Κρυπτογραφία και Εφαρμογές

Οικονομικό Πανεπιστήμιο Αθηνών

TLS 3.0 – SSL - IPSec

ΓΕΩΡΓΙΟΣ ΣΤΕΡΓΙΟΠΟΥΛΟΣ[1], ΜΑΡΙΟΣ ΑΝΑΓΝΩΣΤΟΠΟΥΛΟΣ[2], ΓΕΩΡΓΙΟΣ ΚΑΜΠΟΥΡΑΚΗΣ[1]

[1] ΤΜΉΜΑ ΜΗΧΑΝΙΚΏΝ ΠΛΗΡΟΦΟΡΙΑΚΏΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΏΝ ΣΥΣΤΗΜΆΤΩΝ ΠΑΝΕΠΙΣΤΉΜΙΟ ΑΙΓΑΊΟΥ

[2] NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY, DEPARTMENT OF INFORMATION SECURITY AND COMMUNICATIONS TECHNOLOGY, GJØVIK, NORWAY

ΠΕΡΙΕΧΟΜΕΝΑ

- Επίπεδο μεταφοράς (transport layer)
  - Πρωτόκολλο SSH
  - Πρωτόκολλο TLS
- Επίπεδο δικτύου (IP)
  - Πρωτόκολλο IPSec

ΕΙΣΑΓΩΓΗ

- Ασφάλεια δικτύου δεν αφορά μόνο την ασφάλεια των συστημάτων στα άκρα.
- Τα κανάλια επικοινωνίας είναι ευάλωτα σε επιθέσεις
  - Υποκλοπή / Αλλοίωση δεδομένων κατά την μεταφορά.
- Χρήση πρωτοκόλλων και τεχνολογιών για προστασία επικοινωνίων:
  - Secure Shell – SSH
  - SSL/ TLS
  - IPSec
  - VPN
  - etc…

Secure Shell - SSH

Secure Shell - SSH

- Έκδοση: 2 (SSHv2)
- Χρήση SSH για:
  - (α) σύνδεση σε απομακρυσμένες οντότητες (remote login) και εκτέλεση εντολών
  - (β) λειτουργίες δημιουργίας ασφαλών συνδέσεων από άκρο-σε-άκρο (tunneling) και προώθησης (forwarding) άλλων υπηρεσιών (π.χ. SMTP και HTTP).
- Μοντέλο πελάτη/εξυπηρετητή (client/server)
- Λειτουργεί κυρίως πάνω από το TCP.
- Port 22.
- Πιο διαδεδομένη υλοποίηση: OpenSSH

Στοίβα πρωτοκόλλων SSH

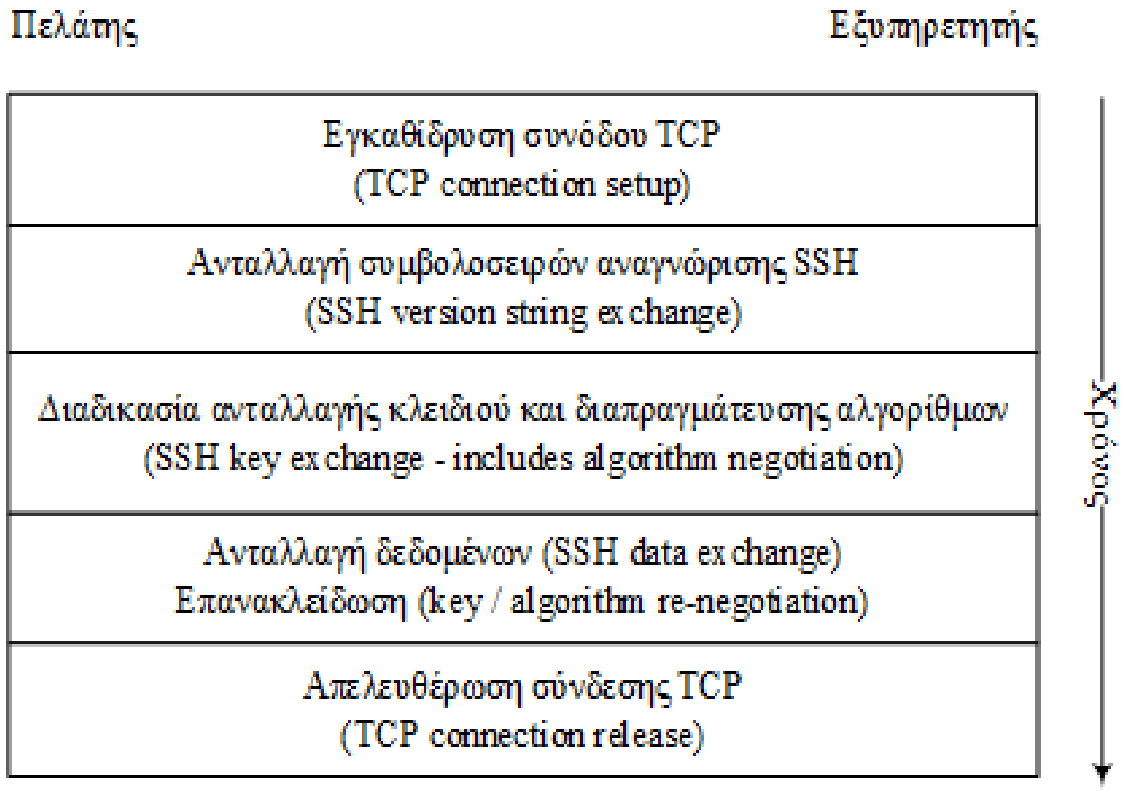
- Αρχιτεκτονική τριών επιπέδων.
  1. Πρωτόκολλο μεταφοράς (peer communication)
     - Επιλογή συμπίεσης, κρυπτογράφησης κτλ.
     - Υπηρεσίες εμπιστευτικότητας και ακεραιότητας
     - Διαδικασία πιστοποίησης ταυτότητας εξυπηρετητή στον πελάτη
  2. Πρωτόκολλο πιστοποίησης ταυτότητας SSH
     - Αυθεντικοποίηση χρήστη στον εξυπηρετητή
  3. Πρωτόκολλο σύνδεσης SSH
     - Εγκαθίδρυση ασφαλών συνόδων (shells), εκτέλεση εντολών κτλ.

