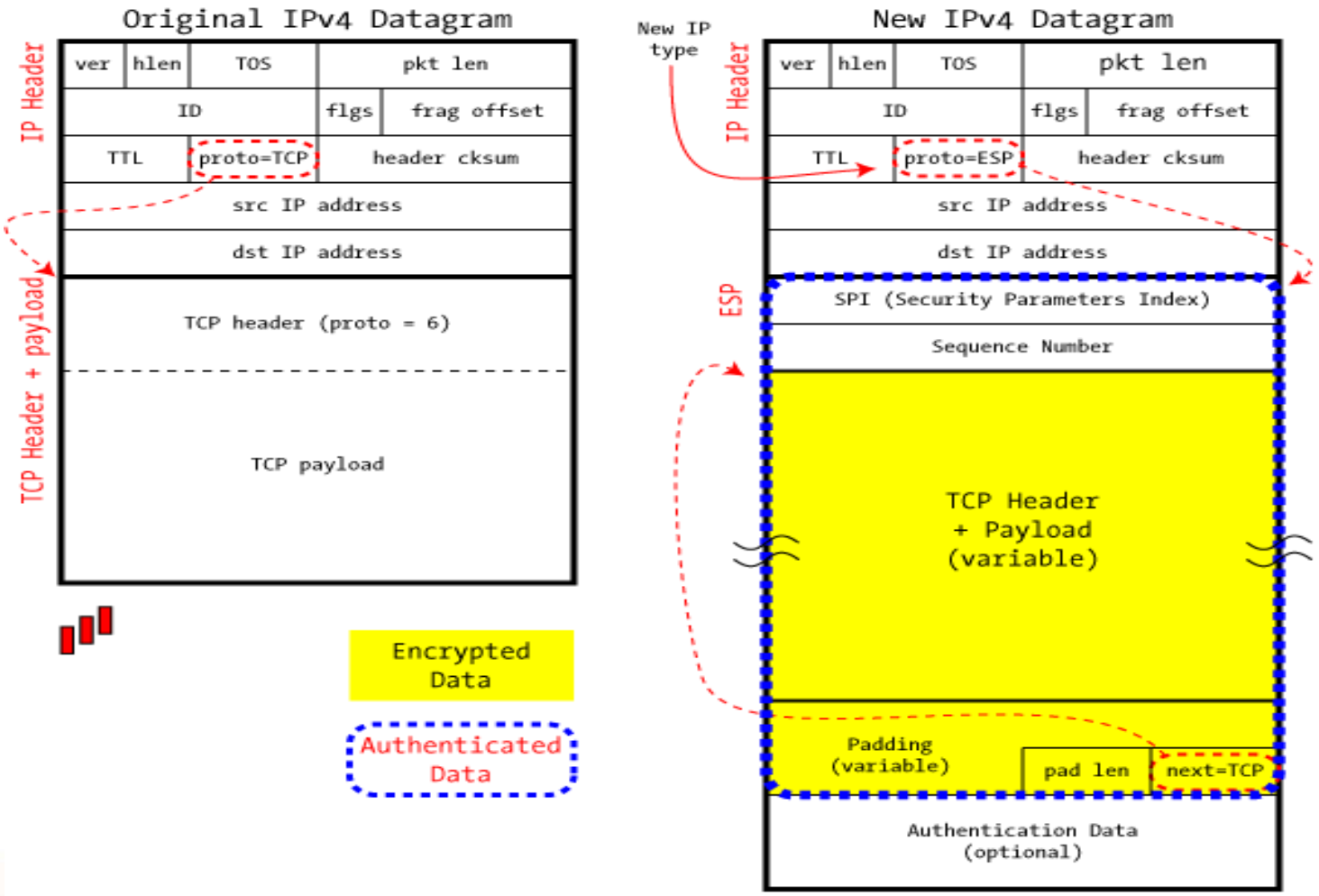
ESP – Encapsulating Security Payload

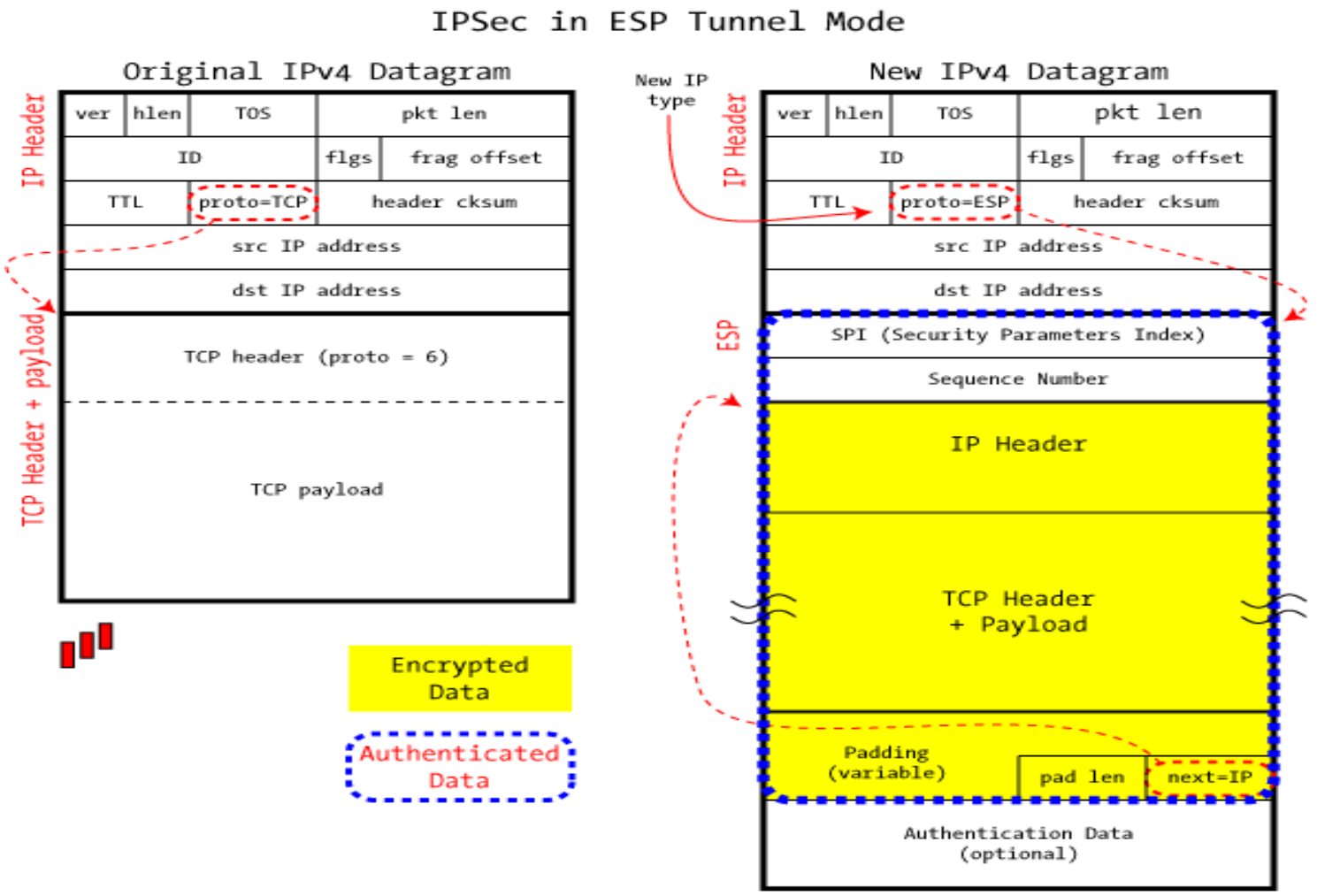
- Εναλλακτικά του AH χρησιμοποιείται η τεχνική ESP που καλύπτει τόσο τις περιπτώσεις transport mode όσο και τις περιπτώσεις tunnel mode.



