Ασφάλεια Συστημάτων

Τζέριες Μπεσαράτ, PhD

18 Μαρτίου 2022, Άρτα

Ασφάλεια Συστημάτων

Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών, είναι ένα **γνωστικό πεδίο** της επιστήμης της πληροφορικής, και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, που ασχολείται με:

την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους.

Στο προηγούμενο μάθημα αναπτύξαμε

- Αγαθά
- Ιδιοκτήτες & Χρήστες
- Ιδιότητες
- Ζημιά
- Κίνδυνοι
- Στόχοι
- Εξασφάλιση
- Μέσα Προστασίας
- Ασφάλεια Υποδομών

Βασικές Έννοιες και Ζητήματα Ασφαλείας

Η Ασφάλεια Πληροφοριών (Information Security) αποσκοπεί στην προστασία των πληροφοριών και των πόρων ενός πληροφοριακού συστήματος γενικότερα, από πιθανές ζημιές που μπορεί να προκαλέσουν μείωση της αξίας τους. Επιπλέον, αποσκοπεί στην παροχή αξιόπιστων πληροφοριών, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες όταν τις χρειάζονται.
Μια πιο πρακτική θεώρηση της ασφάλειας πληροφοριών, με πολλές αναφορές στην καθημερινότητά μας, είναι ως μια διαδικασία που αποτελείται από τρία διακριτά βήματα:

Βήματα για την ασφάλεια

Τα παραπάνω βήματα είναι κοινά σε διαφορετικά πεδία εφαρμογής, που είναι γνωστά από την καθημερινότητα. Για παράδειγμα, για την προστασία ενός εταιρικού χώρου, οι παραπάνω φάσεις θα μεταφράζονταν στις ενέργειες που αναφέρονται στον ακόλουθο Πίνακα:

ΠΡΟΛΗΨΗ	**ΑΝΙΧΝΕΥΣΗ**	**ΑΝΤΙΔΡΑΣΗ**
Προσθήκη κλειδαριάς	Απουσία εξοπλισμού	Κλήση αστυνομίας
Χτίσιμο φράκτη	Χρήση κλειστού κυκλώματος τηλεόρασης (CCTV)	Χρήση ασφαλιστικής κάλυψης
Κάγκελα στα παράθυρα	Σύστημα συναγερμού	Σύμβαση με εταιρεία φύλαξης

Βήματα για την ασφάλεια στον χώρο ΤΠΕ

Στο χώρο των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ), τα πράγματα δεν είναι πολύ διαφορετικά. Για παράδειγμα, στο σύστημα ηλεκτρονικής βιβλιοθήκης ενός πανεπιστημίου, τα παραπάνω βήματα θα αφορούσαν ενέργειες ανάλογες αυτών που εμφανίζονται στον Πίνακα:

ΠΡΟΛΗΨΗ	**ΑΝΙΧΝΕΥΣΗ**	**ΑΝΤΙΔΡΑΣΗ**
Έλεγχος για κρυπτογραφημένη μετάδοση ευαίσθητων δεδομένων σύνδεσης στο υποσύστημα δανεισμού.	Εντοπισμός «περίεργων» εγγραφών στο υποσύστημα δανεισμού.	Αμφισβήτηση δανεισμών και αλλαγή διαπιστευτηρίων σύνδεσης (username και password).