Πρωτόκολλο μεταφοράς SSH

- Πέντε στάδια λειτουργικότητας
- Μορφή συμβολοσειράς:

SSH-protoversion-softwareversion SP comments

  - *π.χ. SSH-2.0-billsSSH_3.6.3q3*
  - SP κενό διάστημα και πεδίο comments προαιρετικό.



Πρωτόκολλο μεταφοράς SSH:
Διαδικασία ανταλλαγής κλειδιού SSH

1. ΒΗΜΑ 1: Εκατέρωθεν αποστολή μηνυμάτων SSH_MSG_KEXINIT
   - Χρήση τυχαίων πεδίων για προστασία παραγωγής κλειδιών και αναγνωριστικού συνόδου.
   - First-choice-first προτάσεις αλγορίθμων
     - *Diffie-hellman-group1-sha1 και diffie-hellman-group14-sha1 υποχρεωτικοί στην ανταλλαγή κλειδιών*
     - *Εμπιστευτικότητα: Προτεινόμενη κρυπτογράφηση aes128-cbc, υποχρεωτική 3des-cbc*
     - *Ακεραιότητα: hmac-sha2-256 ως προτεινόμενος, hmac-sha1 υποχρεωτικός*
2. ΒΗΜΑ 2: Έναρξη ανταλλαγής κλειδιού
   - Παράγει δύο τιμές: (α) Ένα κοινό μυστικό κλειδί K, και (β) μια σύνοψη (ex-change hash) H.
   - Βάσει αυτών, δημιουργεί κλειδιά κρυπτογράφησης, ακεραιότητας και αυθεντικοποίησης μηνυμάτων.

Πρωτόκολλο μεταφοράς SSH:
Αλγόριθμος ανταλλαγής κλειδιού

- S Server, C Client,
- p μεγάλος πρώτος αριθμός
- g γεννήτορας ομάδας Z_p^* τάξης q
- V_S και V_C συμβολοσειρές αναγνώρισης S και C
- K_S δημόσιο κλειδί του S (server's public host key),
- I_S, I_C μηνύματα SSH_MSG_KEXINIT S και C αντίστοιχα.

Πρωτόκολλο μεταφοράς SSH:
Αλγόριθμος ανταλλαγής κλειδιού

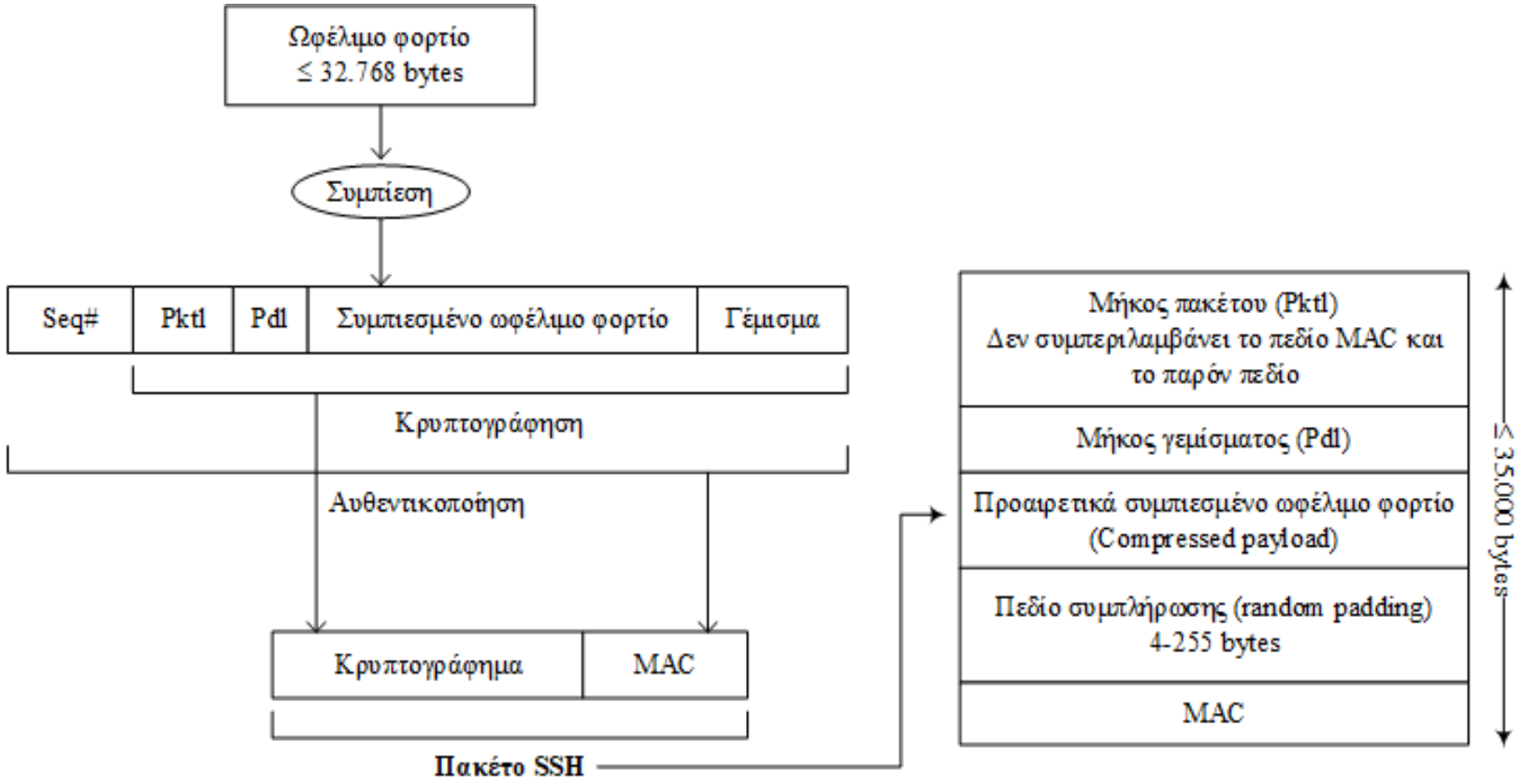
1. C δημιουργεί τυχαία μυστική τιμή x (1 < x < q)
   - $e = g^x \bmod p$ και αποστέλλει e στον S.
2. S δημιουργεί τυχαία μυστική τιμή y (0 < y < q)
   - $f = g^y \bmod p$.
     - Λαμβάνει e και υπολογίζει $K = e^y \bmod p$, κοινό μυστικό κλειδί
   - H = Hash(V_C || V_S || I_C || I_S || K_S || e || f || K) ως αναγνωριστικό συνόδου
   - Υπογράφει το H (s = Sig(H)) με ιδιωτικό κλειδί (private host key).

