Ασκήσεις Ασφάλειας Δικτύων — Πρωτόκολλο TLS / HTTPS

Σημειώσεις Μαθήματος

2.3 Ερωτήσεις – Ασκήσεις – Θέματα για Ανάπτυξη

2.3.1 Ερωτήσεις Σωστού / Λάθους

Εκφώνηση

Πριν την έλευση του WWW δεν υπήρχε τρόπος αναζήτησης στο Διαδίκτυο.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Υπήρχαν μηχανισμοί αναζήτησης (π.χ. Archie, Gopher), αλλά όχι με τη μορφή υπερσυνδέσμων του WWW.

—

Εκφώνηση

Πριν την έλευση του WWW δεν υπήρχε η δυνατότητα ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Το e-mail υπήρχε ήδη από τη δεκαετία του 1970 στο ARPANET.

—

Εκφώνηση

Το μοντέλο πελάτη–εξυπηρετητή είναι αποκλειστικό χαρακτηριστικό του Διαδικτύου.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Το μοντέλο πελάτη–εξυπηρετητή χρησιμοποιείται και σε τοπικά δίκτυα.

—

Εκφώνηση

Ο εξυπηρετητής DNS έχει δύο επίπεδα.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Το DNS λειτουργεί ιεραρχικά με πολλά επίπεδα (root, top-level domains, authoritative servers).

—

Εκφώνηση

Η ονομασία της σελίδας μπορεί να μας δείξει τα επίπεδα του εξυπηρετητή DNS.

- Σωστό
- Λάθος

Απάντηση

Σωστό — Κάθε τμήμα της διεύθυνσης (domain name) αντιστοιχεί σε διαφορετικό επίπεδο DNS.

—

Εκφώνηση

Το Διαδίκτυο δεν υφίσταται χωρίς το WWW.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Το WWW είναι μόνο μία από τις πολλές υπηρεσίες του Διαδικτύου.

—

Εκφώνηση

Δεν μπορούμε να μπούμε στο Διαδίκτυο αν δεν έχουμε ένα φυλλομετρητή.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Μπορούμε να συνδεθούμε και μέσω άλλων εφαρμογών (π.χ. email clients, FTP, SSH).

—

Εκφώνηση

Οι στατικές σελίδες δημιουργούνται στην πλευρά του πελάτη.

- Σωστό
- Λάθος

Απάντηση

Λάθος — Δημιουργούνται στον εξυπηρετητή και απλώς προβάλλονται στον πελάτη.

—

Εκφώνηση

Οι δυναμικές σελίδες δημιουργούνται στην πλευρά του εξυπηρετητή.

- Σωστό
- Λάθος

Απάντηση

Σωστό — Οι δυναμικές σελίδες παράγονται από server-side γλώσσες όπως PHP, JSP, ASP.

—

Εκφώνηση

Τα ενεργά αρχεία εκτελούνται στην πλευρά του πελάτη.

- Σωστό
- Λάθος

Απάντηση

Σωστό — Εκτελούνται στον browser του χρήστη (π.χ. JavaScript, applets).

—

2.3.2 Ερωτήσεις Πολλαπλής Επιλογής

Εκφώνηση

Το ανώνυμο FTP επιτρέπει:

(a) Την πρόσβαση σε οποιαδήποτε πληροφορία υπάρχει στον απομακρυσμένο υπολογιστή

(b) Την πρόσβαση μόνο σε ορισμένες πληροφορίες στον απομακρυσμένο υπολογιστή

(c) Την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες

Απάντηση

(β) Επιτρέπει πρόσβαση μόνο σε συγκεκριμένα δημόσια αρχεία που έχουν οριστεί για ανώνυμη πρόσβαση.

—

Εκφώνηση

Στο μοντέλο πελάτη–εξυπηρετητή:

(a) Ο εξυπηρετητής είναι συγκεκριμένος υπολογιστής με μεγάλη ισχύ

(b) Ο εξυπηρετητής είναι λογισμικό που εξυπηρετεί αιτήματα πελατών

(c) Ο πελάτης και ο εξυπηρετητής είναι πάντα διαφορετικοί υπολογιστές

Απάντηση

(β) Ο όρος “εξυπηρετητής” αναφέρεται στο λογισμικό που δέχεται αιτήματα και τα εξυπηρετεί.