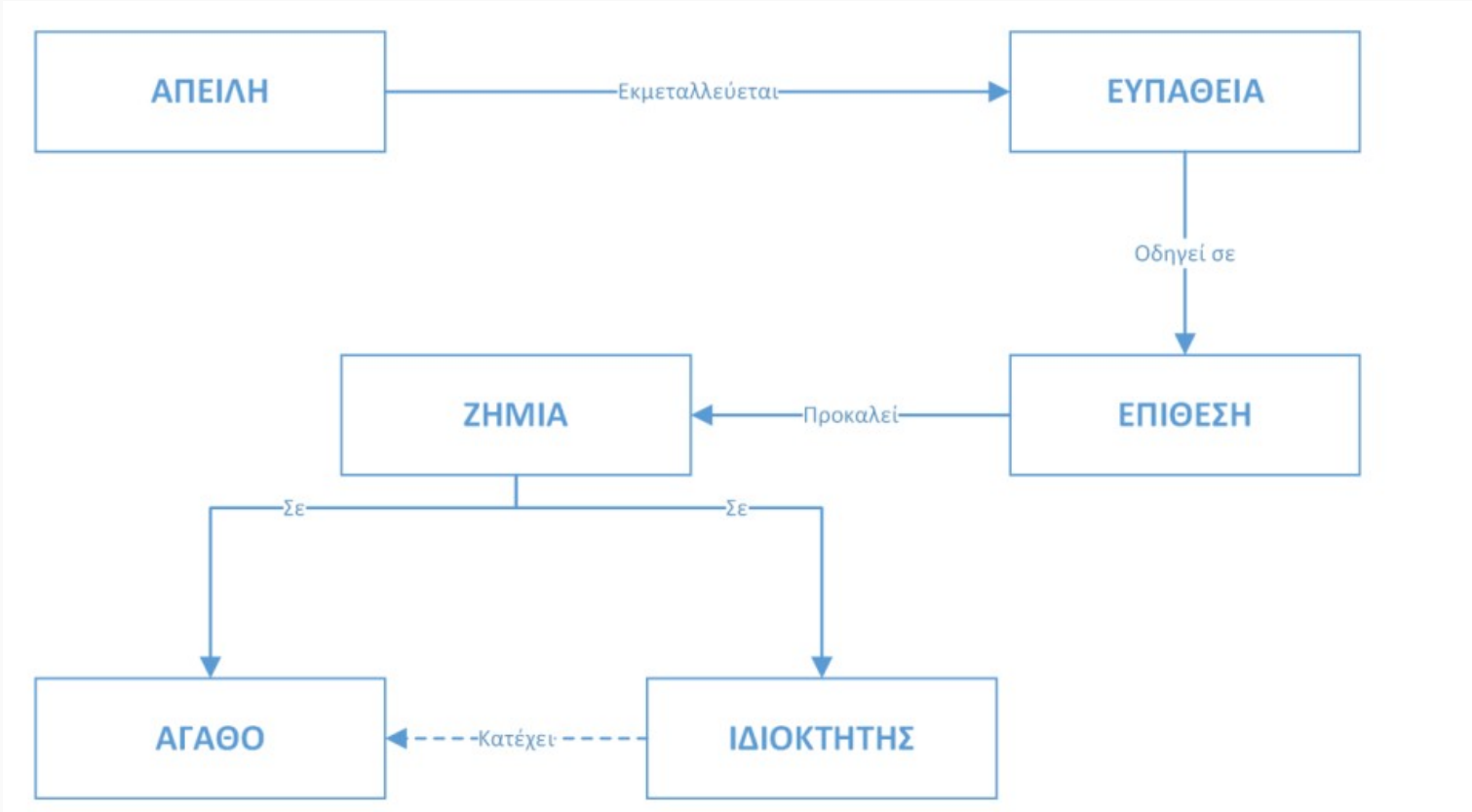
Στόχοι Ασφάλειας στις ΤΠΕ είναι:

- Προστασία Υπολογιστικών Συστημάτων (Computer Security): Διαφύλαξη υπολογιστικών πόρων συστήματος από μη εξουσιοδοτημένη χρήση και προστασία δεδομένων από ακούσια ή σκόπιμη αποκάλυψη ή τροποποίηση ή διαγραφή κατά την επεξεργασία και αποθήκευσή τους.

- Προστασία Επικοινωνιών (Communication Security): Διαφύλαξη δικτυακών πόρων και προστασία δεδομένων από ακούσια ή σκόπιμη αποκάλυψη ή τροποποίηση ή διαγραφή κατά τη μετάδοσή τους μέσω δικτύων υπολογιστών.

Ασφάλεια = Επιτυχημένη εφαρμογή των ακόλουθων μηχανισμών:

- **Αναγνώριση (Identification)**: αφορά τη διαδικασία παρουσίασης της ταυτότητας μιας οντότητας (π.χ. πελάτη) στο σύστημα (π.χ. εξυπηρετητή).
- **Αυθεντικοποίηση (Authentication)**: αφορά τη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα.
- **Εξουσιοδότηση (Authorization)**: αφορά τη διαδικασία λήψης απόφασης σχετικά με την
  αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μιας αυθεντικοποιημένης οντότητας στο σύστημα, στη βάση των δικαιωμάτων πρόσβασης που της έχουν ήδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος.
- **Αδυναμία αποποίησης (Non-Repudiation)**: αφορά τη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μιας ενέργειας στο σύστημα.


ΑΠΕΙΛΗ
Εκμεταλλεύεται
ΕΥΠΑΘΕΙΑ
Οδηγεί σε
ΖΗΜΙΑ
Προκαλεί
ΕΠΙΘΕΣΗ
Σε
Σε
ΑΓΑΘΟ
Κατέχει
ΙΔΙΟΚΤΗΤΗΣ

Ζητήματα Ασφάλειας στο Διαδίκτυο

Πιθανές επιθέσεις:

- **Πλαστοπροσωπία (masquerading)**
- **Παθητική παρακολούθηση (passive tapping)**
- **Ενεργή παρακολούθηση (active tapping)**
- **Αποποίηση (repudiation)**
- **Άρνηση Εξυπηρέτησης (denial of service)**
- **Επανεκπομπή μηνυμάτων (replay)**
- **Ανάλυση επικοινωνίας (traffic analysis)**
- **Κακόβουλο λογισμικό (viruses, Trojan horses, worms)**

Πιθανές Συνέπειες

- **Αποκάλυψη πληροφοριών**
- **Αλλοίωση πληροφοριών**
- **Άρνηση Εξυπηρέτησης**
- **Δυσφήμηση**
- **Κόστος**

Δίκτυα και Διαδίκτυο (1/2)

Αλήθεια.. Γνωρίζουμε τι είναι Δίκτυο;

Δίκτυα και Διαδίκτυο (1/2)

Αλήθεια.. Γνωρίζουμε τι είναι Δίκτυο;