Πρωτόκολλο μεταφοράς SSH:
Αλγόριθμος ανταλλαγής κλειδιού

3. S αποστέλλει το (K_S || f || s) στον C

4. C επαληθεύει K_S ως host key του S μέσω βάσης δημοσίων κλειδιών και υπολογίζει:
   - $K = f^x \bmod p$, δηλαδή, το κοινό μυστικό κλειδί
   - H = Hash(V_C || V_S || I_C || I_S || K_S || e || f || K), και επαληθεύει την υπογραφή s = Sig(H).

Πρωτόκολλο μεταφοράς SSH:
Ενθυλάκωση και πακέτο SSH



Διαδικασία ενθυλάκωσης και πακέτο SSH

Πρωτόκολλο πιστοποίησης ταυτότητας

- SSH_MSG_SERVICE_REQUEST
  - Δήλωση υπηρεσίας π.χ. ssh-userauth, ssh-connection
- SSH_MSG_USERAUTH_REQUEST
  - Επιλογή μεθόδου αυθεντικοποίησης
- SSH_MSG_USERAUTH_BANNER
  - Λοιπές πληροφορίες προς χρήστη

Μοντέλο εμπιστοσύνης SSH

- Βασίζεται σε πιστοποιητικά δημόσιου κλειδιού
  - Οι πελάτες SSH πρέπει να ελέγχουν το δημόσιο κλειδί (host key) του εξυπηρετητή.
    - Case 1: Συγκρίνοντας το αποτύπωμα του κλειδιού (public key fingerprint) με εκείνο που χρησιμοποιήθηκε σε μια προηγούμενη σύνδεση με τον ίδιο εξυπηρετητή
      - *Προϋποθέτει τοπική βάση (ssh_known_hosts) ή χρήση πιστοποιητικών X.509 από έμπιστη αρχή πιστοποίησης*
    - Case 2: Χρήση πιστοποιητικών του τύπου X.509 που εκδίδονται από μια έμπιστη αρχή πιστοποίησης (certification authority).
- Παρέχεται δυνατότητα παράλειψης του ελέγχου

Επιθέσεις στο SSH

- Επιθέσεις επανεκπομπής μηνυμάτων από προηγούμενες συνόδους (replay attacks)
  - Χρήση cookies, timestamps, session ID, και αριθμό πακέτου (Seq#)
- Επιθέσεις ενδιαμέσου (man-in-the-middle)
  - Οι διαχειριστές μπορούν να αξιοποιήσουν σύγχρονα πρωτόκολλα: Secure Shell fingerprint record (SSHFP) και DNS-based Authentication of Named Entities (DANE) για διανομή αποτυπωμάτων κλειδιών εξυπηρετητών.
- Επιθέσεις άρνησης εξυπηρέτησης (denial-of-service)
  - Δυστυχώς δεν υπάρχει αξιοπιστη λύση
- Ανάλυση της δικτυακής κίνησης (traffic analysis)
  - Αξιοποίηση SSH_MSG_IGNORE μαζί με τη χρήση πεδίων συμπλήρωσης τυχαίου μήκους (random lengths of padding) για αποφυγή ανάλυσης κατά την αυθεντικοποίησης του χρήστη.

TLS v3.0

Transport Layer Security (TLS)

- Πρωτόκολλο ασφαλείας επιπέδου μεταφοράς TCP για την προστασία των μεταδιδόμενων δεδομένων σε ένα δίκτυο.
  - Αναπτύχθηκε από την Internet Engineering Task Force (IETF)
- Απόγονος του Secure Socket Layer (SSL) από Netscape (1995).
- Ευρεία κλίμακα εφαρμογών όπως:
  - Διασφάλιση συνδέσεων με email εξυπηρετητές (π.χ., SMTP, POP, και IMAP),
  - Υπηρεσίες ανταλλαγής μηνυμάτων (π.χ., XMPP)
  - Ασφαλής απομακρυσμένη σύνδεση σε εξυπηρετητή
  - Δημιουργία εικονικών ιδιωτικών δικτύων (VPN) στο επίπεδο μεταφοράς.
  - Κύρια χρήση στις συνδέσεις φυλλομετρητών, δηλαδή στο Hypertext Transfer Protocol Secure (HTTPS).