—

Εκφώνηση

Για να στείλουμε μήνυμα με ηλεκτρονικό ταχυδρομείο:

(a) Πρέπει να έχουμε πρόσβαση στον υπολογιστή του παραλήπτη

(b) Πρέπει ο υπολογιστής του παραλήπτη να είναι ανοικτός

(c) Αρκεί ο παραλήπτης να διαθέτει θυρίδα e-mail

(d) Να έχουμε πρόσβαση σε πρόγραμμα ηλεκτρονικού ταχυδρομείου

Απάντηση

(γ) και (δ) — Αρκεί να υπάρχει θυρίδα e-mail και λογισμικό ταχυδρομείου.

—

Εκφώνηση

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου:

(a) Μπορεί να μην έχει θέμα και κείμενο

(b) Μπορεί να μην έχει αποστολέα

(c) Μπορεί να μην έχει παραλήπτη

(d) Μπορεί να μην έχει ημερομηνία

Απάντηση

(α) Είναι δυνατόν να σταλεί μήνυμα χωρίς θέμα ή κείμενο, αλλά πρέπει να υπάρχει παραλήπτης και ημερομηνία.

—

Εκφώνηση

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου:

(a) Μπορεί να σταλεί σε περισσότερους από έναν παραλήπτες

(b) Μπορεί να σταλεί σε πολλούς χωρίς να το γνωρίζουν όλοι οι άλλοι παραλήπτες (BCC)

Απάντηση

Και τα δύο είναι σωστά — το BCC (Blind Carbon Copy) κρύβει τους υπόλοιπους παραλήπτες.

—

Εκφώνηση

Το μήνυμα που θα παραληφθεί μέσω ηλεκτρονικού ταχυδρομείου:

(a) Θα έχει το ίδιο μέγεθος

(b) Θα έχει μεγαλύτερο μέγεθος

(c) Θα έχει μικρότερο μέγεθος

Απάντηση

(β) — Συνήθως έχει ελαφρώς μεγαλύτερο μέγεθος λόγω προσθήκης headers και metadata κατά τη μετάδοση.

2.3.3 Θέματα για Ανάπτυξη

Εκφώνηση

Περιγράψτε τα βήματα που ακολουθεί η αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Συγκρίνετέ τα με την αποστολή:

- ενός φακέλου μέσω κλασικού ταχυδρομείου και
- ενός μηνύματος μέσω κινητού τηλεφώνου.

Σχολιάστε αν πρόκειται για διαδικασία με σύνδεση ή χωρίς σύνδεση.

Απάντηση

Η αποστολή e-mail περιλαμβάνει σύνταξη, δρομολόγηση μέσω SMTP και παράδοση σε θυρίδα. Σε σχέση με το ταχυδρομείο, έχει παρόμοια λογική "αποστολέα–παραλήπτη". Είναι "χωρίς σύνδεση", καθώς ο παραλήπτης δεν χρειάζεται να είναι online τη στιγμή αποστολής.

—

Εκφώνηση

Να συγκρίνετε το DNS με τη χρήση τηλεφωνικού καταλόγου για την εύρεση αριθμών.

Απάντηση

Το DNS αντιστοιχεί ονόματα (domain names) σε αριθμητικές διευθύνσεις IP, όπως ένας τηλεφωνικός κατάλογος αντιστοιχεί ονόματα σε αριθμούς τηλεφώνου.

—

Εκφώνηση

Αναλύστε τι είναι το πρωτόκολλο HTTPS και περιγράψτε πώς λειτουργεί. Αναφέρετε τα οφέλη της χρήσης του.

Απάντηση

Το HTTPS είναι συνδυασμός HTTP και TLS για ασφαλή επικοινωνία. Κρυπτογραφεί τα δεδομένα, εξασφαλίζει την αυθεντικότητα του εξυπηρετητή και την ακεραιότητα των πληροφοριών. Προσφέρει εμπιστευτικότητα και ασφάλεια σε ευαίσθητες συναλλαγές.

Άσκηση 1 – TLS Handshake

Εκφώνηση

Ο browser του χρήστη ζητά τη σελίδα `https://example.com`.

(a) Ποια είναι τα βασικά στάδια της διαδικασίας *TLS Handshake*;

(b) Ποιοι τύποι κλειδιών χρησιμοποιούνται και σε ποιο στάδιο (ασύμμετρα ή συμμετρικά);

Απάντηση

(α) Κατά τη χειραψία TLS: 1. Ο client στέλνει *Client Hello* με τις υποστηριζόμενες εκδόσεις και αλγορίθμους. 2. Ο server απαντά με *Server Hello* και στέλνει το ψηφιακό του πιστοποιητικό (με δημόσιο κλειδί). 3. Ακολουθεί διαπραγμάτευση κλειδιών και δημιουργία ενός *session key*. 4. Και οι δύο πλευρές στέλνουν μηνύματα "Finished" για επιβεβαίωση.
(β) Η αρχική ανταλλαγή γίνεται με **ασύμμετρη κρυπτογράφηση**, ενώ τα δεδομένα της συνεδρίας κρυπτογραφούνται με **συμμετρικό κλειδί**.