- Μια διασυνδεδεμένη ομάδα υπολογιστικών συστημάτων ονομάζεται **δίκτυο**

Τα βασικά συστατικά ενός δικτύου υπολογιστών είναι:

- Υπολογιστικές συσκευές (υπολογιστές, εκτυπωτές, δρομολογητές κλπ.) ως κόμβοι.
- Γραμμές μεταφοράς δεδομένων μεταξύ των κόμβων.
- Λογισμικό και πρωτόκολλα δικτύωσης

Δίκτυα και Διαδίκτυο (2/2)

Ο πιο συχνός διαχωρισμός των δικτύων γίνεται με βάση της διασποράς των συστημάτων στο χώρο, καθώς και του ιδιαίτερου ρόλου που καλούνται να επιτελέσουν. Έτσι, μπορούμε να διακρίνουμε τις παρακάτω κατηγορίες δικτύων υπολογιστών:

- Δίκτυα Τοπικής Περιοχής (Local Area Networks - LAN).
- Δίκτυα Ευρείας Περιοχής (Wide Area Networks - WAN).
- Μητροπολιτικά Δίκτυα (Metropolitan Area Networks - MAN).
- Δίκτυα Προσωπικής Περιοχής (Personal Area Networks - PAN).

Κατηγορίες Δικτύων:
Δίκτυα Τοπικής Περιοχής

Η πιο απλή μορφή δικτύου, που συναντάμε καθημερινά, είναι τα δίκτυα υπολογιστών τα οποία βρίσκονται σε έναν ενιαίο διαχειριστικά χώρο, όπως τα οικιακά δίκτυα ή τα δίκτυα σε μικρές ή μεσαίες επιχειρήσεις.

Τα βασικά συστατικά των δικτύων αυτών είναι υπολογιστές και διακομιστές, μεταγωγείς, ασύρματα σημεία πρόσβασης και συνήθως ένας δρομολογητής που αναλαμβάνει τη διασύνδεσή τους με απομακρυσμένα δίκτυα.

Η διασύνδεση των στοιχείων αυτών γίνεται με συνδέσμους υψηλής διαμεταγωγικής ικανότητας, όπως καλώδια UTP ή οπτικές ίνες.

Κατηγορίες Δικτύων:
Δίκτυα Ευρείας Περιοχής

Τα δίκτυα ευρείας περιοχής, συνήθως, αποτελούνται από διασυνδεδεμένα τοπικά δίκτυα, τα οποία βρίσκονται διασπαρμένα σε μια μεγάλη γεωγραφική περιοχή. Η σύνδεση των δικτύων αυτών μεταξύ τους γίνεται συνήθως με μη-ιδιόκτητες, χαμηλότερης διαμεταγωγικής ικανότητας γραμμές, που ανήκουν σε κάποιο πάροχο υπηρεσιών δικτύωσης. Οι γραμμές αυτές παρουσιάζουν συνήθως υψηλό κόστος, κάτι που αποτελεί περιοριστικό παράγοντα για την ανάπτυξή τους.

Κατηγορίες Δικτύων: Μητροπολιτικά Δίκτυα

Ένα μητροπολιτικό δίκτυο αποτελείται από ένα σύνολο δικτύων στα στενά πλαίσια της γεωγραφικής έκτασης κτιρίων ενός οργανισμού (campus) ή μιας κοινότητας (π.χ. ενός δήμου). Συνήθως, η γεωγραφική διασπορά δεν είναι μεγάλη και η διασύνδεση των τοπικών δικτύων γίνεται με ιδιωτικές ασύρματες ή ενσύρματες ζεύξεις.