TLS v1.3

- Χρήση υβριδικού συστήματος κρυπτογράφησης
  - Κρυπτογραφία δημοσίου κλειδιού για ανταλλαγή/παραγωγή συμμετρικών κλειδιών συνόδου, τα οποία ακολούθως χρησιμοποιούνται για τη διασφάλιση των μεταδιδόμενων δεδομένων.
- Παλαιότερες εκδόσεις χρησιμοποιούσαν αλγόριθμο δημοσίου κλειδιού RSA.
  - Όχι μυστικότητα προς τα εμπρός (perfect forward secrecy) – Κλοπή ιδιωτικού κλειδιού = breach of every packet.
  - Προβλήματα υλοποίησης στο SSL (e.g. million-messages attack)
  - Μη αποδοτικός ως προς το χρόνο εκτέλεσης
- Τρέχουσα έκδοση TLS 1.3 περιγράφεται στο RFC 8446. Οι βελτιώσεις της έκδοσης περιλαμβάνουν:
  1. Χρήση εφήμερου Diffie–Hellman (ephemeral Diffie–Hellman) αλγόριθμου
  2. μείωση χρόνου χειραψίας (handshake) με απάλειψη μηνυμάτων από τη διαδικασία
  3. προστασία των περισσοτέρων μηνυμάτων κατά τη διάρκεια της χειραψίας
  4. ενίσχυση έναντι γνωστών επιθέσεων
  5. απάλειψη μηχανισμών και κρυπτοσουιτών που θεωρούνταν μη ασφαλείς ή ξεπερασμένες.

TLS v1.3

- Σημαντικές αλλαγές στη διαδικασία αυθεντικοποίησης των δύο μερών
  - Ο μηχανισμός ψηφιακών υπογραφών RSA-PKCS#1 v1.5, δεν χρησιμοποιείται για υπογραφή των μηνυμάτων χειραψίας.
  - Χρήση εξελιγμένου RSASSA-PSS (RSA-Probabilistic Signature Scheme) ή του ECDSA (Elliptic Curve Digital Signature).
  - Επανασχεδιασμός διαδικασίας χειραψίας
    - Τα μηνύματα εξυπηρετητή πλέον προστατεύονται με ψηφιακή υπογραφή (στην παλαιότερη διαπραγμάτευση αλγορίθμων, μεταδίδονταν μη προστατευμένα).
- Νέες λειτουργίες τοποθετούνται ως επεκτάσεις στις TLS εγγραφές για backwards compatibility.

Προσφερόμενες υπηρεσίες ασφαλείας

- Αυθεντικοποίηση υποχρεωτικά για τον εξυπηρετητή και προαιρετικά για τον πελάτη.
  - Χρήση ψηφιακών πιστοποιητικών ή προ-μοιρασμένου συμμετρικού κλειδιού (PSK)
- Εμπιστευτικότητα μεταδιδόμενων δεδομένων μέσω κρυπτογραφημένης συνόδου.
  - + προστασία από επιθέσεις ανάλυσης της δικτυακής κίνησης μέσω padding.
  - *Worse attack than you might think*
- Αυθεντικοποίηση της διαδικασίας εγκαθίδρυσης των συμμετρικών κλειδιών
- Ενδιάμεσο (shim) επίπεδο ανάμεσα στο επίπεδο μεταφοράς και εφαρμογών
  - Ανάγκη χρήσης καθορισμένων θυρών για κάθε πρωτόκολλο εφαρμογής με υποστήριξη TLS. Πχ. HTTPS στην 443, ενώ FTP Secure (FTPS) στην 990.

Προσφερόμενες υπηρεσίες ασφαλείας

- **Δύο υπό-πρωτόκολλα.**
- Πρωτόκολλο εγγραφών (TLS record protocol)
  - Ενθυλάκωση και μετάδοση των ανταλλασσόμενων δεδομένων του επιπέδου εφαρμογής καθώς και αυτών που παράγονται από το πρωτόκολλο χειραψίας (TLS handshake protocol).
  - Παρέχει μηχανισμούς για τις υπηρεσίες εμπιστευτικότητας και ακεραιότητας, καθώς και την προστασία από επιθέσεις επανεκπομπής παλαιότερων μηνυμάτων (replay attacks).
- Πρωτόκολλο χειραψίας (TLS handshake protocol)
  - Διαπραγμάτευση των παραμέτρων ασφαλείας μιας σύνδεσης
  - Υπεύθυνο για την αυθεντικοποίηση των δύο μερών

Πρωτόκολλο εγγραφών

- Λαμβάνει δεδομένα από τα πρωτόκολλα υψηλότερων επιπέδων και να παρέχει τις υπηρεσίες κατακερματισμού, αυθεντικοποίησης και κρυπτογράφησης δεδομένων
- Δέχεται ως είσοδο ένα μπλοκ δεδομένων αυθαίρετου μήκους και το κατατμεί σε εγγραφές με μέγιστο μήκος 2^{14} bytes η καθεμία.
- Τέσσερεις τύποι εγγραφών: handshake, application_data, alert, και change_cipher_spec
  - Η τελευταία χρησιμοποιείται μόνο για λόγους συμβατότητας.
  - Κάθε τύπος εγγραφής περιέχει πεδία: content type, legacy record version, Length, fragment, 64-bit αριθμό ακολουθίας (sequence number)

Πρωτόκολλο χειραψίας

- Τρείς βασικές λειτουργίες:
  1. Εφήμερο DH αλγόριθμο με ή χωρίς τη χρήση ελλειπτικών καμπυλών ((EC)DHE)
  2. Προ-μοιρασμένο κλειδί (PSK-only)
  3. Προ-μοιρασμένο κλειδί με χρήση εφήμερου DH αλγορίθμου (PSK με (EC)DHE).

