Ασφάλεια Δικτύων

Δρ. Μαριάς Ιωάννης, Λέκτορας
marias@aueb.gr

Περιεχόμενα

- Ασφάλεια σε επίπεδο δικτύου
  - IPSec
    - AH/ESP
    - Transport mode / Tunnel Mode
    - Key management

Ασφάλεια στο διαδίκτυο

- Το TCP/IP δεν σχεδιάστηκε αρχικά με στόχο την παροχή υπηρεσιών διασφάλισης
  - Απορρήτου των επικοινωνιών
  - Αυθεντικοποίηση επικοινωνούντων
  - Μη-αποποίηση επικοινωνίας
  - Ακεραιότητα μηνυμάτων
- Σήμερα υπάρχει αυξημένη ανάγκη διασφάλισης
  - Κάτω από διαφορετικές πολιτικές
  - Που ορίζονται από χρήστες, παρόχους υπηρεσιών, φορείς μετάδοσης, κατόχους περιεχομένου, aggregators, κατασκευαστές, διαχειριστές λειτουργίας, κυβερνήσεις
  - Που ορίζουν διαφορετικά επίπεδα και ανάγκες ασφάλειας

Ασφάλεια στο διαδίκτυο

- Ωστόσο: Ασφάλεια στο διαδίκτυο είναι μια συνεχής, πολυδιάστατη, διαδικασία
  - ένα σύνολο κανόνων, υλικού, λογισμικού, και ανθρώπων
- Δεν είναι μόνο ένα προϊόν
  - Ούτε μια ανακάλυψη (patent) ή ένα RFC
- Η εφαρμογή της εξαρτάται από τις απαιτήσεις που ορίζουν (άμεσα ή έμμεσα)
  - τα επίπεδα του μοντέλου OSI που θα εφαρμοστεί
  - τα σημεία του δικτύου που θα εφαρμοστεί
    - Υπολογιστές, διακομιστές, δρομολογητές, ειδικές διατάξεις (firewalls)
  - ποιος θα της εφαρμόσει
    - Χρήστης, ISP, τρίτος έμπιστος

Ασφάλεια στο διαδίκτυο

- Απειλές έναντι εμπιστευτικότητας
  - Παθητικές επιθέσεις
  - Ωτακοή κατά τη μετάδοση
  - Υποκλοπή δεδομένων και πληροφοριών από εξυπηρέτες, διακομιστές, υπολογιστές χρηστών
  - Διαπίστωση θέσης χρηστών
  - Αναγνώριση άκρων της επικοινωνίας
  - Ανάγνωση διάρθρωσης δικτύου
- Επιπτώσεις
  - Απώλεια ιδιωτικότητας
  - Βήμα για ενεργητικές (πιο μοχθηρές) επιθέσεις

Ασφάλεια στο διαδίκτυο

- Απειλές έναντι αυθεντικότητας
  - Πλαστογράφηση δεδομένων – πληροφοριών κατά την μετάδοση ή αποθήκευση
  - Πλαστογράφηση γνήσιων οντοτήτων
- Επιπτώσεις
  - Αβεβαιότητα γνησίου πληροφοριών
  - Πίστη ότι η λανθασμένη πληροφορία είναι έγκυρη
  - Απώλεια εγκυρότητας
  - Υποκλοπή ταυτοτήτων
  - Απώλεια φήμης για το γνήσιο χρήστη – υπηρεσία
    - πιθανή μελλοντική απάρνηση υπηρεσίας

Ασφάλεια στο διαδίκτυο

- Απειλές έναντι ακεραιότητας
  - Τροποποίηση δεδομένων
  - Τροποποίηση μηνυμάτων κατά τη μετάδοσή τους
  - Μεταβολή δεδομένων στη μνήμη δικτυακών συσκευών
    - Π.χ. Πινάκων δρομολόγησης
- Επιπτώσεις
  - Ενόχληση
  - Διαφοροποίηση ερμηνείας δεδομένων
  - Απώλεια πληροφοριών
  - Αποτροπή λειτουργίας
  - απομόνωση δικτύων, διακομιστών, υπολογιστών πελάτη

Ασφάλεια στο διαδίκτυο

- Απειλές έναντι διαθεσιμότητας
  - Πλημμυρίδα δικτύου, εμποδίζει κίνηση «νόμιμων» πακέτων;
  - Υπερφόρτωση εξυπηρέτη με αποστολή περισσότερων αιτημάτων από αυτά που μπορεί να διαχειριστεί
  - Εμπόδιο στην πρόσβαση ενός ατόμου σε μια υπηρεσία
- Επιπτώσεις
  - Χαμηλή απόδοση δικτύου
  - Μη διαθεσιμότητα web site
  - Αδυναμία πρόσβασης στο δίκτυο
  - Απώλεια φήμης

IPsec Περιεχόμενα

- Ασφάλεια σε επίπεδο δικτύου – IPsec framework
  - Αυθεντικοποίηση
  - Κρυπτογράφηση
  - Μέθοδοι Λειτουργίας (modes)
  - Σύνοδοι ασφάλειας
  - Διαχείριση κλειδιών

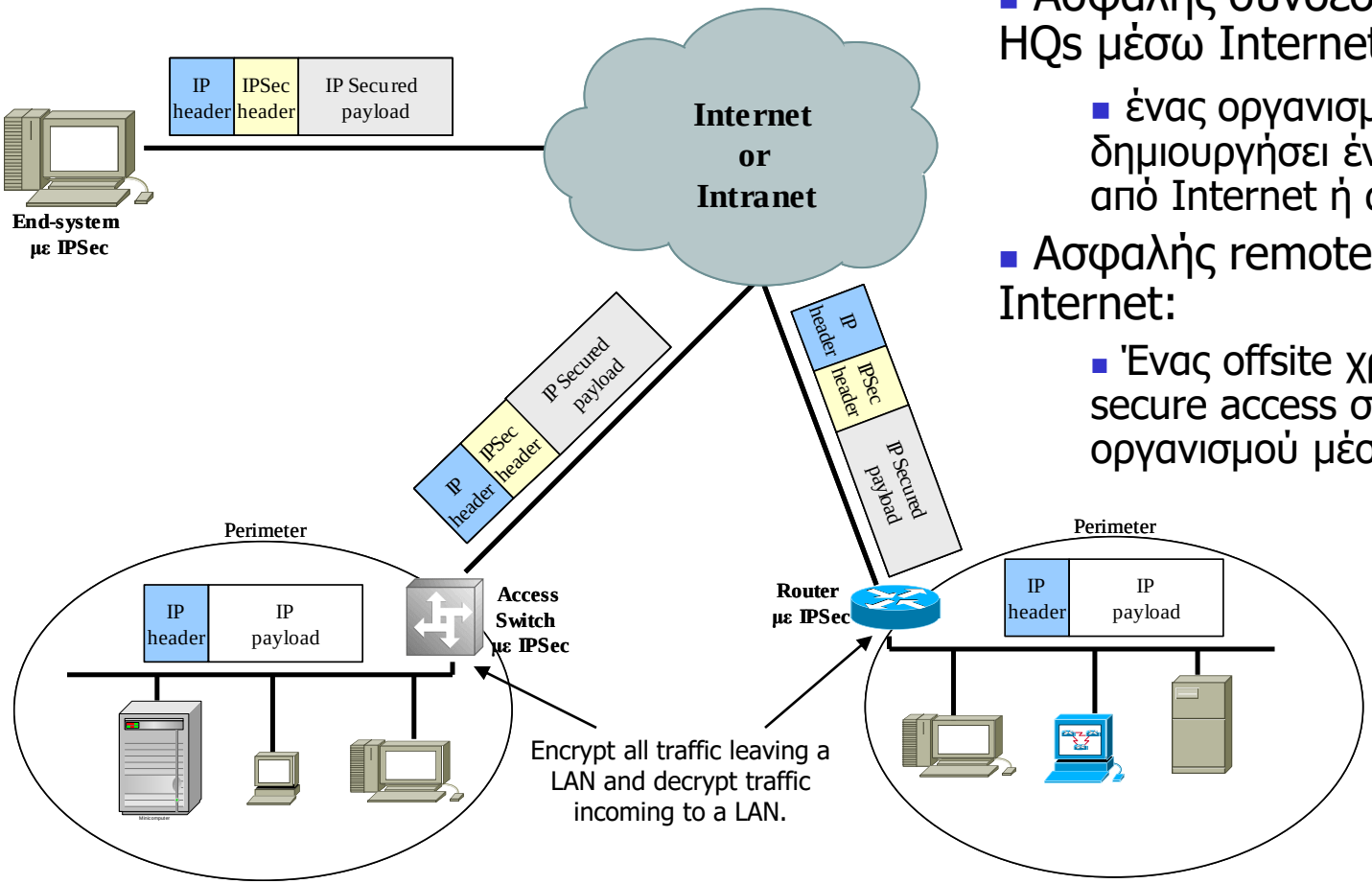
IPsec – Γενικά

- Μέθοδοι λιετουργίας
  - Από άκρο-σε-άκρο ήτοι host-to-host (transport mode) ή
  - Από δίκτυο-σε-δίκτυο ήτοι IPgateway-σε-IPgateway (tunnel mode)
- Μπορεί να χρησιμοποιηθεί
  - Σε τοπικά δίκτυα (LANs)
  - Σε public (π.χ., Internet) ή private WANs (Intranets)
  - Σε extranets (offsite worker με dialup μέσω ISP)
- Αν υλοποιείται σε router, access switch ή firewall (IP gateways), παρέχει ισχυρή ασφάλεια για όλη την κυκλοφορία που διαπερνά την περίμετρο

IPsec – Γενικά

- Λειτουργεί διάφανα προς τον τελικό χρήστη
  - δεν είναι ανάγκη να εκπαιδευτεί σε κρυπτογραφία / μεθόδους ανταλλαγής κλειδιών
- Λειτουργεί σε IP επίπεδο, κάτω από TCP/UDP, άρα διάφανο προς εφαρμογές χρήστη (π.χ., http, ftp)
  - Δεν χρειάζεται να αλλάξουν
- Μπορεί να εφαρμοστεί σε διακριτές συσκευές ή χρήστες
  - όχι σε όλη την κυκλοφορία μεταξύ sites
  - Μέσω Security Associations
- Εφαρμογή σε IPv4 και IPv6

IPSec – Δυο κύριες Εφαρμογές



- Ασφαλής σύνδεση branch office μέ HQs μέσω Internet:
  - ένας οργανισμός μπορεί να δημιουργήσει ένα secure VPN πάνω από Internet ή από public WAN.
- Ασφαλής remote access μέσω Internet:
  - Ένας offsite χρήστης απολαμβάνει secure access στο δίκτυο του οργανισμού μέσω Internet.

IPSec – Στόχοι

- Data Origin Authentication
  - επαληθεύει ότι κάθε πακέτο προέρχεται από τον αποστολέα που ισχυρίζεται ότι το έστειλε.
- Data integrity
  - επαληθεύει ότι τα περιεχόμενα κάθε πακέτου δεν έχουν αλλάξει κατά τη μεταφορά τους, είτε κακόβουλα είτε τυχαία

  E_k[HMAK(k,M,SeqNr)**]||** **E_k [**M||**SeqNr]** (δύο IP άκρα επικοινωνίας που μοιράζονται μυστικό k)
- Data confidentiality
  - το μήνυμα κρυπτογραφείτε κατά την αποστολή του ώστε να μην μπορεί κάποιος ενδιάμεσος να το διαβάσει
- Replay protection
  - Εξασφαλίζει ότι κάποιος τρίτος δεν μπορεί υποκλέπτοντας ένα πακέτο και να το ξαναστείλει μετά από κάποιο χρονικό διάστημα
    - Rejection of replayed IP packets
- Διαχείριση κρυπτογραφικών κλειδιών και Security Associations

IPsec Security Associations

- Το IPSec παρέχει ποικίλες επιλογές για τη χρήση αλγορίθμων κρυπτογράφησης και αυθεντικοποίησης
  - Δύο οντότητες που θέλουν να επικοινωνήσουν πρέπει να συμφωνήσουν εκ των προτέρων στο είδος της ασφάλειας
- Security Association (SA): συμφωνία μεταξύ δύο άκρων για μεθόδους και αλγορίθμους που επιθυμούν να χρησιμοποιήσουν κατά τη σύνοδο
  - αλγόριθμοι κρυπτογράφησης
  - αλγόριθμοι αυθεντικοποίησης
  - κλειδιά, διάρκεια ισχύος κλειδιών κτλ .
- Τελικό λόγο στη διαπραγμάτευση : ο destination host
- SADB (Security Associations Database)
  - Κάθε IPSec end-point διατηρεί μία βάση δεδομένων που αποθηκεύονται τα ενεργά SAs

IPsec Security Associations

- Μία one-way σύνοδος μεταξύ sender και receiver
  - Για two-way secure exchange, δύο SAs αναγκαίες
- Ορίζεται από τρεις παραμέτρους :
  - Security Parameter Index (SPI):
    - bit string assigned to this SA
    - Used by receiver to select the SA
    - 32 bit value πεδίο σε AH και ESP headers
  - IP Destination Address:
    - the address of the destination endpoint
      - end user system, firewall ή router
  - Security Protocol Identifier:
    - AH ή ESP security association
- Επομένως σε κάθε IP packet η SA στην οποία ανήκει προσδιορίζεται από τις τρεις αυτές παραμέτρους στον header

IPsec Security Associations

Παράμετροι μίας SA

- Δεδομένα που χρησιμοποιήθηκαν για αυθεντικοποίηση (AH ή ESP πρωτόκολλα, διάνυσμα αυθεντικοποίησης (IV), δημόσια κλειδιά, χρονική διάρκεια κλειδιών
- Δεδομένα που χρησιμοποιήθηκαν για εμπιστευτικότητα (ESP πρωτόκολλο κρυπτογράφησης, δημόσια κλειδιά, χρονική διάρκεια κλειδιών).
- Δεδομένα που χρησιμοποιήθηκαν για προστασία από επανεκπομπή (μετρητές υπερχείλισης, IP packet seq. numbers)
- Είδος Μεθόδου
  - end-to-end:Transport Mode ή
  - router-to-router: Tunnel Mode
- Διάρκεια ζωής της SA (σε bytes ή χρόνο)

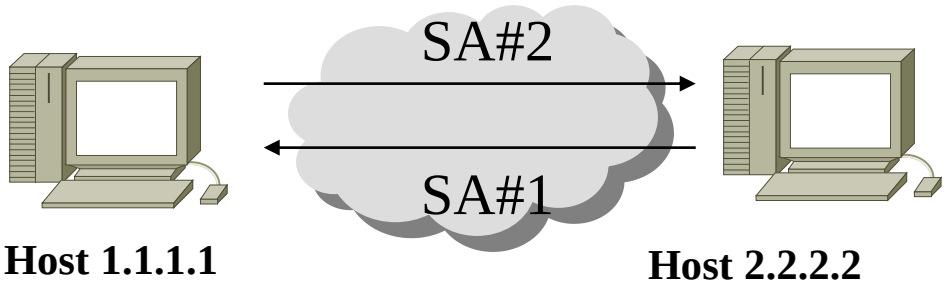
IPsec Security Associations

Πως το IPSec προσδιορίζει τι είδους SA θα εφαρμόσει στα IP packets?