Κατηγορίες Δικτύων:
Δίκτυα Προσωπικής Περιοχής

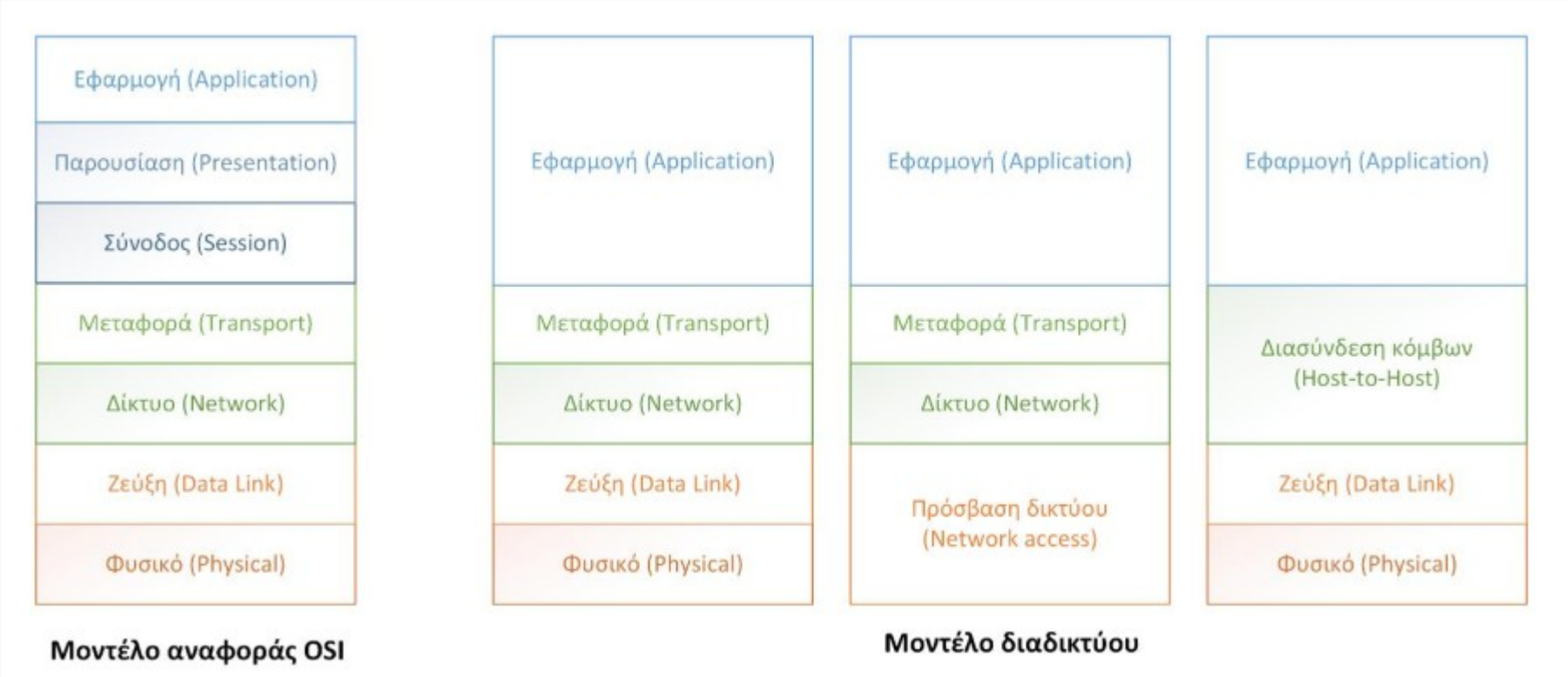
Η ανάπτυξη των σύγχρονων προσωπικών ψηφιακών βοηθών (personal assistant), δηλαδή φορητών υπολογιστικών συσκευών με δυνατότητες δικτύωσης (π.χ. smartphones, smart watches κλπ.), έχουν οδηγήσει στον ορισμό μιας νέας κατηγορίας δικτύων που εκτείνονται γύρω από το πρόσωπο, το οποίο και ακολουθούν καθώς κινείται. Στα δίκτυα προσωπικής περιοχής, οι συμμετέχουσες συσκευές διασυνδέονται με χαμηλής ισχύος ασύρματες ζεύξεις (π.χ. Bluetooth).

Διαστρωμάτωση

Για την διευκόλυνση της μελέτης ενός δικτύου και την καλύτερη σχεδίασή του, μπορούμε να οργανώσουμε τα πρωτόκολλα επικοινωνίας σε επίπεδα.

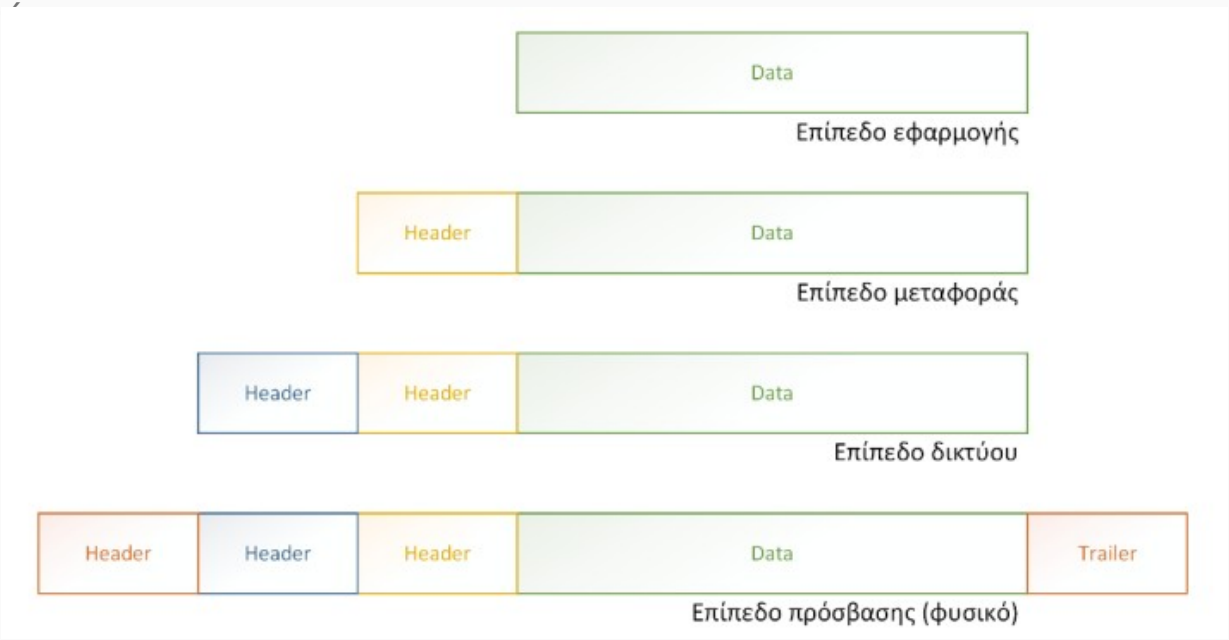
Το πιο γνωστό μοντέλο οργάνωσης πρωτοκόλλων επικοινωνίας είναι το Μοντέλο Διεπαφής Ανοικτών Συστημάτων (Open Systems Interconnection Model – OSI Model) ISO/IEC 7498-1, το οποίο διαμορφώθηκε από το Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization) με την τελευταία αναθεώρησή του το 1994. Το μοντέλο αυτό περιγράφει επτά (7) επίπεδα οργάνωσης πρωτοκόλλων και η πληρότητά του το αναγάγει σε μοντέλο αναφοράς (Reference Model).