1. Μετά την εγκαθίδρυση μιας συνόδου TCP, οι TLS οντότητες εκκινούν τη διαδικασία χειραψίας προκειμένου να συμφωνήσουν στις παραμέτρους ασφαλείας.
   1. **Ανταλλαγή κλειδιών**: εγκαθιδρύονται τα κοινά κλειδιά και συμφωνούνται οι κρυπτογραφικές παράμετροι
   2. **Παράμετροι εξυπηρετητή**: miscellaneous προαιρετικά flags
   3. **Αυθεντικοποίηση**: Υποχρεωτικά εξυπηρετητή/προαιρετικά πελάτη. Επιβεβαιώνεται η χρήση των κλειδιών και η ακεραιότητα της χειραψίας.

Αυθεντικοποίηση - Πρωτόκολλο χειραψίας

1. Ο εξυπηρετητής στέλνει ψηφιακό πιστοποιητικό του και οποιαδήποτε επέκταση.
2. Ο εξυπηρετητής στέλνει την ψηφιακή υπογραφή προηγούμενων μηνυμάτων της χειραψίας υπογεγραμμένη με το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί του πιστοποιητικού που στάλθηκε.
   - Επιβεβαιώνει ότι ο εξυπηρετητής κατέχει το ιδιωτικό κλειδί του πιστοποιητικού που δήλωσε.
   - Επιβεβαιώνεται η ακεραιότητα όλων των προηγούμενων μηνυμάτων της χειραψίας.
3. Ο εξυπηρετητής στέλνει το HMAC των προηγούμενων μηνυμάτων της χειραψίας. Το κλειδί για τη διαδικασία MAC παράγεται από το συμφωνημένο κοινό κλειδί της συνόδου με χρήση της συνάρτησης HKDF.
   - Επιβεβαιώνει τη συμφωνία του κοινού κλειδιού και συνδέει τη χρήση του με τις συγκεκριμένες οντότητες
4. Ο πελάτης στέλνει το πιστοποιητικό. Στην περίπτωση που δε διαθέτει, η λίστα είναι κενή.
5. Αν είχε στείλει το πιστοποιητικό του, ο πελάτης επιβεβαιώνει το ιδιωτικό κλειδί του.
6. Ο πελάτης αποκρίνεται με το μήνυμα Finished και ολοκληρώνεται η χειραψία.