(a) transport mode. (b) tunnel mode.

IPSec in ESP Transport Mode




IPSec in ESP Tunnel Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
Encrypted Data
Authenticated Data
New IP type
New IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=ESP
header cksum
src IP address
dst IP address
ESP
SPI (Security Parameters Index)
Sequence Number
IP Header
TCP Header + Payload
Padding (variable)
pad len
next=IP
Authentication Data (optional)

Η επικεφαλίδα του ESP

- 2 X 32-bit λέξεις
  - Security parameters index
  - Sequence number
  - Initialization vector (εναλλακτικά για την κρυπτογράφηση)
- ESP trailer
  - HMAC (Hashed Message Authentication Code)
  - Το ότι είναι στο τέλος βοηθάει στην υλοποίηση γιατί μπορεί να υπολογίζεται κατά την έξοδο των πακέτων

TLS/SSL

Γιατί υπάρχει το SSL

1. Κρυπτογράφηση
   - Κρύβω αυτό που μεταδίδεται από τρίτους
2. Ταυτοποίηση
   - Πιστοποιώ ότι αυτός με τον οποίον μιλάω είναι αυτός που λέει

Transport Layer Security (TLS)

- **Τόσο το Transport Layer Security (TLS)** όσο και ο προκάτοχός του, **Secure Sockets Layer (SSL)**, είναι κρυπτογραφικά πρωτόκολλα για την ασφαλή επικοινωνία πάνω από το Internet.
- Το TLS και το SSL κρυπτογραφούν τα πακέτα (segments) του επιπέδου μεταφοράς χρησιμοποιώντας συμμετρική κρυπτογραφία για την μυστικότητα και *message authentication code – MAC* για την αξιοπιστία των μηνυμάτων.
- Οι διάφορες εκδόσεις των πρωτοκόλλων χρησιμοποιούνται ευρύτατα σε εφαρμογές όπως *web browsing, electronic mail, Internet faxing, instant messaging* και *voice-over-IP (VoIP).*
- Το TLS έχει εκδοθεί από την IETF. Η τελευταία έκδοσή του είναι το RFC 5246 και βασίζεται σε προηγούμενες τυποποιήσεις του SLL που ανέπτυξε η Netscape Corporation.

TLS διαδικασία χειραψίας

- A TLS client and server negotiate a stateful connection by using a handshaking procedure.[3] During this handshake, the client and server agree on various parameters used to establish the connection's security.
  - The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported CipherSuites (ciphers and hash functions).
  - From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.
  - The server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA) and the server's public encryption key.
  - The client may contact the server that issued the certificate (the trusted CA as above) and confirm the validity of the certificate before proceeding.
  - In order to generate the session keys used for the secure connection, the client encrypts a random number with the server's public key and sends the result to the server. Only the server should be able to decrypt it, with its private key.
  - From the random number, both parties generate key material for encryption and decryption.
- This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the key material until the connection closes.
- If any one of the above steps fails, the TLS handshake fails and the connection is not created.

Πηγή: "SSL/TLS in Detail". *Microsoft TechNet*. Updated July 31, 2003.

Πώς εμπιστεύομαι κάποιον;

1. Ο οργανισμός ζητά ένα πιστοποιητικό από μια CA
2. Η CA δημιουργεί ένα πιστοποιητικό και το υπογράφει
3. Το πιστοποιητικό εγκαθίσταται στον server του οργανισμού
4. Ο χρήστης διαθέτει έναν φυλλομετρητή στο οποίον έχουν προεγκατασταθεί τα πιστοποιητικά των CA
5. Ο φυλλομετρητής εμπιστεύεται τα πιστοποιητικά των servers που είναι υπογεγραμμένα από αποδεκτή CA

Τέλος Ενότητας