Τα πρωτόκολλα των σύγχρονων TCP/IP δικτύων ακολουθούν το Μοντέλο αναφοράς του Διαδικτύου (Internet Model), το οποίο διακρίνει λιγότερα επίπεδα από το Μοντέλο OSI



Ενθυλάκωση πληροφορίας

Σύμφωνα με το μοντέλο αναφοράς, όταν ένας κόμβος αποστέλλει πληροφορία, η πληροφορία αυτή μεταφέρεται μεταξύ των επιπέδων. Η πληροφορία που προέρχεται από το ανώτερο επίπεδο, ενθυλακώνεται κατάλληλα έτσι ώστε να αποσταλεί στο αμέσως κατώτερο. Η ενθυλάκωση αυτή γίνεται με την προσθήκη κεφαλίδας, έτσι ώστε τα πρωτόκολλα του αντίστοιχου επιπέδου στη μεριά του παραλήπτη να μπορούν να χειριστούν κατάλληλα την πληροφορία αυτ



Τέσσερα επίπεδα του Μοντέλου του Διαδικτύου

- Το Επίπεδο Πρόσβασης Δικτύου
  - Πρόσβαση στο μέσο
  - Ανίχνευση και διόρθωση σφαλμάτων
  - Έλεγχος ισοτιμίας
  - Κυκλικός Έλεγχος Πλεονασμού
  - Δημιουργία κύκλων
  - Επιθέσεις επιπέδου ζεύξης
    - Sniffing
    - MAC Spoofing
- **Το Επίπεδο Δικτύου**
  - IPv4
    - Subnetting
    - Μετάφραση διεύθυνσης
    - Επίθεση IP Spoofing
  - IPv6
  - Δρομολόγηση
  - ICMP
  - ARP
- **Το επίπεδο Μεταφοράς**
  - Το πρωτόκολλο TCP
  - Το πρωτόκολλο UDP
- **Το επίπεδο Εφαρμογής**
  - Σύστημα ονοματοδοσίας
  - Επιθέσεις επιπέδου εφαρμογής
    - Packet Interception
    - Betrayal by Trusted Server
    - Distributed Denial of Service
    - Cache Poisoning
  - Το πρωτόκολλο HTTP
  - Ηλεκτρονική αλληλογραφία

Το Επίπεδο Πρόσβασης Δικτύου

Το επίπεδο πρόσβασης δικτύου (ή επίπεδο ζεύξης) και τα πρωτόκολλα που υλοποιούνται σε αυτό, ασχολούνται με τη μεταφορά πλαισίων (frames) από άκρο σε άκρο μιας ζεύξης και ελέγχουν ενέργειες, όπως:

- η πρόσβαση στο μέσο (medium access),
- η ανίχνευση σφαλμάτων (error detection),
- η διόρθωση σφαλμάτων (error correction),
- η αναμετάδοση (retransmission) και ο έλεγχος ροής (flow control)

Το Επίπεδο Πρόσβασης Δικτύου

Κάθε κόμβος αποκτά πρόσβαση στο φυσικό μέσο με τη χρήση κατάλληλων διεπαφών, γνωστών ως Network Interface Cards (NIC).

Κάθε τέτοια διεπαφή έχει μια μοναδική διεύθυνση πρόσβασης στο μέσο (Media Access Control address), γνωστή ως διεύθυνση MAC (MAC address) με μήκος 48 bit.

Η MAC address που αποτελείται μόνο από 1 (FF:FF:FF:FF:FF:FF), ονομάζεται broadcast address (διεύθυνση εκπομπής) και έχει ως προορισμό κάθε συνδεδεμένο κόμβο.

Το Επίπεδο Πρόσβασης Δικτύου:
Πρόσβαση στο μέσο

Μια μη αποδεκτή κατάσταση σε ότι αφορά την πρόσβαση στο φυσικό μέσο είναι η σύγκρουση πλαισίων. Σε κάθε χρονική στιγμή, επιτρέπεται η κυκλοφορία ενός μόνο πλαισίου σε κάθε collision domain.