IPSEC

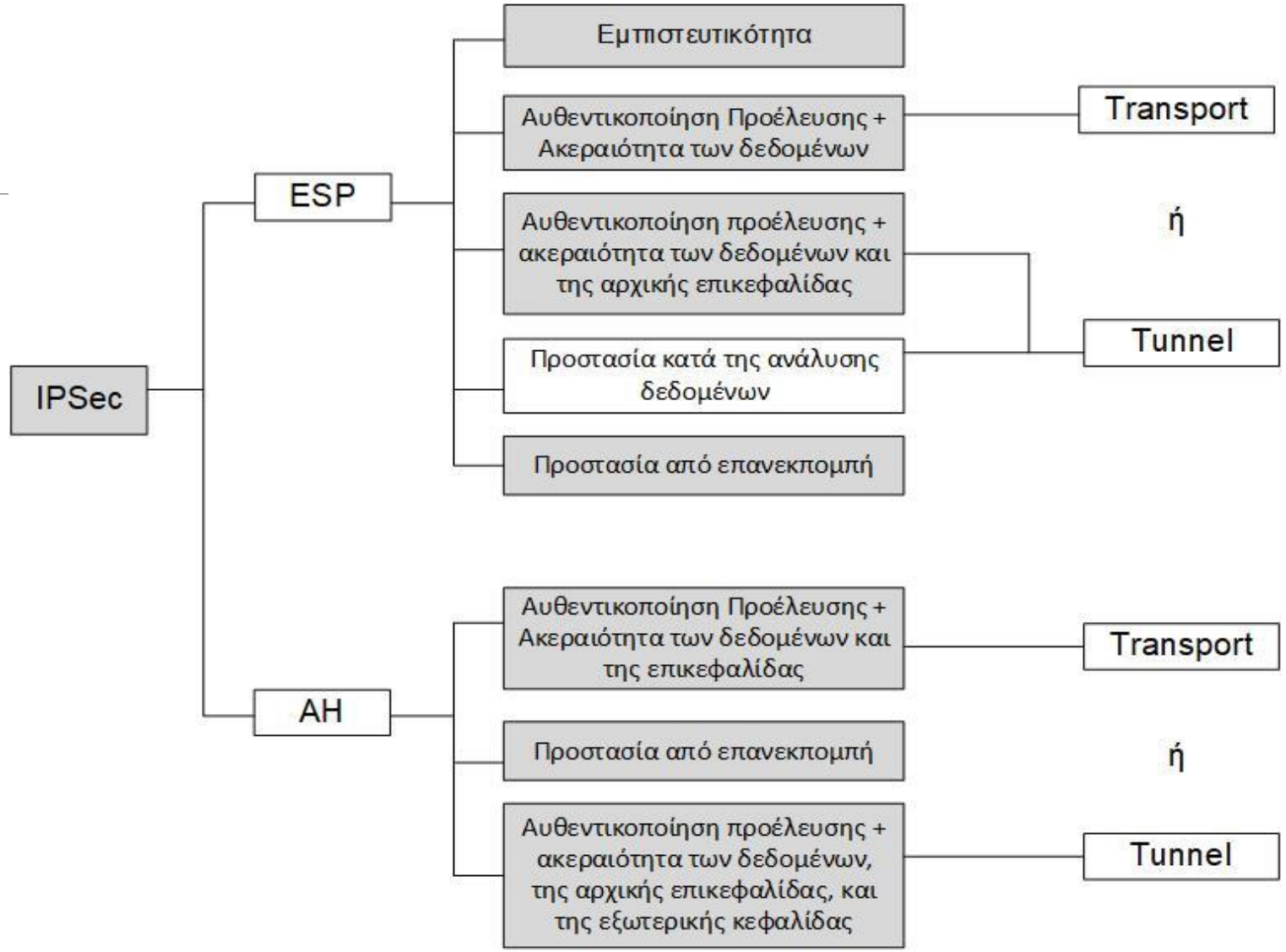
IPSEC

- Σύνολο πρωτοκόλλων που αναπτύχθηκε από τον IETF με σκοπό την ενσωμάτωση δυνατοτήτων ασφάλειας στο πρωτόκολλο IP.
- Υλοποιείται στο επίπεδο δικτύου (IP) με σημαντικό πλεονέκτημα ότι είναι διαφανές ως προς το επίπεδο εφαρμογών.
- Μπορεί να χρησιμοποιηθεί από το IPv4, ενώ αποτελεί αδιάσπαστο τμήμα του IPv6.
- Κύρια χρήση η ανάπτυξη εικονικών ιδιωτικών δικτύων (Virtual Private Network - VPN).
- Βασικές υπηρεσίες ασφάλειας:
  - Αυθεντικοποίηση (IP-level authentication) και ακεραιότητα δεδομένων
  - Εμπιστευτικότητα
  - Προστασία από επιθέσεις επανεκπομπής μηνυμάτων

Γενική Αρχιτεκτονική IPSEC

- Μηχανισμός Αυθεντικοποίησης Επικεφαλίδας (Authentication Header - AH) και Μηχανισμός Κρυπτογράφησης (Encapsulating Security Payload - ESP)
- Πρωτόκολλο ανταλλαγής κλειδιών Internet Key Exchange (IKE)
  - Διαχείριση και ασφαλή διανομή των κλειδιών
- Βάση πολιτικών ασφάλειας (Security Policy Database - SPD)
  - Ορίζονται πολιτικές επεξεργασίας πακέτων, π.χ. αν θα πρέπει να το απορρίψει η σύνδεση
- Βάση συσχετίσεων ασφαλείας (Security Association Database - SAD)
  - Αποθηκεύονται οι συγκεκριμένοι παράμετροι ασφαλείας που συμφωνήθηκαν
- Δυο καταστάσεις λειτουργίας:
  - Λειτουργία διόδου (Tunnel Mode): Παρέχεται προστασία σε ολόκληρο το IP πακέτο
  - Λειτουργία Μεταγωγής (Transport Mode): Η επικεφαλίδα του IP πακέτου μεταδίδεται μη κρυπτογραφημένη

Υπηρεσίες ασφάλειας IPSec

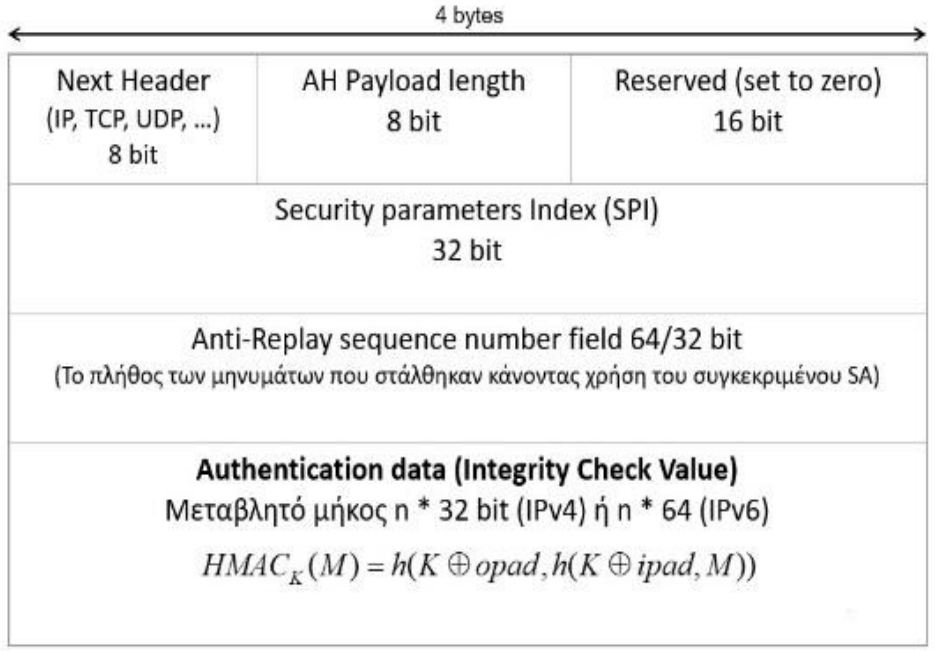


Συσχετίσεις Ασφαλείας (SA) IPSEC

- Συμφωνία μεταξύ δύο μερών που θέλουν να επικοινωνήσουν, σε υπηρεσίες ασφαλείας που επιθυμούν να χρησιμοποιήσουν καθώς και στον τρόπο που αυτές πρόκειται να παρασχεθούν.
  - Μονόδρομη σχέση μεταξύ του αποστολέα και του παραλήπτη
  - Ένα πακέτο μπορεί να αυθεντικοποιηθεί και αποκρυπτογραφηθεί μόνον αν συνδέεται με μια ενεργή SA
- Βασικές πληροφορίες που περιλαμβάνει:
  - **Επιλογείς** (SPD Selectors): IP διεύθυνση πηγής και προορισμού, οι θύρες (ports) πηγής και προορι-σμού, το πρωτόκολλο του επόμενου (ανώτερου) επιπέδου κτλ.
  - **Κατάσταση λειτουργίας**: λειτουργία μεταγωγής ή διόδου
  - **Δεδομένα για αυθεντικοποίηση**: κλειδιά, AH αλγόριθμος αυθεντικοποίησης
  - **Δεδομένα για εμπιστευτικότητα**: ESP αλγόριθμος, κλειδιά, και διάνυσμα αρχικοποίησης (IV), αν υπάρχει
  - **Δείκτης παραμέτρων ασφαλείας** (Security Parameter Index): πρωτόκολλα ασφαλείας έχουν χρησιμοποιηθεί
  - **Αριθμός ακολουθίας**
  - **Διάρκεια ζωής**: Κάθε SA ισχύει μόνο για συγκεκριμένο διάστημα ή όγκο δεδομένων που μεταδόθηκε