- Κάθε IPSec-aware host διατηρεί μία Security Policy Database (SPDB).
- Για κάθε outbound και inbound packet το IPsec συμβουλεύεται την SPDB
- Τα πεδία στο IP packet συγκρίνονται με τα πεδία στο SPDB entries για να βρεθούν ταιριάσματα (matches).
  - Ταιριάσματα: βασίζονται σε
    - source and dest addresses (ή ranges of addresses),
    - transport layer protocol,
    - transport layer port numbers, ...
- Το ταίριασμα καθορίζει ένα SA ή μια ανάγκη για νέο SA

IPsec Security Associations

Host 1.1.1.1 SADB
INBOUND-SA#1
ESP – DES (enc)
ESP – MD5 (auth)
…
OUTBOUND-SA#2
ESP – 3DES (enc)
ESP – SHA (auth)
…

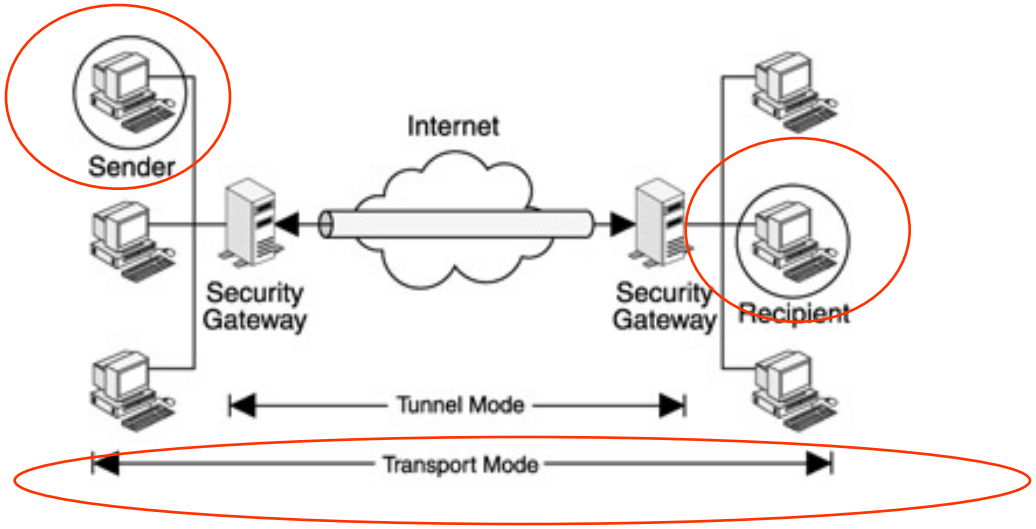


Host 2.2.2.2 SADB
INBOUND-SA#2
ESP – 3DES
ESP – SHA
…
OUTBOUND-SA#1
ESP – DES
ESP – MD5
…

- Όταν λαμβάνεται ένα IP packet, μπορεί να αυθεντικοποιείται και να αποκρυπτογραφείται μόνον εάν ο παραλήπτης μπορεί να το συνδέσει με το περιεχόμενο ενός κατάλληλου SA
- Πολλαπλές SA μπορούν να δημιουργηθούν για την επικοινωνία μεταξύ δύο μερών (π.χ. για διαφορετικές εφαρμογές).

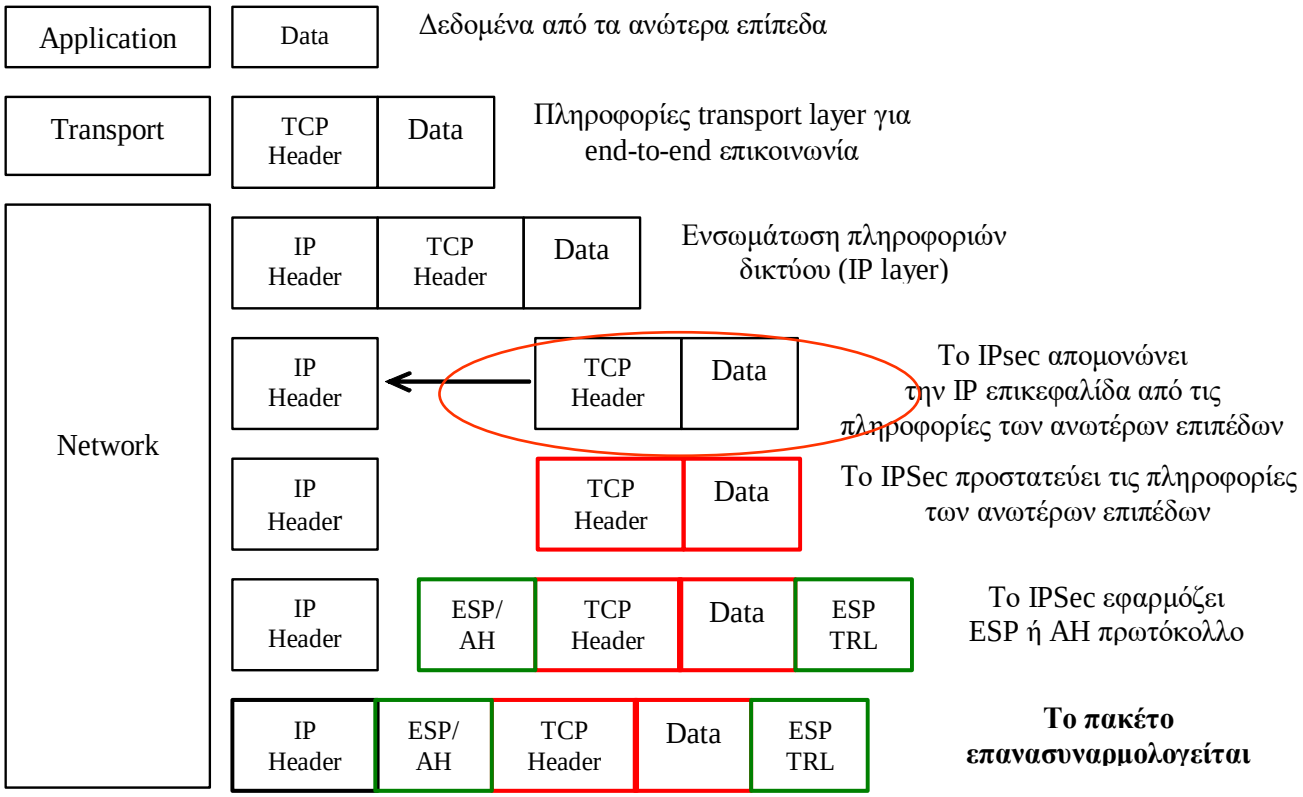
IPSec –Μέθοδοι λειτουργίας

- Transport Mode (Μεταφοράς)
  - η ασφάλεια εφαρμόζεται μεταξύ hosts (end-to-end)
  - μόνο το IP packet payload αυθεντικοποιείται ή κρυπτογραφείται
  - ο αρχικός IP packet header μένει αμετάβλητος και δεν προστατεύεται



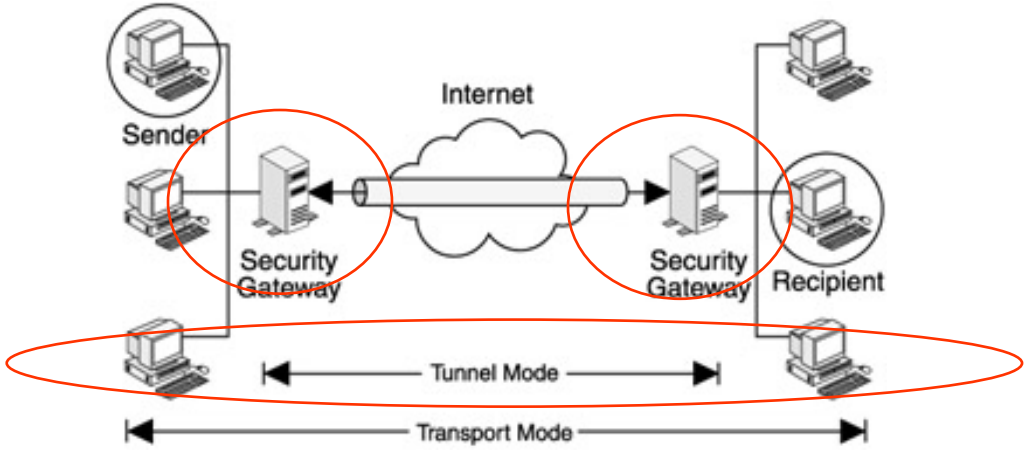
IPSec –Μέθοδοι λειτουργίας

- Transport Mode (Μεταφοράς)



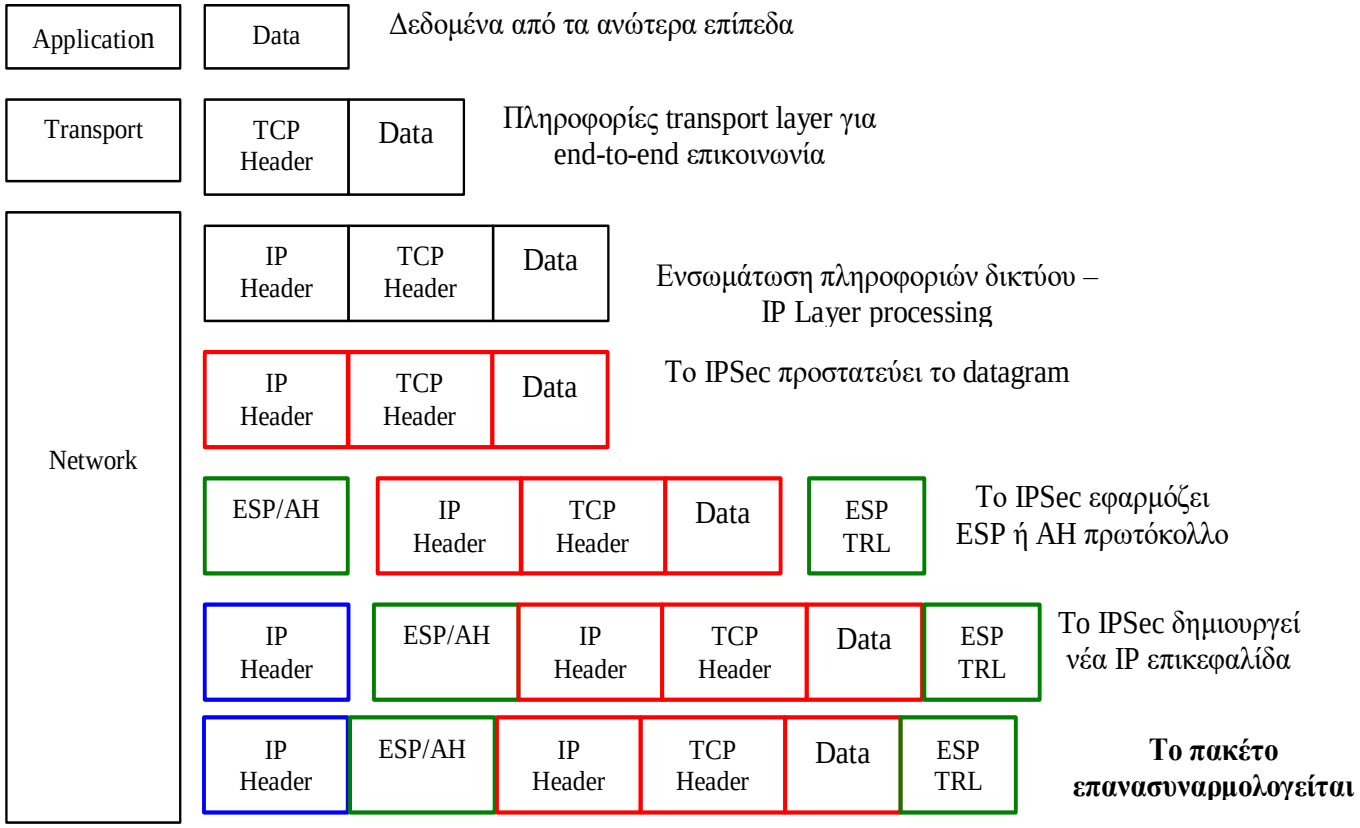
IPSec –Μέθοδοι λειτουργίας

- Tunnel Mode (Διόδου):
  - Όλο IP packet γίνεται payload σε ένα νέο IP packet
  - Ένας νέος IP header προστίθεται (κατά ESP ή AH)
  - Το νέο IP packet οδεύεται (tunneled) από την μια IP gateway στην άλλη.
  - Οι endhosts δεν είναι ανάγκη να υλοποιούν IPsec capabilities.