—

Άσκηση 2 – Θύρα HTTPS

Εκφώνηση

Κατά τη ρύθμιση ενός web server, ο διαχειριστής χρησιμοποίησε θύρα `80` για HTTPS.

(a) Γιατί η σύνδεση αποτυγχάνει;

(b) Ποια είναι η σωστή θύρα για HTTPS;

Απάντηση

(α) Η θύρα 80 είναι προκαθορισμένη για HTTP χωρίς κρυπτογράφηση. Το TLS απαιτεί ειδική διαχείριση της συνεδρίας με handshake, που δεν υποστηρίζεται στη θύρα 80. (β) Η σωστή θύρα είναι η **443**, η οποία χρησιμοποιεί το πρωτόκολλο TLS/SSL.

—

Άσκηση 3 – Ανακατεύθυνση σε HTTPS

Εκφώνηση

Δίνεται η απάντηση:

```
HTTP/1.1 301 Moved Permanently
Location: https://secure.example.com/login
```

(a) Τι επιτυγχάνει ο εξυπηρετητής με αυτή την απάντηση;

(b) Ποιος είναι ο λόγος που οι ιστότοποι κάνουν redirect σε HTTPS;

Απάντηση

(α) Ο server ενημερώνει τον client ότι η σελίδα έχει μετακινηθεί μόνιμα στη νέα, ασφαλή διεύθυνση HTTPS. (β) Το redirect εξασφαλίζει ότι όλες οι επικοινωνίες θα γίνουν κρυπτογραφημένα, προστατεύοντας δεδομένα login και cookies.

—

Άσκηση 4 – Πιστοποιητικό HTTPS

Εκφώνηση

Σε ένα πιστοποιητικό εμφανίζεται:

- Εκδότης: Let’s Encrypt Authority X3
- Λήξη: 10/05/2026
- Αλγόριθμος: RSA 2048-bit

(a) Τι ρόλο παίζει η αρχή έκδοσης (CA);

(b) Πώς επηρεάζει η ημερομηνία λήξης την ασφάλεια;

Απάντηση

(α) Η CA επιβεβαιώνει την ταυτότητα του κατόχου του domain. (β) Μετά τη λήξη, το πιστοποιητικό θεωρείται μη έγκυρο και η σύνδεση HTTPS δεν επιτρέπεται.

—

Άσκηση 5 – Καθυστέρηση TLS

Εκφώνηση

Η αποστολή μέσω HTTPS φαίνεται πιο αργή από HTTP.

(a) Γιατί αυξάνεται η καθυστέρηση;

(b) Ποιο είναι το πλεονέκτημα του HTTPS παρά το overhead;

Απάντηση

(α) Το TLS χρειάζεται επιπλέον βήματα handshake, δημιουργία κλειδιών και κρυπτογράφηση/αποκρυπτογράφηση. (β) Αν και πιο αργό, παρέχει εμπιστευτικότητα, ακεραιότητα και αυθεντικοποίηση.

—

Άσκηση 6 – Μήνυμα σφάλματος πιστοποιητικού

Εκφώνηση

Ο browser εμφανίζει: “Your connection is not private”.

(a) Τι σημαίνει για τη TLS σύνδεση;

(b) Τι πρέπει να κάνει ο χρήστης;

Απάντηση

(α) Το πιστοποιητικό έχει λήξει ή δεν είναι αξιόπιστο. (β) Ο χρήστης πρέπει να ελέγξει τη διεύθυνση URL και να περιμένει ανανέωση του πιστοποιητικού — όχι να συνεχίσει τη μη έγκυρη σύνδεση.

—

Άσκηση 7 – Ανάλυση πακέτων Wireshark

Εκφώνηση

Στο Wireshark εμφανίζονται:

`Client Hello → Server Hello → Certificate → Server Hello Done`

(a) Ποιο στάδιο TLS αντιπροσωπεύουν;

(b) Ποιο μήνυμα περιέχει το δημόσιο κλειδί του server;

Απάντηση

(α) Είναι τα αρχικά στάδια του TLS Handshake: διαπραγμάτευση αλγορίθμων και παρουσίαση πιστοποιητικού. (β) Το δημόσιο κλειδί περιλαμβάνεται στο μήνυμα **Certificate**.