Όταν διαπιστωθεί πως κυκλοφορούν περισσότερα του ενός πλαίσια, δηλαδή δυο τουλάχιστον κόμβοι μεταδίδουν ταυτόχρονα, τα πλαίσια συγκρούονται και κατά συνέπεια απορρίπτονται

Το Επίπεδο Πρόσβασης Δικτύου: Ανίχνευση και διόρθωση σφαλμάτων

Ένα σημαντικό πρόβλημα στο επίπεδο ζεύξης είναι οι αλλοιώσεις που μπορεί να προκύψουν κατά τη μεταφορά των πλαισίων μέσω των γραμμών επικοινωνίας.

Για την ανίχνευση των αλλοιώσεων αυτών, χρησιμοποιούνται τεχνικές ανίχνευσης όπως:

- Έλεγχος ισοτιμίας.
- Κυκλικός έλεγχος πλεονασμού (CRC).

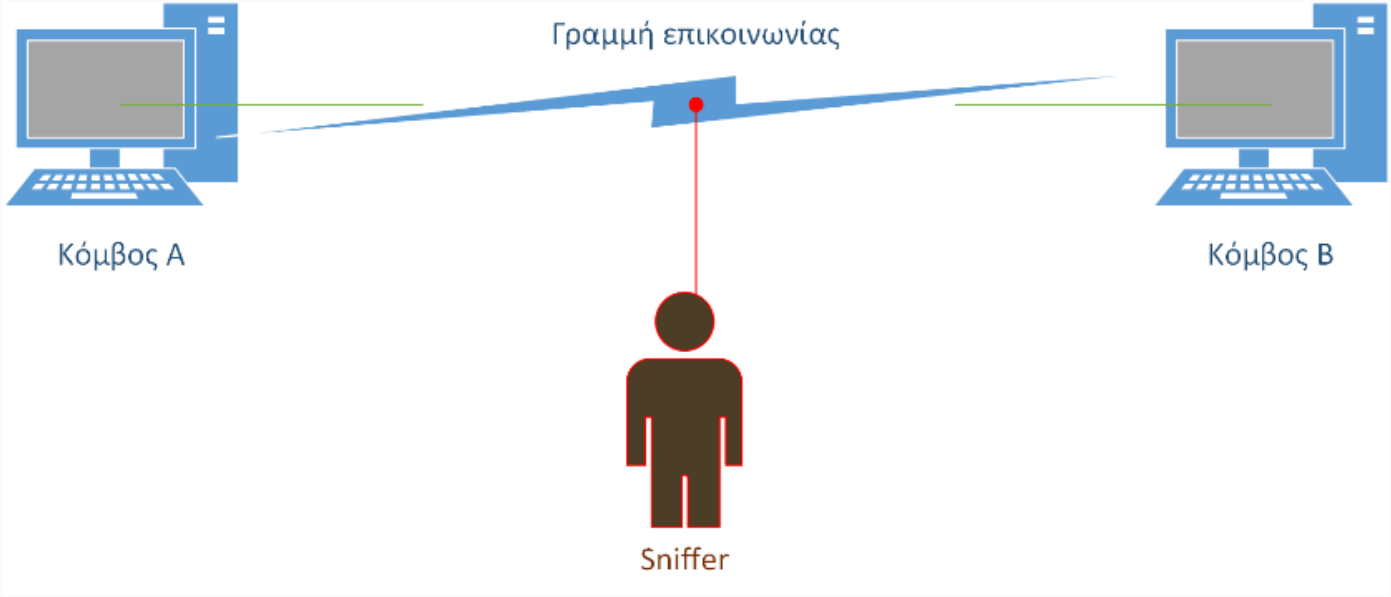
Το Επίπεδο Πρόσβασης Δικτύου: Δημιουργία κύκλων

Η δημιουργία κύκλων σε ένα δίκτυο προκύπτει όταν ένας κόμβος προορισμού είναι προσβάσιμος από διαφορετικά μονοπάτια. Σε μια τέτοια περίπτωση, τα πλαίσια εκπομπής (broadcast) ταξιδεύουν συνεχώς στο δίκτυο.

Για την αντιμετώπιση του φαινομένου αυτού, έχει εισαχθεί το πρωτόκολλο STP (Spanning Tree Protocol), το οποίο με κάθε νέα σύνδεση δημιουργεί εκ νέου ένα δέντρο επικάλυψης (spanning tree) με κόμβους-γράφου τους κόμβους του δικτύου.