IPSec –Μέθοδοι λειτουργίας

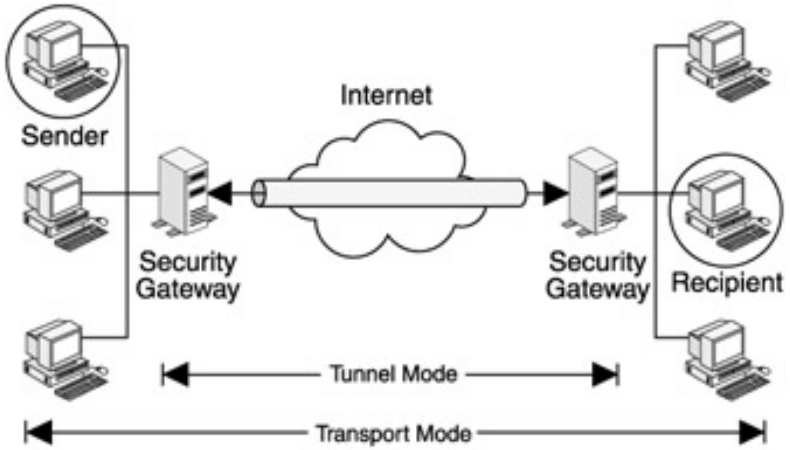
- Tunnel Mode (Διόδου)



IPSec –Μέθοδοι λειτουργίας

Σημαντικό:

Τα AH και ESP
μπορούν να λειτουργήσουν
είτε σε Transport mode
είτε σε Tunnel mode



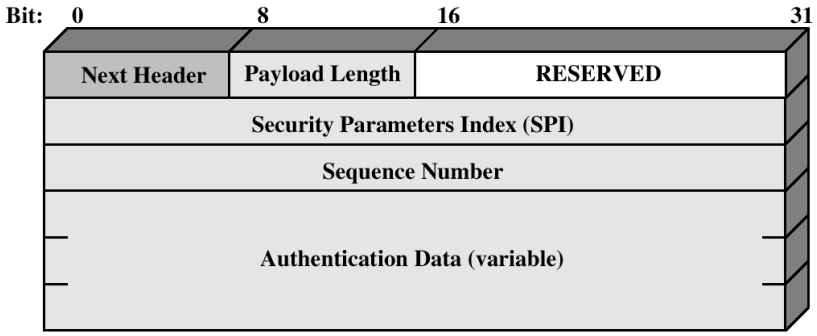
IPSec –Μέθοδοι λειτουργίας και πρωτόκολλα

	Transport Mode SA	**Tunnel Mode SA**
AH	Authenticates IP payload and selected portions of IP header	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload but not the IP header	Encrypts inner IP packet including the IP header
ESP with authentication	Encrypts IP payload and Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

IPsec AH - Authentication Header

- Υποστηρίζει
  - Data integrity του IP packet.
    - Τροποποίηση IP packet κατά την μεταφορά: ανιχνεύσιμο
  - Authentication του IP packet.
    - End-system verify αποστολέα
    - Αποτρέπει address spoofing attacks.
  - Βασίζεται σε Message Authentication Code (MAC)
    - Τυπικά μέσω HMAC και MD5/SHA-1 για σύνοψη
    - Κοινό συμμετρικό κλειδί
  - Επίσης μέριμνα απέναντι σε replay attacks

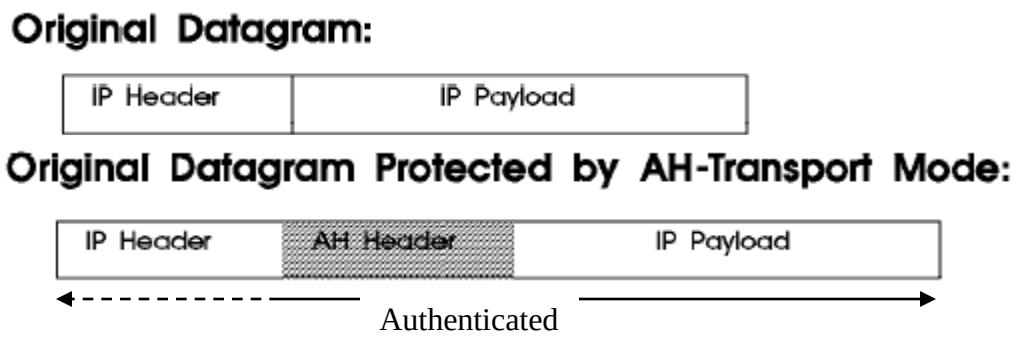
IPsec AH - Header



- Next header (8):
  - Ο τύπος του header που έπεται του AH
  - Η τιμή του επιλέγεται από το σύνολο των IP Protocol Numbers όπως ορίζονται από IANA
    - Π.χ., TCP
- Payload length (8):
  - Μήκος του AH σε 32-bit words
- Reserved (16)
  - για μελλοντική χρήση
- SPI (32):
  - Προσδιορίζει μια SA.
- Sequence number (SeqNr, 32):
  - Αυξάνων μετρητής (anti replay attack)
- Authentication data (variable):
  - Περιέχει integrity check value (ICV) ή MAC για αυτό το πακέτο.

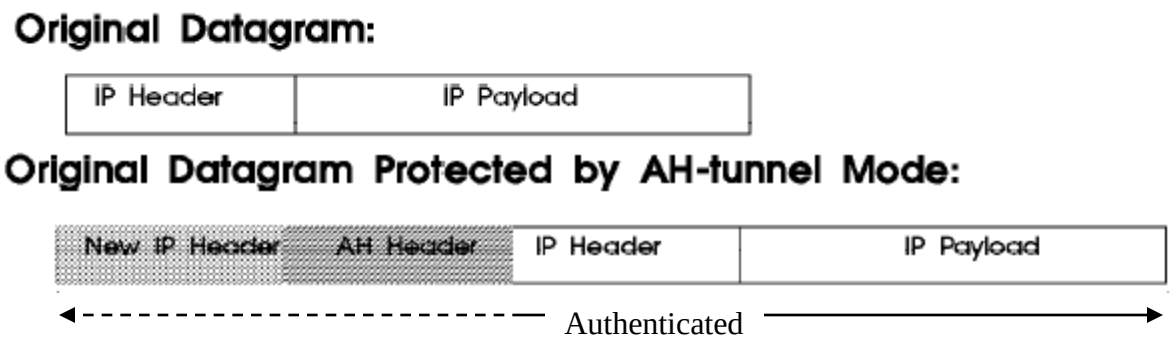
IPsec AH - Transport mode

- Transport mode
  - Η αυθεντικοποίηση παρέχεται απευθείας μεταξύ δύο end systems
    - π.χ., client and server workstations
  - η αρχική header του IP packet είναι η εξωτερική επικεφαλίδα του νέου IP packet, ακολουθούμενη από την AH header και στη συνέχεια ακολουθεί το payload του αρχικού IP packet.
  - Το αρχικό IP packet αυθεντικοποιείται ως προς τον αποστολέα και προστατεύεται ως προς την ακεραιότητά του



IPsec AH - Tunnel mode

- Tunnel mode
  - Όλο το IP packet αυθεντικοποιείται.
  - Ο AH header τοποθετείται μεταξύ original IP header και new, outer, IP header
  - Η outer IP address περιέχει την IP addresses του security gateway (router, firewall)
  - Η Inner IP address περιέχει την διεύθυνση του end system.



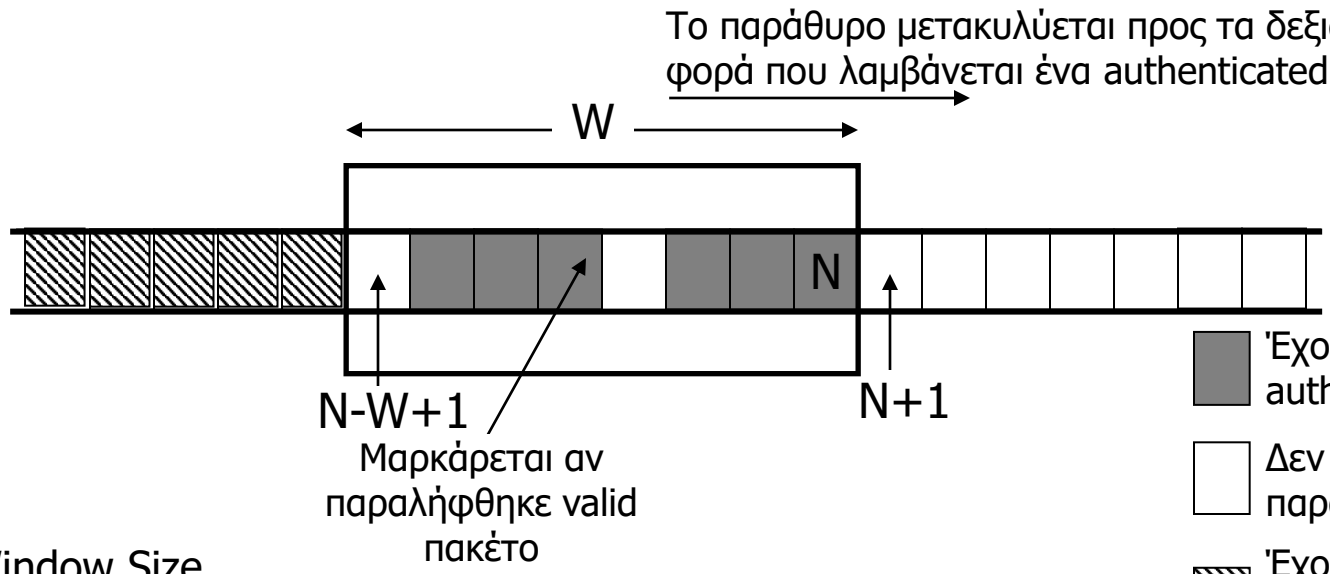
IPsec AH – Anti-Replay Attacks

- Το IPsec AH χρησιμοποιεί sequence number για αποτροπή replay attacks
  - Τίθεται 0 όταν ξεκινά μια νέα SA
- Ωστόσο reordering των IP packets είναι πιθανό να συμβεί στο επίπεδο IP
  - Packet switching / routing
  - Packets με larger sequence number μπορούν να παραληφθούν στον παραλήπτη πριν από packets με smaller sequence numbers
- Όταν out-of-order packets με μικρότερο sequence number ληφθούν αργότερα, απορρίπτονται (discarded)

IPsec AH – Anti-Replay Attacks

- Anti-Replay Window Protocol:
  - Προστατεύει IP packets απέναντι σε replay attacks και επικουρεί στο ζήτημα του reordering
  - Ο αποστολέας εισάγει ένα sequence number (SeqNr) σε κάθε IP packet
    - Αρχικοποίηση με την εγκαθίδρυση SA
    - Μονοτονικά αύξων
  - Ο παραλήπτης χρησιμοποιεί ένα κυλιόμενο παράθυρο (sliding window) για να ιχνηλατεί τα λαμβανόμενα SeqNr από την SA
    - Δανεισμός ιδέας από TCP …

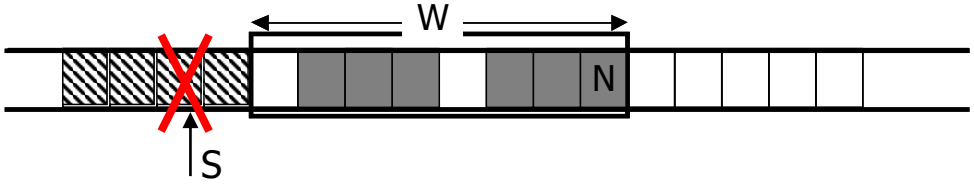
IPsec AH – Anti-Replay Attacks



- **W.** Window Size
- **N.** Right edge of Window
  - The highest SeqNr of valid packet received so far
- **S.** Το SeqNr του επόμενου πακέτου που θα ληφθεί.Υπάρχουν τρεις περιπτώσεις
  - S μικρότερο από όποιο SeqNr μέσα στο W (S < N-W+1)
  - S μέσα στο W (N-W+1 ≤ S ≤ N)
  - S μεγαλύτερο από όποιο SeqNr μέσα στο W (S > N)