Μηχανισμός Αυθεντικοποίησης Επικεφαλίδας (AH)

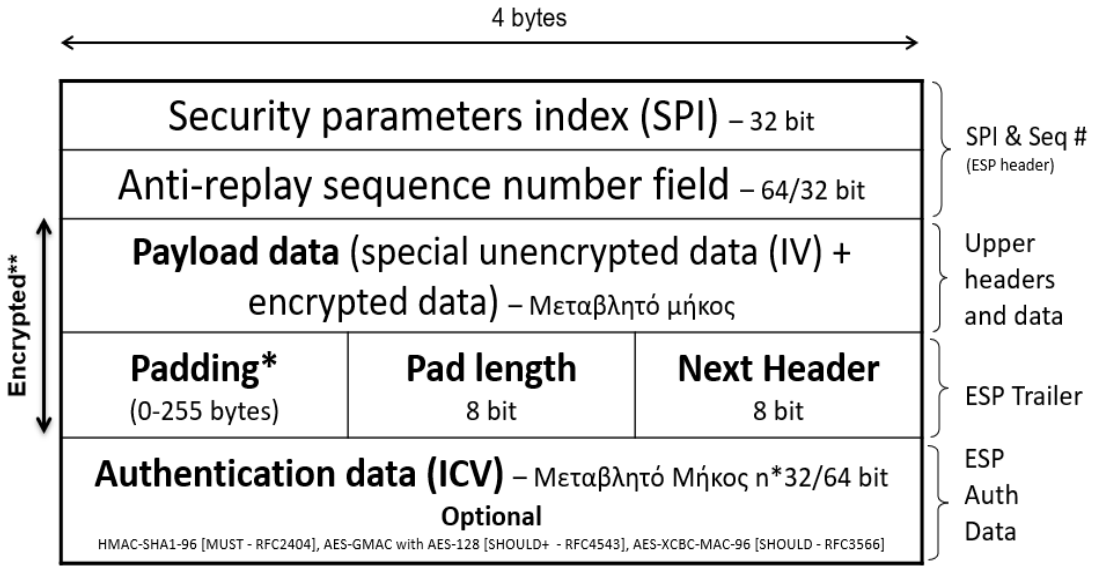
- Διασφαλίζει την αυθεντικοποίηση προέλευσης των δεδομένων, την ακεραιότητα των δεδομένων αλλά και την αποφυγή επιθέσεων επανεκπομπής.
  - Next Header: Τύπος επικεφαλίδας που ακολουθεί την AH, π.χ., ESP=50, TCP=6, UDP=17, SCTP=132, ICMP=1, κ.ά.
  - Payload Length: Μήκος AH επικεφαλίδας
  - SPI: SA για το πακέτο
  - Sequence number field: Πλήθος μηνυμάτων που στάλθηκαν από τον αποστολέα
  - Authentication data: Πεδίο μεταβλητού μήκους (96 ή 128 bits) με τιμή ελέγχου ακεραιότητας (ICV).



Μορφή επικεφαλίδας AH

Μηχανισμός Ασφαλούς Ενθυλάκωσης Ωφέλιμου Φορτίου (ESP)

- Παρέχει υπηρεσίες αυθεντικοποίησης και ακεραιότητας των IP πακέτων και επιπλέον εμπιστευτικότητα με εφαρμογή αλγορίθμων κρυπτογράφησης.
- Αποτελείται από τα πεδία SPI και αριθμός ακολουθίας (Sequence number) και ένα κρυπτογραφημένο ESP trailer που περιλαμβάνει τα πεδία Padding, Pad length, και Next Header.