—

Άσκηση 8 – Επικοινωνία χωρίς HTTPS

Εκφώνηση

Ένας ιστότοπος χρησιμοποιεί μόνο HTTP.

(a) Ποια είναι η βασική αδυναμία αυτής της προσέγγισης;

(b) Πώς βελτιώνεται η ασφάλεια με την ενεργοποίηση HTTPS;

Απάντηση

(α) Στο HTTP τα δεδομένα μεταδίδονται ως απλό κείμενο χωρίς καμία προστασία. (β) Με το HTTPS ενεργοποιείται το TLS, που προσφέρει κρυπτογράφηση και επιβεβαίωση ταυτότητας του server.

—

Άσκηση 9 – Μικτό περιεχόμενο (Mixed Content)

Εκφώνηση

Σε ιστότοπο HTTPS υπάρχουν εικόνες με σύνδεσμο `http://`.

(a) Γιατί εμφανίζεται προειδοποίηση “Mixed Content”;

(b) Πώς λύνεται το πρόβλημα;

Απάντηση

(α) Το HTTPS εγγυάται ασφάλεια μόνο αν όλα τα στοιχεία της σελίδας φορτώνονται κρυπτογραφημένα. Αν κάποιο στοιχείο έρθει από HTTP, υπάρχει ασυνέπεια στην ασφάλεια. (β) Όλες οι αναφορές πρέπει να γίνουν σε `https://` URLs.

—

Άσκηση 10 – Διάγραμμα ροής HTTPS

Εκφώνηση

Περιγράψτε τη ροή λειτουργίας HTTPS:

(a) Εγκαθίδρυση TCP.

(b) Διαπραγμάτευση TLS.

(c) Κρυπτογραφημένη επικοινωνία.

Απάντηση

1. Δημιουργείται TCP σύνδεση στη θύρα 443. 2. Πραγματοποιείται TLS handshake και δημιουργία session key. 3. Όλη η μεταφορά δεδομένων (HTTP αιτήματα/απαντήσεις) γίνεται κρυπτογραφημένα. Όταν η σύνδεση κλείσει, τα προσωρινά κλειδιά διαγράφονται.

—

Άσκηση 11 – Έλεγχος εγκυρότητας πιστοποιητικού

Εκφώνηση

Κατά τη φόρτωση μιας σελίδας HTTPS, ο browser ελέγχει το πιστοποιητικό.

(a) Ποιες πληροφορίες ελέγχει για να το αποδεχθεί;

(b) Τι συμβαίνει αν η υπογραφή ή το όνομα δεν ταιριάζουν;

Απάντηση

(α) Ελέγχει: — αν η υπογραφή είναι έγκυρη από αξιόπιστη CA, — αν το όνομα domain ταιριάζει, — και αν δεν έχει λήξει. (β) Αν κάποιο κριτήριο αποτύχει, εμφανίζεται προειδοποίηση και η σύνδεση δεν θεωρείται ασφαλής.

—

Άσκηση 12 – Τύποι Κρυπτογράφησης στο TLS

Εκφώνηση

Αντιστοιχίστε τον τύπο κρυπτογράφησης με τον σωστό σκοπό χρήσης στο πρωτόκολλο TLS:

(a) **Δημόσιο κλειδί (Public Key)**

(b) **Συμμετρικό κλειδί (Symmetric Key)**

(c) **Hash συνάρτηση (Hash Function)**

Πιθανοί σκοποί:

(i) Έλεγχος ακεραιότητας μηνυμάτων.

(ii) Ανταλλαγή κλειδιών και αυθεντικοποίηση server/πελάτη.

(iii) Γρήγορη κρυπτογράφηση και αποκρυπτογράφηση δεδομένων της συνεδρίας.

Να γίνει η σωστή αντιστοίχιση:

Απάντηση

(a) Δημόσιο κλειδί → Ανταλλαγή κλειδιών και αυθεντικοποίηση.
(b) Συμμετρικό κλειδί → Γρήγορη κρυπτογράφηση δεδομένων.
(c) Hash συνάρτηση → Έλεγχος ακεραιότητας μηνυμάτων.

—

Άσκηση 13 – Ενημέρωση Πιστοποιητικού

Εκφώνηση

Ο server έχει πιστοποιητικό που λήγει σε 2 μέρες.

(a) Τι πρέπει να κάνει ο διαχειριστής;

(b) Τι συμβαίνει αν το αφήσει να λήξει;

Απάντηση

(α) Να εκδώσει νέο πιστοποιητικό (renew) από την ίδια ή άλλη CA. (β) Οι browsers θα μπλοκάρουν τις συνδέσεις HTTPS, εμφανίζοντας προειδοποίηση κινδύνου.