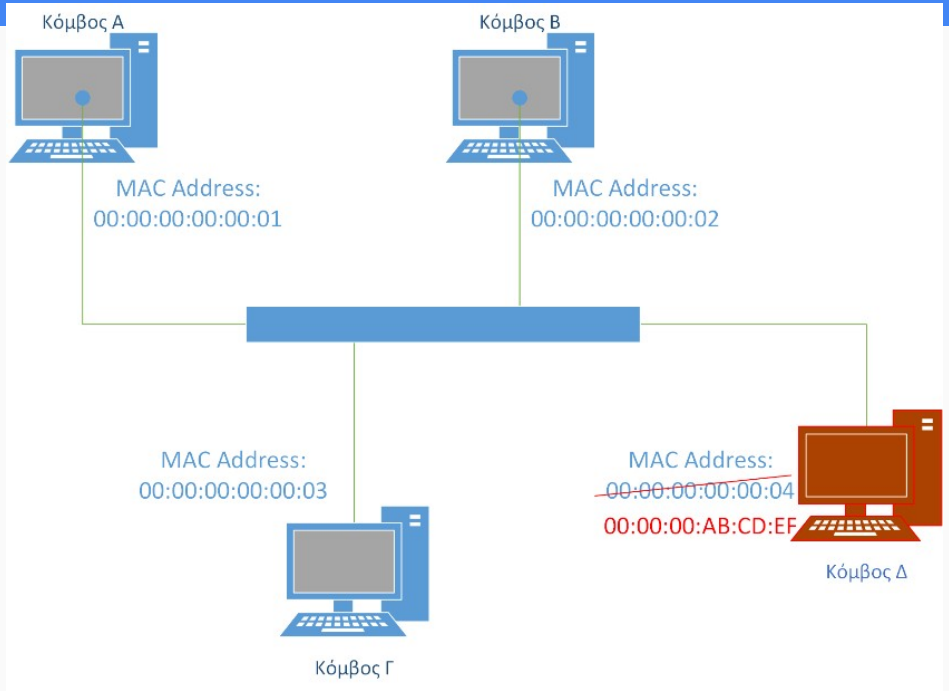
Το Επίπεδο Πρόσβασης Δικτύου: Επιθέσεις επιπέδου ζεύξης

1. Sniffing



Το Επίπεδο Πρόσβασης Δικτύου: Επιθέσεις επιπέδου ζεύξης

2. MAC Spoofing



Το Επίπεδο Δικτύου

Το επίπεδο δικτύου είναι αυτό στο οποίο λαμβάνει χώρα η προώθηση των πακέτων δεδομένων (δεδομενογραμμάτων – datagrams) μεταξύ των δικτύων, στη βάση των κανόνων δρομολόγησης (routing).

Στο επίπεδο αυτό, υπάρχουν πρωτόκολλα δρομολόγησης, πρωτόκολλα ελέγχου, καθώς και το βασικό πρωτόκολλο που καθορίζει την προώθηση και διευθυνσιοδότηση, το Internet Protocol (IP).

Σήμερα, στο μεγαλύτερο μέρος του Internet χρησιμοποιείται παραδοσιακά η έκδοση 4 του πρωτοκόλλου (IPv4). Λόγω των περιορισμών της, όμως, υπάρχει η ανάγκη αντικατάστασής της από την πιο πρόσφατη έκδοση 6 (IPv6).

Το Επίπεδο Δικτύου:
IPv4

Η τέταρτη έκδοση του πρωτοκόλλου IP είναι αυτή που χρησιμοποιείται τις τελευταίες δεκαετίες.
Στην έκδοση αυτή, κάθε διεύθυνση αποτελείται από 32 bit, τα οποία μπορούν να χωριστούν σε τέσσερις ομάδες, των οκτώ (8) bit (1 Byte). Ένα τμήμα αυτών των 32 bit προσδιορίζει το δίκτυο (τμήμα δικτύου) και το υπόλοιπο προσδιορίζει μοναδικά την κάθε υπολογιστική συσκευή (τμήμα κόμβων). Για ευκολία απομνημόνευσης, καθώς ο άνθρωπος είναι εξοικειωμένος με το δεκαδικό σύστημα αρίθμησης, μια διεύθυνση IP μπορεί να γραφεί ως μια ακολουθία από τέσσερις δεκαδικούς αριθμούς (που προκύπτουν από τα τέσσερα Byte της διεύθυνσης), που ξεχωρίζουν μεταξύ τους με χρήση της τελείας.

Το Επίπεδο Δικτύου:
IPv6

Παρά τη χρήση των τεχνικών subnetting και NAT/PAT στο διαδίκτυο με πρωτόκολλο IPv4, ο διαθέσιμος χώρος διευθύνσεων παρέμεινε αισθητά περιορισμένος. Ακόμη και αν είχαμε στη διάθεσή μας το σύνολο των διαθέσιμων διευθύνσεων, αυτές θα ήταν μόλις 232= 4.294.967.296 (λίγο πάνω από 4 δισεκατομμύρια), που έχει αποδειχθεί ότι είναι πολύ λίγες σε σχέση με τις τρέχουσες ανάγκες.

Για παράδειγμα, είναι απαγορευτικές για σκέψεις υλοποίησης τεχνολογιών όπως το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT).

Το Επίπεδο Δικτύου: Δρομολόγηση

Με τον όρο δρομολόγηση (routing), αναφερόμαστε στο σχεδιασμό των διαδρομών κίνησης των πακέτων, καθώς και στη δημιουργία των σχετικών πινάκων δρομολόγησης, στη βάση των οποίων οι δρομολογητές θα μπορούν να παίρνουν αποφάσεις προώθησης μέσω της κατάλληλης διεπαφής.