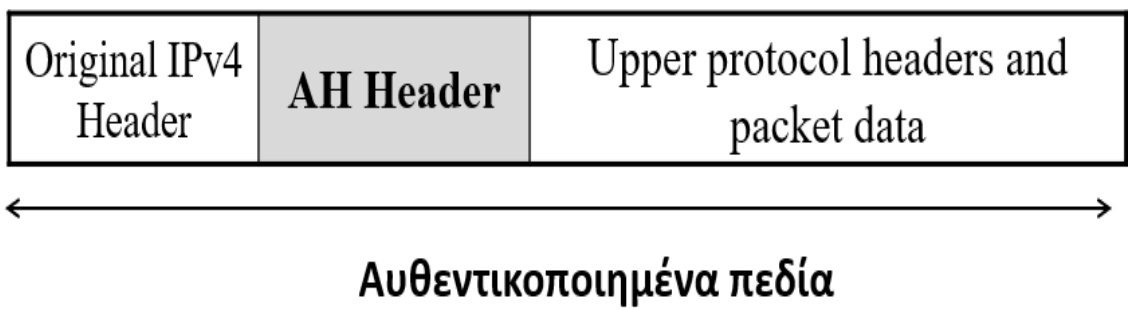
Μορφή επικεφαλίδας ESP

AH vs ESP

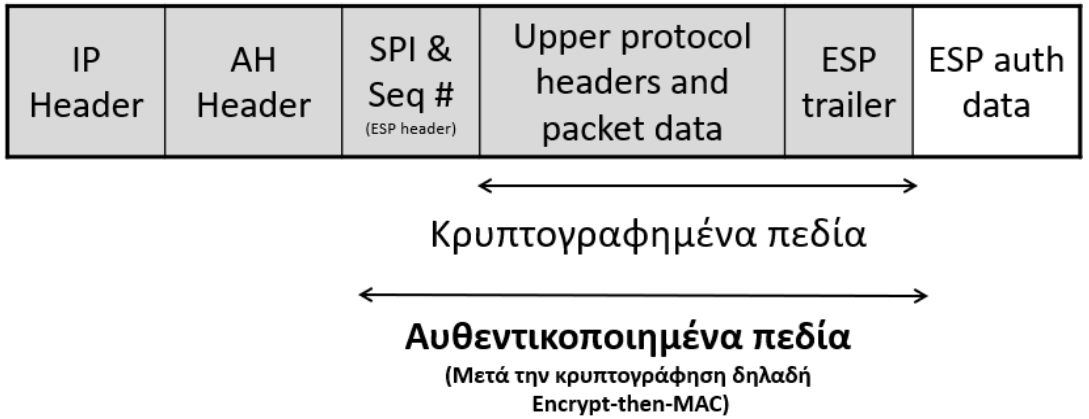
- Το πρωτόκολλο AH παρέχει ένα μηχανισμό μόνο για έλεγχο ταυτότητας.
  - Η ακεραιότητα των δεδομένων εξασφαλίζεται με τη χρήση μιας σύνοψης μηνυμάτων
  - Το AH ελέγχει κεφαλίδες IP και τα ωφέλιμα φορτία τους, με εξαίρεση ορισμένα πεδία που μπορούν να αλλάξουν κατά τη μεταφορά
- Το ESP παρέχει εμπιστευτικότητα δεδομένων (κρυπτογράφηση) και έλεγχο ταυτότητας (ακεραιότητα δεδομένων, έλεγχος προέλευσης δεδομένων και προστασία αναπαραγωγής).
  - Λειτουργεί ως: confidentiality only, authentication only, ή μαζί confidentiality and authentication.
- Όταν το ESP παρέχει λειτουργίες ελέγχου ταυτότητας, χρησιμοποιεί ίδιους αλγόριθμους με το AH, αλλά η κάλυψη είναι διαφορετική.
  - Ο έλεγχος ταυτότητας τύπου AH ελέγχει την ταυτότητα ολόκληρου του πακέτου IP, συμπεριλαμβανομένης της εξωτερικής κεφαλίδας IP
  - Ο μηχανισμός ελέγχου ταυτότητας ESP ελέγχει την ταυτότητα μόνο το datagram του πακέτου IP.

Κατάσταση Μεταγωγής vs Κατάσταση Διόδου

- Στην κατάσταση μεταγωγής μόνο το ωφέλιμο φορτίο είναι αυτό που κρυπτογραφείται ενώ οι αρχικές κεφαλίδες του IP πακέτου όχι.



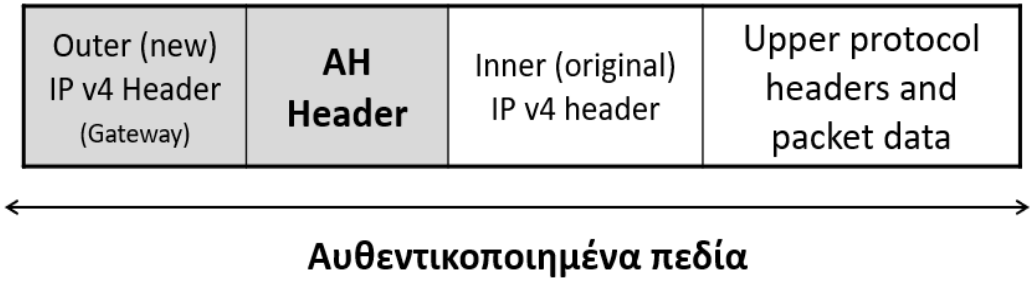
AH header σε κατάσταση μεταγωγής



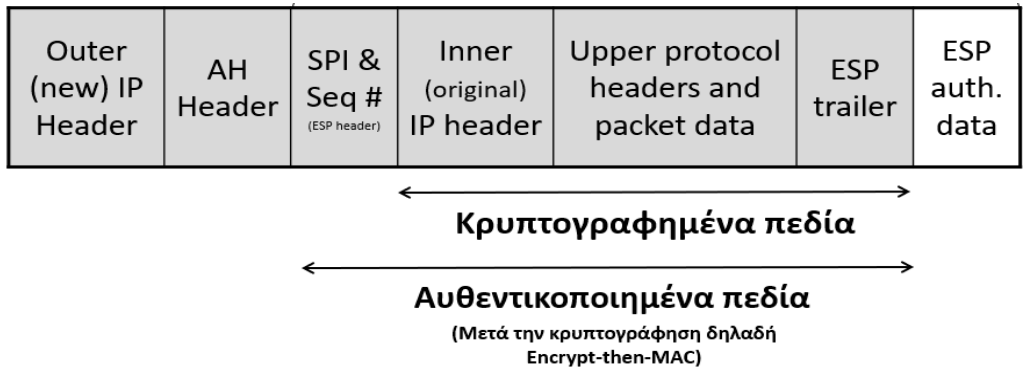
ESP header σε κατάσταση μεταγωγής

Κατάσταση Μεταγωγής vs Κατάσταση Διόδου

- Στην κατάσταση διόδου κρυπτογραφείται ολόκληρο το πακέτο IP συμπεριλαμβανομένων των IP διευθύνσεων
- Διαμορφώνεται νέο πακέτο IP, το οποίο έχει ως ωφέλιμο φορτίο το αρχικό.



AH header σε κατάσταση διόδου



ESP header σε κατάσταση διόδου

Βιβλιογραφία

Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο, NewTech Pub, επ. Επιμέλεια: Σωκράτης Κ. Κάτσικας, Στέφανος Γκρίτζαλης, Κωνσταντίνος Λαμπρινουδάκης

https://newtech-pub.com/βιβλία/πληροφορική/ασφάλεια-διοίκηση-έργου/ασφάλεια-πληροφοριών-συστημάτων-στο/