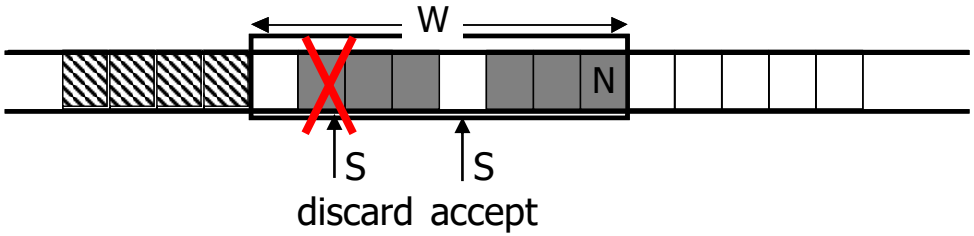
IPsec AH – Anti-Replay Attacks

S < N-W+1 → Replay attack, discard packet

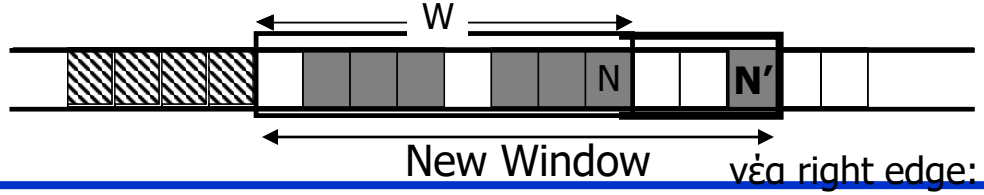


N-W+1 ≤ S ≤ N . Έλεγξε S. Αν S exist στο W → Replay attack, discard packet

Διαφορετικά → accept packet



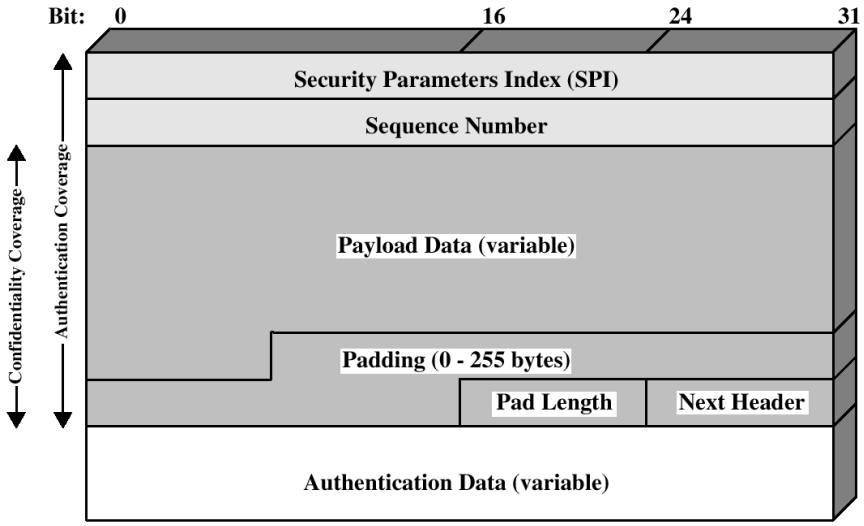
S > N . → Accept packet. Slide the window so that S becomes its new right edge



IPsec ESP – Encapsulating Security Payload

- Υποστηρίζει
  - confidentiality services.
    - confidentiality του IP packet
  - περιορισμένης έκτασης authentication service
    - Authenticates το payload αλλά όχι το IP packet header

IPsec ESP – Header / Trailer



- SPI (32):
  - Προσδιορίζει μια SA.
- Sequence number (32):
  - Αυξάνων μετρητής (replay attack)
- Payload data (Variable):
  - packet data (transport mode) ή
  - IP packet (tunnel mode).
- Padding (0-255):
  - Προσθήκη χαρακτήρων για να προκύψουν αποδεκτά πολλαπλάσια μήκη πακέτου
- Pad length (8)
  - Αριθμός padded χαρακτήρων.
- Next header (8):
  - Ο τύπος του header που έπεται του ESP
- Authentication data (variable):
  - Περιέχει integrity check value (ICV) για αυτό το πακέτο

IPsec ESP – Algorithms

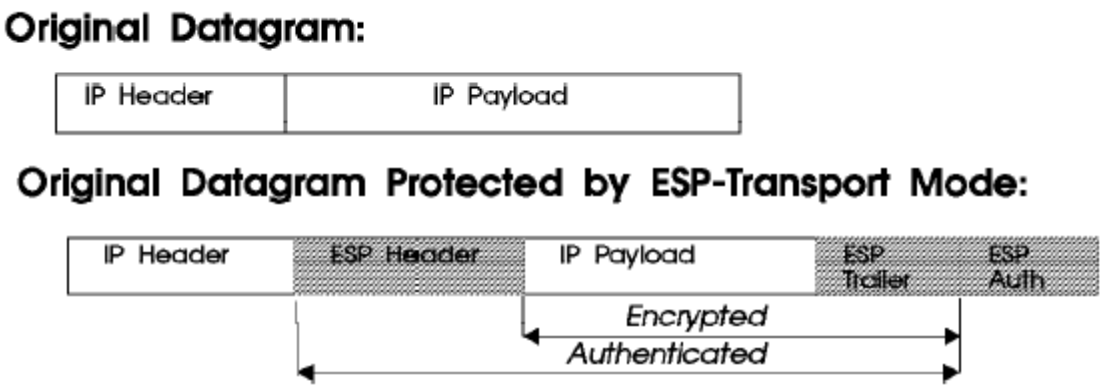
- Encryption
  - Ποια πεδία «καλύπτονται»:
    - Payload data, Padding, Padding length, και Next Header
  - Αλγόριθμοι (DOI document)
    - DES with CBC, mandatory
    - Three-key 3DES, RC5, IDEA, CAST, Blowfish
- Authentication
  - Ποια πεδία «καλύπτονται»:
    - SPI, SeqNr, Payload data, Padding, Padding length, και Next Header
  - Αλγόριθμοι
    - Όπως AH: Το ESP υποστηρίζει HMAC με default length των 96 bits (HMAC-MD5-96 και HMAC-SHA-1-96)

IPsec ESP – Transport mode

- Transport mode
  - Χρησιμοποιείται για encryption και authentication (optional) των δεδομένων (κυρίως payload) IP packet
  - Η κρυπτογράφηση υποστηρίζεται μεταξύ δύο end systems
    - π.χ., client και server workstations
  - Η IP επικεφαλίδα του IP datagram διατηρείται (routing)
    - Δεν προστίθεται νέα
  - Η IP επικεφαλίδα του IP datagram δεν κρυπτογραφείται
    - Πληροφορίες για διευθύνσεις τελικό αποστολέα - παραλήπτη της επικεφαλίδας είναι ορατές για κάποιον passive attacker (traffic analysis)
  - Η IP επικεφαλίδα του IP datagram δεν αυθεντικοποιείται

IPsec ESP – Transport mode

- Transport mode
  - ESP header: εισάγεται μετά το IP header.
  - ESP trailer (Padding, Padding length, Next Header): εισάγεται στο τέλος του IP packet
  - Αν χρησιμοποιείτε authentication, τα authentication data τοποθετούνται μετά τον ESP trailer

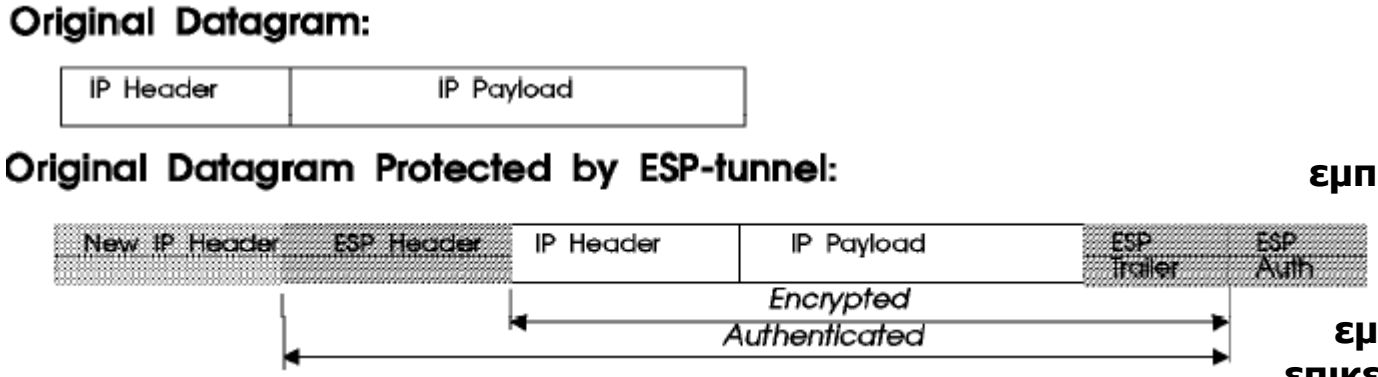


IPsec ESP – Tunnel mode

- Tunnel mode
  - Όλο το αρχικό IP packet is encrypted.
    - Όλο το αρχικό IP packet γίνεται payload ενός νέου IP packet (ονομάζεται inner packet).
      - Νέος IP header προστίθεται.
      - Ο νέος IP header χρησιμοποιείται πλέον για routing.
  - Το νέο IP packet διοδεύεται (tunneled) από μια IP gateway (router/firewall) σε άλλη
  - Όλο το αρχικό IP packet (και ο ESP Trailer) είναι encrypted. Η αρχική IP header δεν μπορεί να διαβαστεί από passive attacker.
    - βασική χρήση ESP σε tunnel mode: απόκρυψη των εσωτερικών διευθύνσεων δικτύου μεταξύ δύο IP gateways
  - Οι Hosts δεν είναι υποχρεωμένοι να υλοποιούν IPsec ESP security capabilities

IPsec ESP – Tunnel mode

- Tunnel mode
  - ESP header: εισάγεται μετά το νέο IP header.
  - ESP trailer (Padding, Padding length, Next Header): εισάγεται στο τέλος του αρχικού (inner πλεόν) packet.
  - Αν χρησιμοποιείτε authentication, τα authentication data τοποθετούνται μετά τον ESP trailer

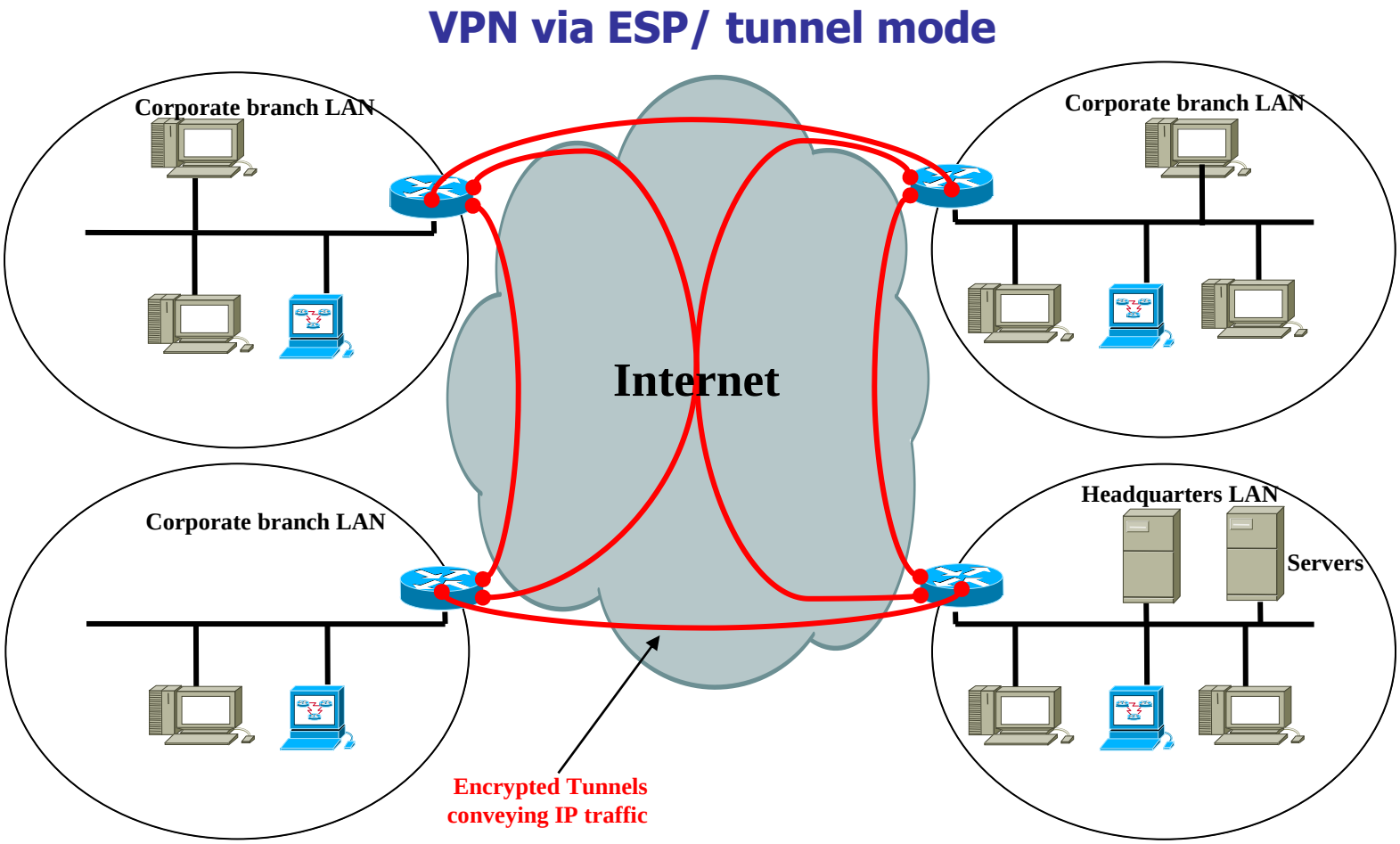


Hint:

Η Transport παρέχει εμπιστευτικότητα στο payload του αρχικού datagram,

Η Tunnel παρέχει εμπιστευτικότητα και για την επικεφαλίδα και για το payload.