—

Άσκηση 14 – TLS 1.3 vs 1.2

Εκφώνηση

Συγκρίνετε TLS 1.2 και TLS 1.3 ως προς:

(a) Ταχύτητα χειραψίας,

(b) Ασφάλεια,

(c) Υποστηριζόμενους αλγορίθμους.

Απάντηση

(α) Το TLS 1.3 χρειάζεται μόνο 1 round-trip, ενώ το TLS 1.2 χρειάζεται 2. (β) Το TLS 1.3 καταργεί παλαιούς αδύναμους αλγόριθμους. (γ) Υποστηρίζει ισχυρούς όπως AES-GCM και ChaCha20, με αυξημένη ταχύτητα και ασφάλεια.

—

Άσκηση 14 – TLS 1.3 vs 1.2

Εκφώνηση

Συγκρίνετε TLS 1.2 και TLS 1.3 ως προς:

(a) Ταχύτητα χειραψίας,

(b) Ασφάλεια,

(c) Υποστηριζόμενους αλγορίθμους.

Απάντηση

(α) Το TLS 1.3 χρειάζεται μόνο 1 round-trip, ενώ το TLS 1.2 χρειάζεται 2. (β) Το TLS 1.3 καταργεί παλαιούς αδύναμους αλγόριθμους. (γ) Υποστηρίζει ισχυρούς όπως AES-GCM και ChaCha20, με αυξημένη ταχύτητα και ασφάλεια.

—

Άσκηση 15 – Παράδειγμα HTTP vs HTTPS

Εκφώνηση

Δίνεται το παρακάτω αίτημα:

```
GET /login HTTP/1.1
Host: example.com
```

(a) Τι διαφορά έχει το ίδιο αίτημα όταν αποστέλλεται μέσω HTTPS;

(b) Ποια επιπλέον στρώματα ασφαλείας προστίθενται;

Απάντηση

(α) Στο HTTPS, το αίτημα μεταφέρεται μέσα σε κρυπτογραφημένο κανάλι TLS, άρα δεν είναι αναγνώσιμο. (β) Προστίθεται το στρώμα ασφαλείας TLS που εξασφαλίζει εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα του server.

—

Άσκηση 16 – Παράδειγμα Header Πιστοποιητικού

Εκφώνηση

Στο παρακάτω απόσπασμα HTTPS απάντησης:

```
Server: Apache/2.4.57 (Unix)
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

(a) Τι κάνει η επικεφαλίδα `Strict-Transport-Security`;

(b) Γιατί είναι σημαντική για την ασφάλεια HTTPS;

Απάντηση

(α) Υποχρεώνει τον browser να συνδέεται πάντα μέσω HTTPS για το domain, ακόμη κι αν ο χρήστης πληκτρολογήσει HTTP. (β) Προστατεύει από ακούσια ή σκόπιμη υποβάθμιση σύνδεσης σε μη ασφαλές HTTP.

—

Άσκηση 17 – Παράδειγμα Επικοινωνίας TLS

Εκφώνηση

Ο client και ο server ολοκληρώνουν επιτυχώς το TLS Handshake.

(a) Πώς εξασφαλίζεται ότι τρίτος δεν μπορεί να δει τα δεδομένα της συνεδρίας;

(b) Πώς ο server γνωρίζει ότι το μήνυμα ήρθε από τον σωστό client;

Απάντηση

(α) Όλα τα δεδομένα κρυπτογραφούνται με το session key, που είναι μοναδικό για τη συνεδρία. (β) Χρησιμοποιούνται μηχανισμοί MAC (Message Authentication Code) και hash, ώστε κάθε μήνυμα να συνοδεύεται από έλεγχο ακεραιότητας.

—

Άσκηση 18 – Ανάλυση Πεδίων HTTPS Απάντησης

Εκφώνηση

Αναλύστε τα παρακάτω πεδία HTTP απάντησης που στάλθηκε μέσω HTTPS:

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 1456
Connection: close
```

(a) Τι δηλώνει κάθε γραμμή;

(b) Ποιο από αυτά τα πεδία σχετίζεται με τη διαχείριση της σύνδεσης;

Απάντηση

(α) - `HTTP/1.1 200 OK`: Επιτυχής απάντηση. - `Content-Type`: Ορίζει τον τύπο δεδομένων (HTML). - `Content-Length`: Δηλώνει το μέγεθος σε bytes. - `Connection: close`: Ο server θα κλείσει τη σύνδεση μετά τη μετάδοση. (β) Το πεδίο `Connection` αφορά τη διαχείριση της σύνδεσης.