IPsec ESP – Tunnel mode



IPsec ESP vs AH

- Η AH παρέχει αυθεντικοποίηση αποστολέα και ακεραιότητα των δεδομένων.
- Η ESP παρέχει υπηρεσίες εμπιστευτικότητας (authntication is optional). Η κρυπτογράφηση μπορεί να γίνει:
  - είτε σε transport mode για τα upper-layer protocol data (TCP data)
  - είτε σε tunnel mode για τα ίδια τα IP πακέτα, δημιουργώντας νέα κρυπτογραφημένα IP πακέτα
    - επιτυγχάνεται και προστασία κατά της ανάλυσης δεδομένων
- Πρέπει να λάβουμε υπόψη τους αυξημένους επεξεργαστικούς φόρτους που απαιτούνται κατά την υλοποίηση IPSec
  - Από άκρο-σε-άκρο (transport)
  - Από gateway-σε- gateway (tunnel)

IPSec – Key Management

IPSec – Key Management

- IPSec απαιτεί τον προσδιορισμό και τη διανομή secret keys
  - Encryption στο ESP
  - HMAC στο AH και ESP
- Δύο τύποι διαχείρισης κλειδιών
  - Manual
  - Automated

IPSec – Key Management

- Manual
  - Ο System administrator χειροκίνητα εγκαθιστά σε όλα τα συστήματα τα κλειδιά
    - Πρακτικό για μικρής κλίμακας IP δίκτυα
- Automated
  - Κατά απαίτηση δημιουργία κλειδιών και διανομή κλειδιών για SAs
    - Ιδανικά για large scale distributed networking
  - Default:
    - OAKLEY Key Determination Protocol
    - Internet Security Association and Key Management Protocol (ISAKMP)

OAKLEY / ISAKMP

- OAKLEY
  - key exchange protocol
  - Βασισμένο σε Diffie-Hellman (DH)
    - Παρέχει πρόσθετη ασφάλεια σε σχέση με το pure DH
  - Είναι γενικό, δεν απαιτεί ειδικά formats
- ISAKMP
  - Παρέχει ένα πρωτόκολλο για διαχείριση κλειδιών και διαπραγμάτευση παραμέτρων / αλγορίθμων
    - Establish, modify, delete SAs.
    - Ορίζει procedures και packet formats

OAKLEY

- Βασίζεται σε DH
- Ελκυστικές ιδιότητες DH:
  - Secret keys παράγονται όταν χρειάζονται
    - π.χ., για μία σύνοδο
    - Δεν απαιτείται μακράς διάρκειας αποθήκευση που δημιουργεί ευπάθεια
  - Η συμφωνία για κοινό κλειδί δεν απαιτεί προϋπάρχουσα εμπιστοσύνη, αλλά γνώση και συμφωνία κοινών παραμέτρων

OAKLEY

- Αδυναμίες DH:
  - Δεν παρέχει πληροφορίες για τις ταυτότητες των οντοτήτων
    - Αναποτελεσματικός σε ενεργητικές επιθέσεις (man in the middle attacks)
  - Υπολογιστικά «ακριβός» και επικίνδυνος
    - Κακόβουλος αιτείται μεγάλο αριθμό κλειδιών από οντότητα (θύμα)
    - Το θύμα εκτελεί συνεχώς εκθετικές πράξεις
    - Αποτέλεσμα: το θύμα εξαντλεί τα resources του
    - Επίθεση τύπου DoS
      - Αναφέρεται ως Sleep Deprivation torture ή clogging attack

OAKLEY

- Αδυναμίες DH και αντιμετώπιση από OAKLEY:
  - χρήση cookies για αποφυγή clogging attacks
  - Χρήση δημόσιας κρυπτογραφίας για να αυθεντικοποιεί τις οντότητες κατά το DH key exchange.
    - Αποφυγή man-in-the-middle attack
- Επιπρόσθετα
  - Επιτρέπει σε δύο οντότητες
    - Να διαπραγματευτούν τις global parameters του DH key exchange
    - Να ανταλλάξουν τα δημόσια κλειδιά τους κατά το DH key exchange

OAKLEY Cookie exchange

- Χαλαρός (weak) source-address identification και για τις δύο νόμιμες (γνήσιες) οντότητες
- Το cookie exchange πραγματοποιείται πριν την εκτέλεση υπολογιστικά ακριβών πράξεων
  - Π.χ. large integer exponentiations
- Πρέπει να είναι δύσκολο να παραχθεί από άλλη οντότητα (forger) ένα cookie που αφορά τη γνήσια οντότητα
- Το cookie exchange πρέπει να είναι γρήγορο
  - Να μην επιτρέπει επιθέσεις DoS
- Συνήθως είναι το output μιας one-way hash function (MD5) σε μία local/remote IP address, και local/remote UDP port και nonce

OAKLEY Cookie exchange

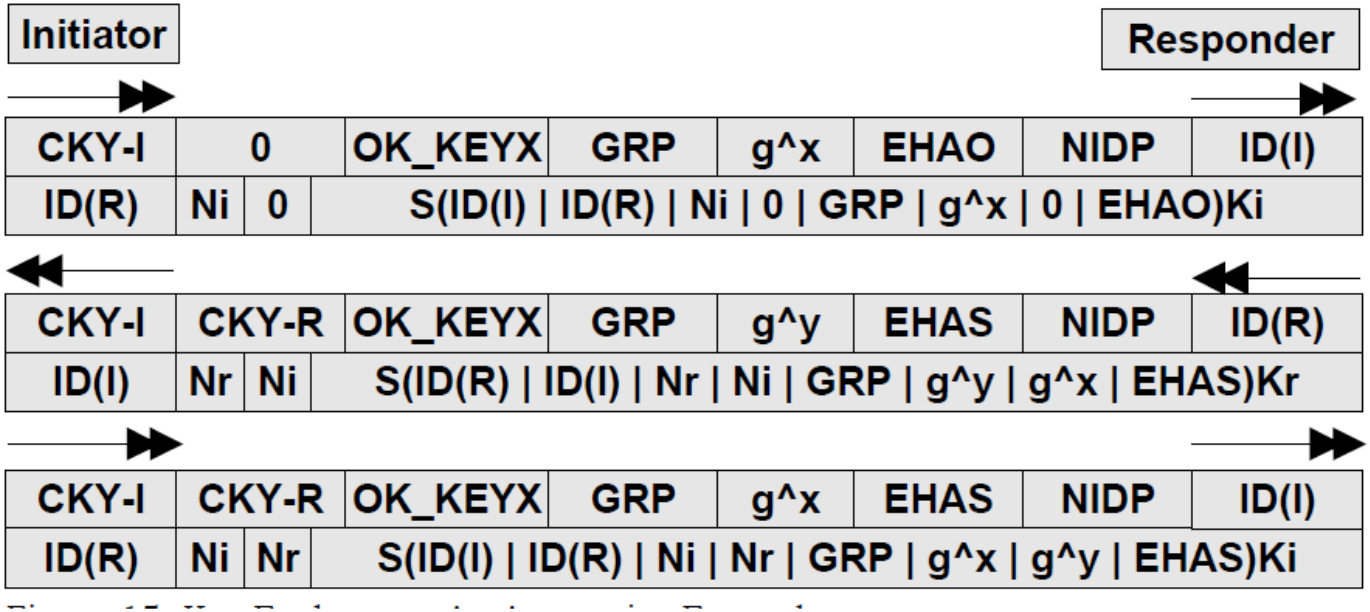
- Πως γίνεται clogging:
  - Ένας επιτιθέμενος αντιγράφει την source address μίας από τις νόμιμες οντότητες που θέλουν να ανταλλάξουν κλειδιά
  - Στέλνει ένα δημόσιο DH κλειδί στο θύμα, το οποίο προσπαθεί να υπολογίσει το συμμετρικό κλειδί και εξαντλείται ....
- Anti-clogging
  - Ο αιτών στέλνει ως πρώτο μήνυμα στην άλλη πλευρά ένα cookie (με ένα random number ως nonce)
  - Η άλλη νόμιμη πλευρά επιβεβαιώνει άμεσα τη λήψη και στέλνει το δικό της cookie (με το ίδιο nonce έλαβε) αντί να εκτελεί εκθετικές πράξεις
  - Ο επιτιθέμενος δε θα λάβει τίποτα αν έχει χρησιμοποιήσει πλαστή IP addr

OAKLEY Authentication

Key exchange αυθεντικοποιείται με

- Digital signatures
  - υπογραφή μιας hash (encrypting με χρήση private key του sender)
  - Η Hash δημιουργείται με χρήση IDs και nonces
- Public-key encryption
  - encrypting με το ιδιωτικό κλειδί του sender
- Symmetric-key encryption
  - Το Secret key μπορεί να προκύψει μέσω out-of-band μηχανισμών

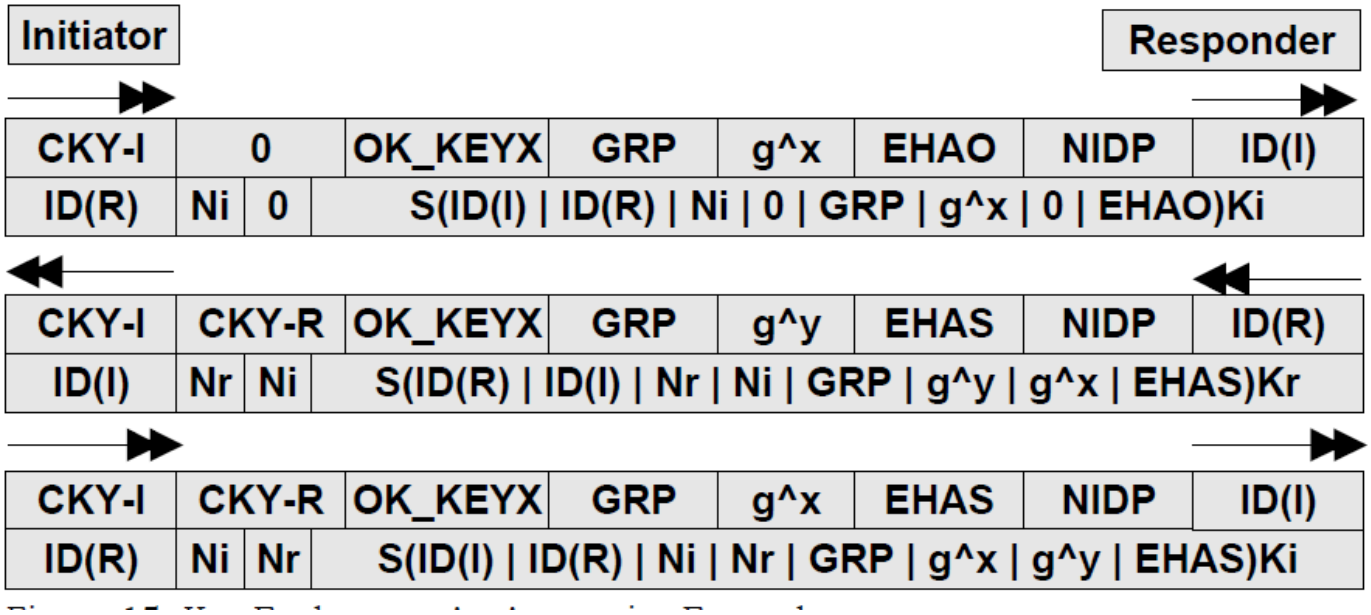
OAKLEY



Initiator I στέλνει αρχικό μήνυμα σε Responder R
Responder R επιβεβαιώνει υπογραφή μηνύματος με χρήση I's public key
Initiator I επιβεβαιώνει υπογραφή μηνύματος με χρήση R's public key

KEYID = CKY-I|CKY-R
Value of key **sKEYID=prf(Ni|Nr, CKY-I|CKY-R)**
pseudo-random function με δείκτη Ni|Nr στη παράμετρο CKYI|CKY-R.

OAKLEY



CKY-I, CKY-R	Initiator και Responder Cookie
OK_KEYX	message type
GRP	η ομάδα του DH key exhange (g,n)
g^x, g^y	τα δημόσια στοιχεία των I και R. x και y είναι private random numbers που παράγονται από I και R κατά DH
IDP, NIDP	bit, δηλώνει αν πεδία που ακολουθούν είναι encrypted (IDP) ή όχι (NIDP)
EHAQ	Λίστα από encryption, hash και authentication που προτείνονται από I.
EHAS	Η λίστα που γίνεται αποδεκτή
ID(I), ID(R)	Ταυτότητες I και R
E(x)Ki	encryption του x με το the public key του μέλους i
S(x)Ki	signature του x με το private key του μέλους i

Secure Socket Layer – SSL
Transport Layer Security - TLS

SSL

- Αναπτύχθηκε από την Netscape (1995)
- Παρέχει ασφαλή επικοινωνία μεταξύ browsers και servers
  - Από άκρο σε άκρο
- Χρησιμοποιεί το TCP ως reliable underlying transport protocol
- Είναι υλοποιημένο στο socket level
  - Ανεξάρτητο από τις εφαρμογές στο ανώτερο επίπεδο
    - Παρέχει ασφάλεια σε διαφορετικές εφαρμογές
    - SMTP, TELNET, FTP, HTTP, SIP
- Open-source implementation www.openssl.org
  - Αλλά και βιβλιοθήκες (cryptlib, GnuTLS)

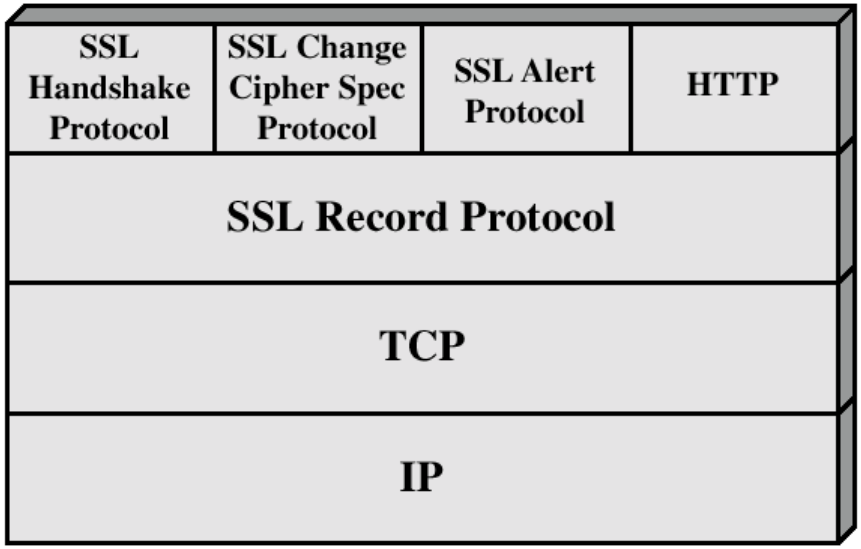
SSL

Αποτελείται από επιμέρους πρωτόκολλα:

- Handshake Protocol
  - Αυθεντικοποίηση, διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφαλείας στα δύο άκρα της σύνδεσης
- Record Protocol
  - Εμπιστευτικότητα και ακεραιότητα μηνυμάτων
- Cipher Change Protocol
  - Παράμετροι κρυπτογραφίας
- Alert Protocol
  - Μηνύματα ελέγχου

SSL/TLS protocol stack

Το SSL αναπτύσσεται σε δύο layers



- SSL Record πρωτόκολλο
  - παρέχει υπηρεσίες εμπιστευτικότητας και ακεραιότητας δεδομένων, προστασία από replay attacks πάνω από μια προσανατολισμένη στη σύνδεση, αξιόπιστη υπηρεσία μεταφοράς (TCP)
- Οι υπηρεσίες αυτές παρέχονται σε όλα τα πρωτόκολλα του ανώτερου επιπέδου
  - SSL Handshake
  - SSL Change Cipher
  - SSL Alert

Network security essentials (International edition), William Stallings, Prentice-Hall, 2002

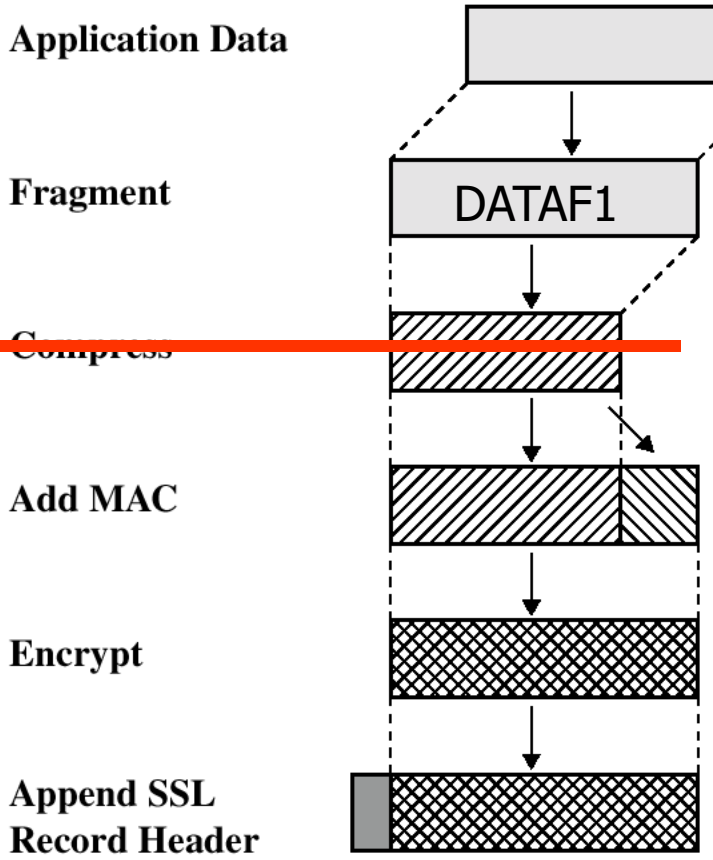
SSL σύνοδοι και συνδέσεις

- SSL Σύνοδος (Session)
  - Μπορούμε να φανταστούμε μια SSL session ως μια security association.
  - Το SSL session ορίζεται από
    - Session ID
    - X.509 public-key certificate of peer (could be null for client**, mandatory for server KU_S**)
    - Cipher spec:
      - Encryption algorithm, HMAC message digest algorithm, etc.
    - **Master secret: 48 byte secret shared between the client and server**

SSL Record protocol

- Παρέχει δύο υπηρεσίες :
  - **Confidentiality:**
    - Shared secret key χρησιμοποιείται για συμμετρική κρυπτογραφία του SSL payload
  - **Message Integrity:**
    - Shared secret key χρησιμοποιείται για παραγωγή MAC
  - Λαμβάνει application message και εκτελεί:
    - Fragmentation
    - Compression
    - Add a MAC (a shared secret key is used)
    - Encryption (symmetric encryption)
    - Appends an SSL record header
    - Send the message to TCP

SSL Record protocol

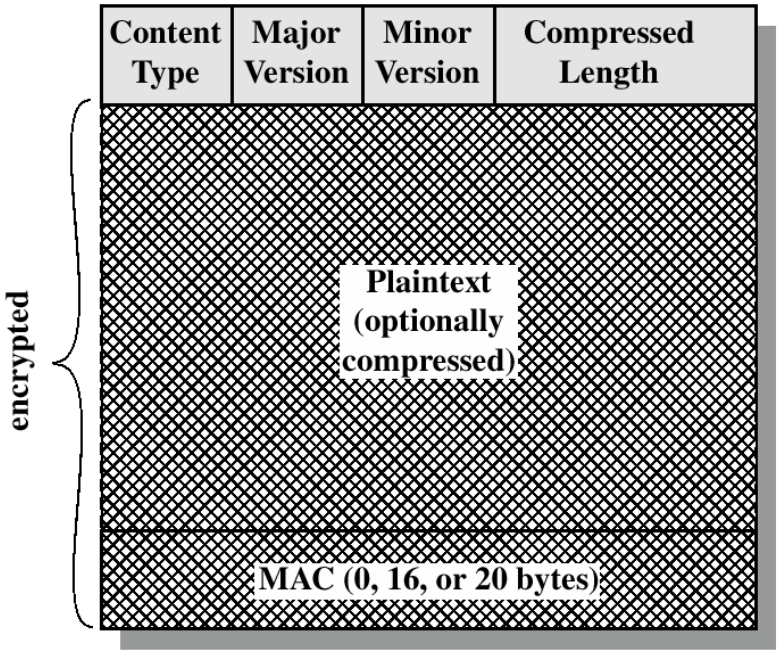


- HMAC (a shared secret key is used)
  - MAC algorithm: similar to HMAC.
  - Based SHA-1 or later hash algorithms
- Encryption (symmetric encryption)
  - Block: IDEA, RC2-40, 3DES, AES…
  - Stream: RC4-40 and RC4-128
- Για block encryption padding προστίθεται μετά το MAC

E_{MK} [HMAC(C(DATAF1),MK) || C(DATAF1)] || HEADER

Network security essentials (International edition), William Stallings, Prentice-Hall, 2002

SSL Record Protocol – format

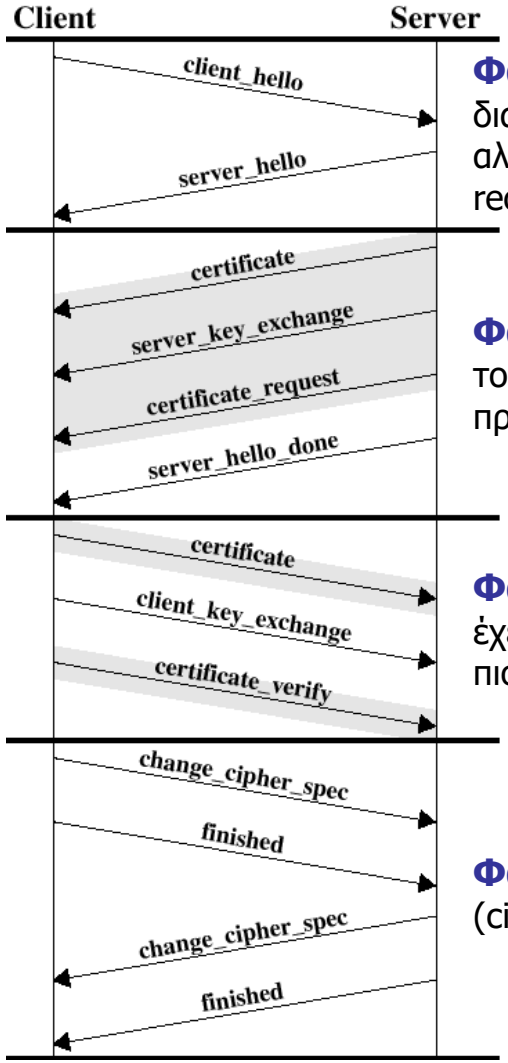


- Content Type (8): To higher layers protocol που θα χρησιμοποιήσει το enclosed fragment.
  - ChangeCipherSpec
  - Alert
  - Handsake
  - Application data
- Major Version (8): Δηλώνει το major version του SSL που χρησιμοποιείται
- Minor Version (8): Δηλώνει το minor version του SSL που χρησιμοποιείται
- Compressed length (16): το μήκος του compressed fragment σε bytes (max size 2^{14} bytes).

SSL Handshake protocol

- Το πιο σύνθετο τμήμα του SSL
- Επιτρέπει σε Server και client να
  - Αυθεντικοποιηθούν μεταξύ τους
    - **Server to Client mandatory**
    - Client to Server optional
  - Διαπραγματευτούν encryption, hash algorithms και cryptographic keys
- Χρήση πριν από όποια μετάδοση application data
- Εγκαθιδρύει σύνοδο

SSL Handshake protocol – Φάση 1



Φάση 1. Διαπραγμάτευση δυνατοτήτων. Εγκαθιδρύει σύνοδο, διαπραγματεύεται ικανότητες μεταξύ των ομότιμων, οριοθετεί παραμέτρους και αλγορίθμους κρυπτογράφησης (cipher stack), μεθόδους compression (για το SSL record protocol), και συμφωνούνται αρχικά random numbers

Φάση 2. Αυθεντικοποίηση Server. Ο Server μπορεί να δώσει το πιστοποιητικό του στον Client ή να ζητήσει το πιστοποιητικό του Client. Σηματοδοτεί τη λήξη της πρώτης φάσης της χειραψίας .

Φάση 3. Αυθεντικοποίηση Client. Ο Client παρέχει το πιστοποιητικό του (αν έχει ζητηθεί), στέλνει την ανταλλαγή κλειδιών, και μπορεί να επαληθεύσει το πιστοποιητικό του Server

Φάση 4. Τερματισμός Διαπραγμάτευσης. Ο Server και ο Client τροποποιούν το (cipher stack). Σηματοδοτεί τη λήξη της χειραψίας.

Network security essentials (International edition), William Stallings, Prentice-Hall, 2002

SSL Handshake protocol – Φάση 1

Client Hello message

- Version: Η μεγαλύτερη έκδοση του πρωτοκόλλου που ο Client μπορεί να υποστηρίξει.
- Random: Ένας 32-bit τυχαίος αριθμός.
  - Secure random number generator
  - Λειτουργούν ως nonces για να αποτρέψουν replay attacks κατά τη διαπραγμάτευση κλειδιών
- Session ID: Αναγνωρίζει μοναδικά την SSL σύνοδο.
  - **Value 0** : client wants to establish a new connection on a new session,
  - **Value :Non zero**:client wants to update parameters of an existing connection or create a new connection on this session.
- Cipher Suites : Μια λίστα με τις κρυπτογραφικές μεθόδους που ο client προτιμά
  - key exchange ,encryption, hashing
- Compression Methods: μεθόδους συμπίεσης που ο client μπορεί να υποστηρίξει.

SSL Handshake protocol – Φάση 1

Cipher Suite παράμετρος:

- Υπόλοιπα τμήματα της παραμέτρου
  - Cipher algorithm
  - MAC algorithm: SHA-1/2
  - Cipher Type: Block or Stream
  - Hash Size: 0,16,[MD5] or 20 [SHA-1] bytes
  - IV size : which is used for CBC mode encryption.

SSL Handshake protocol – Φάση 1

Παράδειγμα.

Ο Client στέλνει στον Server plaintext message για να προτείνει παραμέτρους συνόδου

- Version:
  - SSL 3.1 if you can, else SSL 3.0
- Key Exchange:
  - RSA if you can, else Diffie-Hellman
- Secret Key Cipher Method:
  - TripleDES if you can, else DES
- Message Digest:
  - MD5 if you can, else SHA-1
- Random Number:
  - 777,666,555

SSL Handshake protocol – Φάση 1

Παράδειγμα.

Ο Server απαντά στον Client με plaintext message για να δηλώσει τις παραμέτρους συνόδου με βάση τις προτάσεις του Client και τις δυνατότητές του

- Version:
  - SSL 3.1
- Key Exchange:
  - Diffie-Hellman
- Secret Key Cipher Method:
  - TripleDES
- Message Digest:
  - SHA-1
- Random Number:
  - 444,333,222

SSL Handshake protocol – Φάση 1

Server Hello message

- Version: Η μικρότερη έκδοση του πρωτοκόλλου που ο Client έχει προτείνει που είναι η μεγαλύτερη για τον Server
- Random: Ένας 32-bit τυχαίος αριθμός.
  - Ανεξάρτητος από αυτόν που είχε διαλέξει ο Client
- Session ID:
  - αν η πρόταση του Client ήταν **non zero** τότε η τιμή χρησιμοποιείται από τον Server,
  - Διαφορετικά ο Server παράγει νέα session ID.
- Cipher Suites : Μια λίστα με τις κρυπτογραφικές μεθόδους που ο Client έχει προτείνει και ο Server συμφωνεί
- Compression Methods: Η μέθοδος συμπίεσης που έχει προτείνει Client και ο Server συμφωνεί

SSL Handshake protocol – Φάση 1

Cipher Suite παράμετρος:

- 1ο τμήμα της παραμέτρου: Shared key exchange method
- Shared Key: χρήση σε conventional encryption και MAC
  - RSA παράγει σταθερό *(fixed on session)* shared key
    - Το συμμετρικό κλειδί κρυπτογραφείτε με το public key του Server.
    - Το public-key certificate είναι απαραίτητο
  - Fixed Diffie–Hellman παράγει σταθερό *(fixed on session)* shared key
    - DH key exchange. Το Server Certificate (από CA) περιέχει το DH pubic key του Server και τις μεταβλητές : πρώτος αριθμός p και γεννήτορα g)
    - Ο Client παρέχει το DH pubic key του είτε σε certificate (αν απαιτείται Client Authentication) ή στο key exchange message
  - Ephemeral Diffie–Hellman παράγει εφήμερα, *one-time shared keys*
    - Dynamic DH public keys
    - Η πιο ασφαλής μέθοδος
    - λόγω one-time shared keys

SSL Handshake protocol – Φάση 1

Cipher Suite παράμετρος:

- 1ο τμήμα της παραμέτρου: Shared key exchange method
- Shared Key: χρήση σε conventional encryption και MAC
  - RSA παράγει σταθερό *(fixed on session)* shared key
    - Το συμμετρικό κλειδί κρυπτογραφείτε με το public key του Server.
    - Το public-key certificate είναι απαραίτητο

$$E_{PU_S}(K_{cs})$$

SSL Handshake protocol – Φάση 1

Cipher Suite παράμετρος:

- 1ο τμήμα της παραμέτρου: Shared key exchange method
- Shared Key: χρήση σε conventional encryption και MAC
  - Fixed Diffie–Hellman παράγει σταθερό *(fixed on session)* shared key
    - DH key exchange. Το Server Certificate (από CA) περιέχει το DH pubic key του Server και τις μεταβλητές : πρώτος αριθμός p και γεννήτορα g)
    - Ο Client παρέχει το DH pubic key του είτε σε certificate (αν απαιτείται Client Authentication) ή στο key exchange message

$S_{PR_{CA}}(PU_s, ID_s, g, p, Y_s)$ όπου $[Y_s = g^{Xs} \bmod p]$

$Y_c = g^{Xc} \bmod p$
$E_{PU_S}(Y_c)$ → κρυπτογραφεί προς S
$K_{cs} = (Y_c)^{Xs} = (Y_s)^{Xc}$

$Y_{c2} = g^{Xc2} \bmod p$
$E_{PU_S}(Y_{c2})$ → κρυπτογραφεί προς S
$K_{cs2} = (Y_{c2})^{Xs} = (Y_s)^{Xc2}$

SSL Handshake protocol – Φάση 1

Cipher Suite παράμετρος:

- 1ο τμήμα της παραμέτρου: Shared key exchange method
- Shared Key: χρήση σε conventional encryption και MAC
  - Ephemeral Diffie–Hellman παράγει εφήμερα, *one-time shared keys*
    - Dynamic DH public keys
    - Η πιο ασφαλής μέθοδος
    - Λόγω one-time shared keys
    - Perfect Forward Secrecy

Ephemeral Diffie–Hellman παράγει εφήμερα, *one-time shared keys*

$S_{PR_{CA}}(PU_s, ID_s)$ $[Y_{sc1}=g^{Xsc1} \text{mod} p]$ διαδικασία Server

$S_{PR_S}(Y_{sc1}, ID_s)$ → προς client

$Y_{c1} = g^{Xc1} \text{mod} p$

$E_{PU_S}(Y_{c1})$ → κρυπτογραφεί προς S

$K_{cs1} = (Y_{c1})^{Xsc1} = (Y_s)^{Xc1}$

SSL Handshake protocol – Φάση 2

Server Authentication

- Ο server στέλνει **certificate message**
  - Υπογεγραμμένο από trusted CA
  - Πιστοποιεί το δημόσιο κλειδί του Server
  - Ο Client χρησιμοποιεί το trusted CA's public key για decrypt του certificate και ανάκτηση server's public key
- Έπειτα αποστέλλεται το **server key exchange message**.
  - Δεν στέλνεται όταν η μέθοδος key exchange που έχει συμφωνηθεί είναι RSA ή Fixed DH με πιστοποίηση
  - Στο Ephemeral DH στέλνονται οι δύο καθολικά γνωστές μεταβλητές
    - πρώτος αριθμός και πρωτογενής ρίζα=γεννήτορας
    - και το public DH key του Server

SSL Handshake protocol – Φάση 2

Server Authentication

- Το **certificate request message** περιέχει δύο παραμέτρους
  - Certificate_Type: Public Key Algorithm και η χρήση του
    - RSA signature / DSS signature etc.
  - Certificate Authority name
- Το **Server_Done Message**:
  - Πάντα απαιτείται
  - Χωρίς παραμέτρους
  - Δηλώνει τέλος φάσης 2.

SSL Handshake protocol – Φάση 3

Client Authentication

- Αν ο Server αιτήθηκε certificate από Client, ο Client αποστέλλει **certificate message**.
  - Αν δεν υπάρχουν έγκυρα certificate στέλνετε *no_certificate* alert.
- **Client key exchange message**: το περιεχόμενο εξαρτάται από το **type of key exchange**
  - Στην RSA μέθοδο: Ο Client παράγει ένα 48 byte pre-master secret, και το κρυπτογραφεί με το public key από το Server certificate πριν το στείλει
    - θα χρησιμοποιηθεί για παραγωγή Master Secret
  - Στην Ephemeral DH μέθοδο στέλνεται το public key του Client
  - Στην Fixed DH μέθοδο οι παράμετροι έχουν ήδη σταλεί στο **certificate message**

SSL Handshake protocol – Φάση 3

Client Authentication

- Ο Client στέλνει **certificate verify message** για explicit verification του client certificate
  - Στέλνοντας ο client το δικό του certificate δε σημαίνει αυτομάτως ότι έχει αυθεντικοποιηθεί.
  - Πρέπει επίσης να αποδείξει ότι κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιέχεται στο πιστοποιητικό που έστειλε στο Server.
  - Το μήνυμα περιέχει ψηφιακά υπογεγραμμένη σύνοψη (hash) των πληροφοριών που είναι διαθέσιμες και στα δύο μέρη (key info + messages contents).

SSL Handshake protocol – Φάση 4

Τερματισμός Διαπραγμάτευσης

- Όταν μια session εγκαθιδρύεται ορίζεται μια τρέχουσα κατάσταση λειτουργίας τόσο για αποστολή fragments (receive) όσο και για λήψη fragments (send).
  - Κατά το handshake protocol δημιουργούνται pending καταστάσεις receive και send
  - Στη φάση αυτή οι pending states ορίζονται να είναι current states με χρήση των **change_cipher_specs** μηνυμάτων
- Τα μηνύματα **finished** ολοκληρώνουν τον κύκλο της διαπραγμάτευσης
  - MAC στα messages που έχουν αποσταλεί so far (both sides).
  - MAC υπολογίζεται με το master_secret.

SSL Master Key Creation

- Έχει ήδη πραγματοποιηθεί ανταλλαγή του pre-master key και των random (nonces) στα hello messages
- Το master secret key υπολογίζεται και από τα δύο parties

master_secret := MD5(pre_master_secret||SHA("A" pre_master_secret||
ClientHello.random||ServerHello.random))||
MD5(pre_master_secret||SHA("BB" pre_master_secret||
ClientHello.random||ServerHello.random))||
MD5(pre_master_secret||SHA("CCC" pre_master_secret||
ClientHello.random||ServerHello.random))

SSL auxiliary protocols

- Alert protocol.
  - Διαχείριση SSL συνόδου,
  - error messages (fatal, warnings)
    - Fatal errors τερματίζουν τη σύνδεση
    - Παραδείγματα
      - Decompression failure, certificate_revoked, certificate_unknown, …
- Change cipher spec protocol.
  - Το απλούστερο της οικογένειας
  - Αποτελείται από ένα απλό message που ορίζεται από ένα byte Χρησιμοποιείται για να ενημερώσει ολοκλήρωση αλλαγής cipher suite.
    - Από pending state σε current state
- Και τα δύο πρωτόκολλα χρησιμοποιούν το Record Protocol

SSL application port

- https 443
- smtps 465
- ldaps 636
- pop3s 995
- ftps 990
- imaps 991

SSL and TLS

- Ορίζεται στο
  - RFC 2246 (1.0),
  - RFC 4346 (1.1),
  - RFC 5246 (1.2)
  - RFC 8446 (1.3) 2018
- Πολλές ομοιότητες με SSLv3.
- Διαφορές:
  - message authentication code: χρήση μόνο HMAC
  - Προσθήκη νέων alerts
  - Ο υπολογισμός master secret στο TLS είναι διαφορετικός
  - Αποτροπή downgrade κατά το negotiation
  - TLS1.1: Χρήση αλγόριθμου CBC
  - TLS1.2: Χρήση αλγόριθμου SHA-256

SSL and TLS 1.3

- Στην τυπική έκδοση: το Ephemeral Diffie–Hellman είναι το default key exchange mechanism
- Υποστηρίζει forward secrecy
- Forward secrecy:
  - χαρακτηριστικό πρωτοκόλλων συμφωνίας κλειδιού
  - παρέχει διαβεβαιώσεις ότι τα κλειδιά περιόδου σύνδεσης δεν θα παραβιαστούν ακόμη και αν το ιδιωτικό κλειδί του server παραβιαστεί
  - προστατεύει προηγούμενα sessions από μελλοντικά compromises μυστικών κλειδιών ή κωδικών πρόσβασης.
  - Δημιουργώντας ένα μοναδικό κλειδί συνεδρίας για κάθε σύνοδο

Forward secrecy is designed to prevent the compromise of a long-term secret key from affecting the confidentiality of past conversations.

SSL/TLS Συμπεράσματα

- Το SSL/TLS μπορεί να χρησιμοποιηθεί για την εγκαθίδρυση ασφαλών, αξιόπιστων από άκρο σε άκρο συνδέσεων μεταξύ clients και servers.
  - Αυθεντικοποιεί τον εξυπηρέτη και προαιρετικά τον εξυπηρετούμενο.
  - Υποστηρίζει ανταλλαγή κλειδιών και παρέχει αυθεντικοποίηση μηνυμάτων.
  - Παρέχει υπηρεσίες εμπιστευτικότητας και ακεραιότητας δεδομένων για TCP/IP εφαρμογές.
- Δεν παρέχει υπηρεσίες
  - μη αποποίησης.
  - προστασίας από επιθέσεις ανάλυσης κυκλοφορίας (traffic analysis attacks).

CVE-2014-0160
the SSL Heartbleed bug

SSL Renegotiation Attack

CVE-2014-0160
the SSL Heartbleed bug

- Ευπαθείς εκδόσεις του OpenSSL δεν επιβεβαιώνουν SSL μηνύματα για το μέγεθος της μνήμης
- Bug στο OpenSSL version 1.0.1: Μάρτιος 2012
  - Non affected versions: .99 και 1.0.0
  - Affected versions: 1.0.1 έως 1.0.1f
- Patched στην 1.0.1g
  - έχει προσθέσει ελέγχους ορίων για να αποτρέψει υπερχείλιση της προσωρινής περιοχής μνήμης

Τι είναι bleeding?

- Το bug επιτρέπει σε attackers να αντλούν 64K chunks μνήμης
  - γειτονικής στην SSL heartbeat ενός vulnerable host
- Είναι random chunks δεδομένων σε αυτόν τον χώρο μνήμης
- Η επίθεση μπορεί να επαναληφτεί πολλές φορές
  - Αντλεί περισσότερα random chunks of data
- 64k δε μοιάζει μα αρκετή μνήμη αλλά είναι!

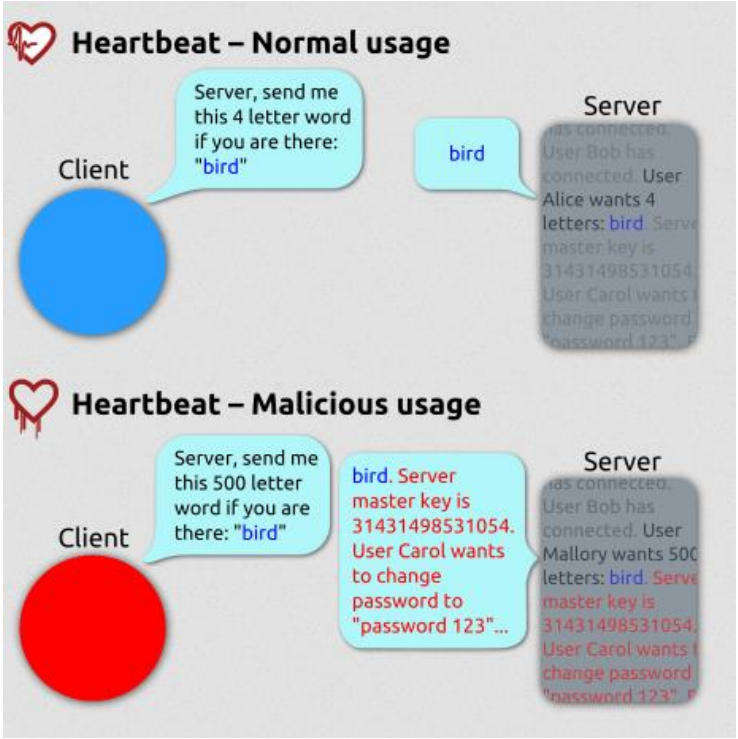
Memory disclosure: τι αντλεί ο επιτιθέμενος

- Shared crypto keys
- Private keys
- Usernames and Passwords
- Session identifiers
- Private data – data payloads

Netcraft: σχεδόν 30.000 από τα άνω των 500.000 πιστοποιητικών X.509 που ήταν ευάλωτα στο κενό ασφαλείας Heartbleed επανεκδόθηκαν ως τις 11 Απριλίου 2014

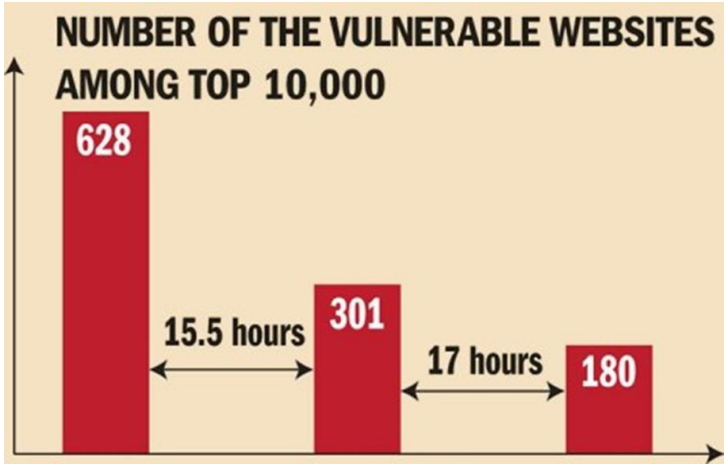
Λεπτομέρειες

- SSL V3 RECORD protocol – messages
- SSL V3 RECORD MESSAGE LENGTH (limited to 4 bytes)
- Η επέκταση RFC 6520 (Heartbeat) ελέγχει τις συνόδους SSL/TLS
  - Ο υπολογιστής στη μία άκρη της σύνδεσης στέλνει «Αίτημα Heartbeat» (περιέχει το φορτίο=μία συμβολοσειρά και το μήκος της).
  - Ο άλλος υπολογιστής, πρέπει να αποστείλει πίσω στον αποστολέα το ίδιο ακριβώς μήνυμα.
  - Όταν η μηχανή του θύματος απαντά υπάρχει επιπλέον χώρος 64k της μνήμης του διακομιστή που επιστρέφετε στον εισβολέα.



Common sites affected

Dropbox	Norton
Facebook	Skype
Google	Wikipedia
Netflix	Yahoo



How may sites are vulnerable
(After vulnerability was reported publically)

List

http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

Search for site

https://lastpass.com/heartbleed/

How do I manage?

http://www.pcmag.com/article2/0,2817,2407168,00.asp
https://lastpass.com/misc_download2.php

SSL Renegotiation Attack

- διαδικασία επαναδιαπραγμάτευσης SSL που επιτρέπει σε έναν εισβολέα να εισφέρει απλό κείμενο σε αιτήματα του θύματος (client)
- ο εισβολέας δεν μπορεί να αποκρυπτογραφήσει την επικοινωνία πελάτη-εξυπηρετητή. Απλά εισφέρει (injects) μυνήματα
- Χρειάζεται MITM attacks (ARP poisoning

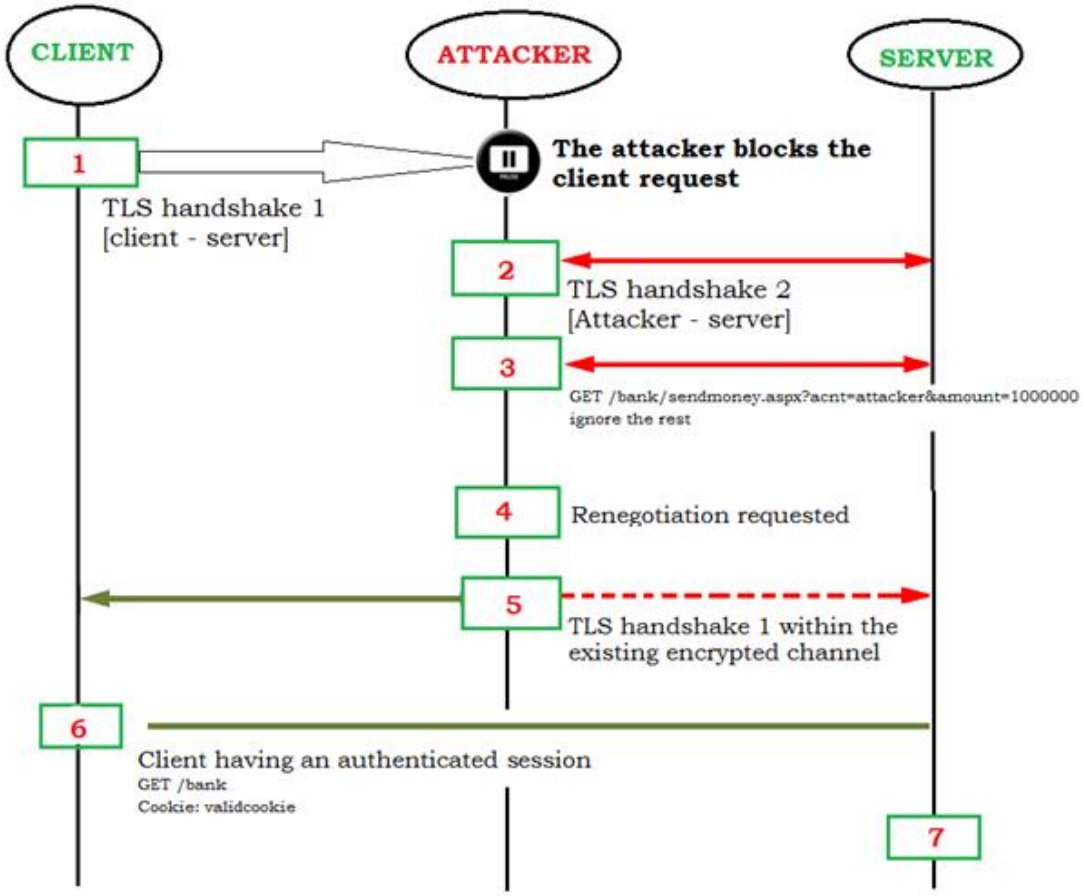
SSL Renegotiation Attack

- Επαναδιαπραγμάτευση SSL χρήσιμη όταν η σύνοδος SSL έχει ήδη καθιερωθεί και πρέπει να λάβει χώρα έλεγχος ταυτότητας πελάτη.
- Πχ σε e-shop που χρησιμοποιεί SSL (HTTPS).
- Αρχικά, στο site ο πελάτης προσθέτει αντικείμενα στο καλάθι
- Όταν αποφασίσει αγορά με κάρτα ή paypal θα ζητηθεί να συνδεθεί στο site
- Πρέπει η σύνοδος SSL να προσαρμοστεί ώστε να επιτρέπει αυθεντικοποίηση. Όποιες και αν είναι οι πληροφορίες που συγκεντρώθηκαν πριν (π.χ., στοιχεία στο καλάθι) πρέπει να διατηρηθούν και μετά την είσοδο χρήστη.
- Η νέα σύνδεση SSL που πρέπει να καθοριστεί θα χρησιμοποιεί την ήδη υπάρχουσα σύνοδο.

SSL Renegotiation Attack

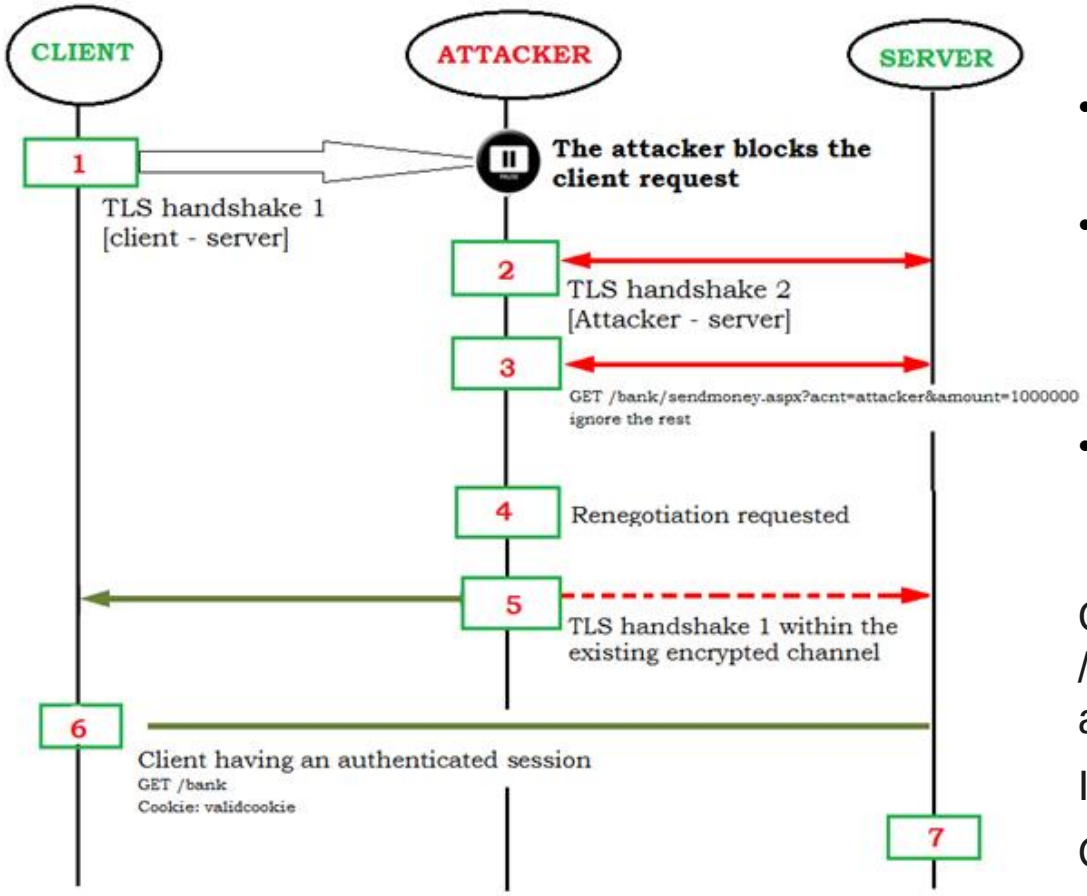
- Χρησιμοποιώντας την επίθεση επανα-διαπραγμάτευσης, ένας εισβολέας μπορεί να εισφέρει εντολές σε μια συνεδρία HTTPs
  - να εισάγει custom responses
  - να εκτελέσει επιθέσεις άρνηση υπηρεσίας
- Ας υποθέσουμε ότι ένας πελάτης θέλει να συνδεθεί με ένα online banking site.
- Ο πελάτης κινεί τη διαδικασία ρουτίνας χειραψίας TLS

SSL Renegotiation Attack



- Τα αίτημα πελάτη μπλοκάρεται από τον MITM
- Ο MITM ξεκινά μια νέα σύνοδο και ολοκληρώνει μια πλήρη χειραψία TLS.
- Ο MITM στέλνει μια αίτηση GET (ζητώντας κατάθεση στον λογαριασμό του) στην εφαρμογή τράπεζας.
- Ο Server ζητά επαναδιαπραγμάτευση (Βήμα 4) για να γίνει login ο αιτούμενος (εδώ ο attacker).
- Η χειραψία TLS που ξεκίνησε στο βήμα 1 (και μπλοκαριστείτε από τον MITM), θα πρέπει τώρα να πρωωθηθεί στο Server

SSL Renegotiation Attack



- Μια νέα χειραψία TLS πάνω από την προηγουμένως established & encrypted TLS session
- Ο πελάτης έχει αυθεντικοποιηθεί στο βήμα 6 και έχει valid cookie
- Λόγω της επαναδια-πραγμάτευσης, ο Server υποθέτει ότι το αίτημα στο βήμα 4 έχει σταλεί από πελάτη.
- το αίτημα που πηγαίνει στο Server έχει ως εξής (θα ερμηνευθεί ως νόμιμο και θα εκτελεστεί).

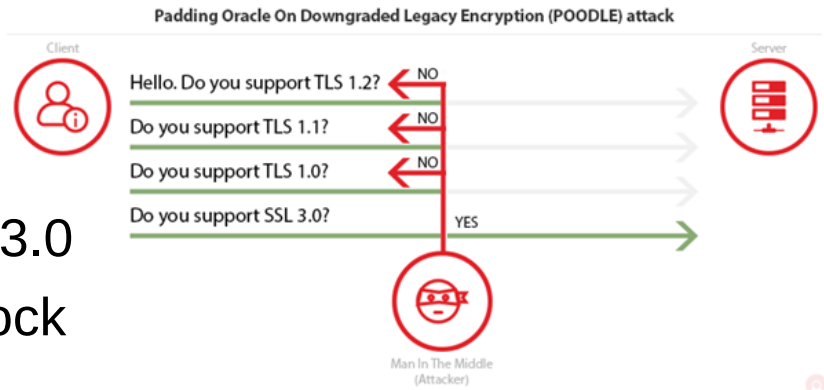
GET /bank/sendmoney.asp?acct=attacker&amount=100000

Ignore the rest: GET /ebanking

Cookie: validcookie

OTHER SSL/TLS Attacks

- POODLE (CVE-2014-3566)
- The Padding Oracle On Downgraded Legacy Encryption. October 2014



- Απαιτεί MiTM για downgrade σε SSL v3.0
- vulnerability in SSL v3.0: σχετικό με Block Padding:
- λόγω Cipher Block Chaining mode οι Block Ciphers έχουν fixed length, άρα τα data στο last block αν δεν είναι multiple του block size, τότε padding. Αν γίνει padding τότε αυτό αγνοείται από server ο οποίος ελέγχει μόνο αν το padding length είναι correct.
- Ένας εισβολέας μπορεί να αποκρυπτογραφήσει encrypted blocks βάζοντας pads και βλέποντας απόκριση από server. Θέλει το πολύ 256 SSL 3.0 requests για να αποκρυπτογραφήσει ένα μόνο byte.
- κωδικός πρόσβασης, cookie

OTHER SSL/TLS Attacks

- BEAST (CVE-2011-3389)
  - Browser Exploit Against SSL/TLS attack (September 2011)
  - affects SSL 3.0 and TLS 1.0
  - vulnerability σε implementation του Cipher Block Chaining (CBC)
  - chosen plaintext attack – requires penetration on victim's browser
- CRIME (CVE-2012-4929)
  - Compression Ratio Info-leak Made Easy
  - ευπάθεια που διαπιστώθηκε στη μέθοδο συμπίεσης του TLS
- BREACH (CVE-2013-3587)
  - Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext
  - ευπάθεια που διαπιστώθηκε στη μέθοδο συμπίεσης του HTTP