Η δρομολόγηση μπορεί να είναι στατική ή δυναμική

Το Επίπεδο Δικτύου:
ICMP

Το Internet Control Messaging Protocol (ICMP) είναι ένα πρωτόκολλο ελέγχου που χρησιμοποιείται από το πρωτόκολλο IP με σκοπό τη μεταφορά μηνυμάτων ελέγχου, λαθών και πληροφοριών κατάστασης.

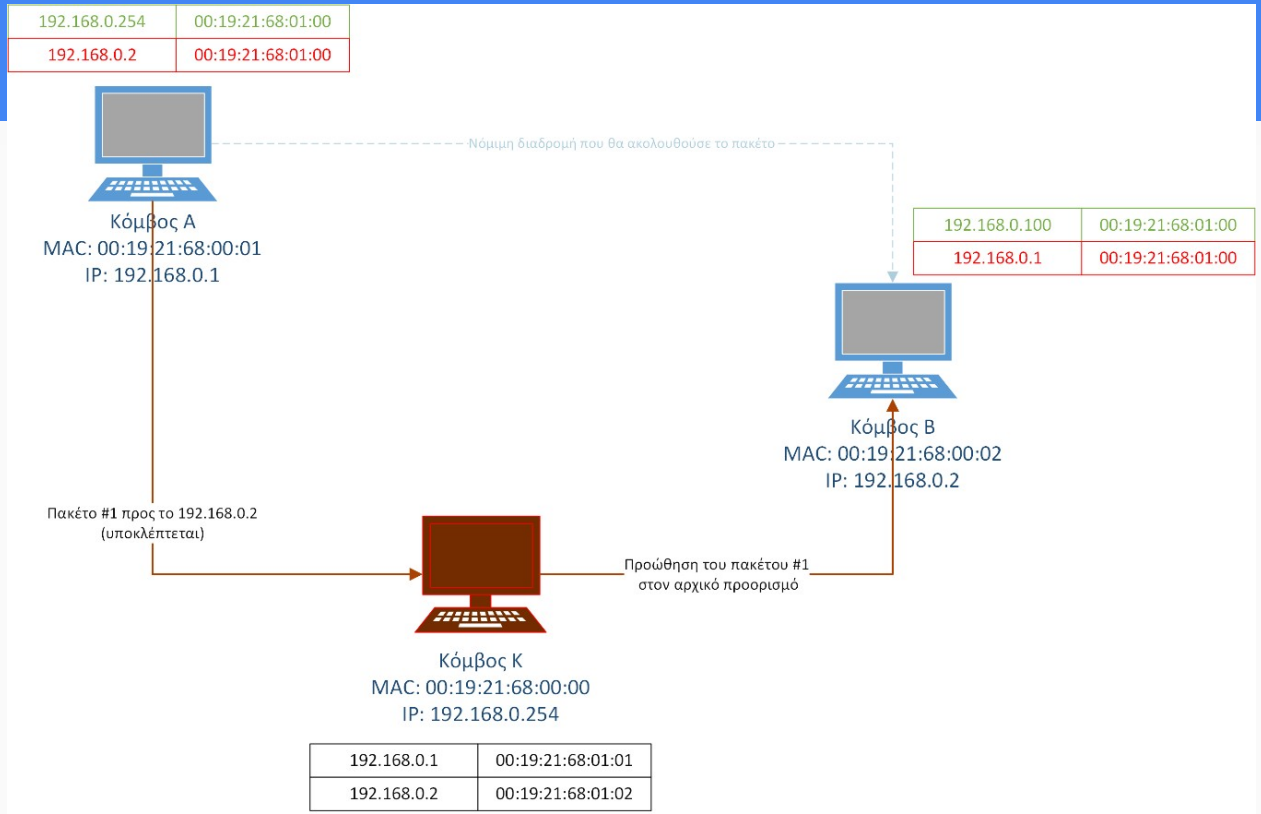
Το ICMP χρησιμοποιείται από το IPv4 και σε νεότερη μορφή του (ICMP6) από το IPv6. Υλοποιείται με μικρού μεγέθους μηνύματα που προσδιορίζονται με συγκεκριμένο κωδικό τύπου (type). Η πιο συχνή χρήση του ICMP είναι το μήνυμα αιτήματος echo request (ICMP type 8), το οποίο απαντάται με μήνυμα απόκρισης ICMP echo reply (type 0) από τον απέναντι host εφόσον υπάρχει και επιθυμεί να κάνει αισθητή την παρουσία του.

Το Επίπεδο Δικτύου: ARP

Αναφέρθηκε, νωρίτερα, πως κάθε επίπεδο του Μοντέλου του Διαδικτύου παρέχει υπηρεσίες στο αμέσως επόμενο, ενθυλακώνοντας την πληροφορία που λαμβάνει από το αμέσως προηγούμενο. Άρα, όταν ένα πακέτο πρέπει να ταξιδέψει από τον κόμβο Α στον κόμβο Β (έχοντας ως διεύθυνση προέλευσης την IP διεύθυνση του κόμβου Α και ως διεύθυνση προορισμού την IP διεύθυνση του κόμβου Β) θα ενθυλακωθεί σε πλαίσια με διεύθυνση προέλευσης τη διεύθυνση MAC της διεπαφής (NIC) του κόμβου Α και διεύθυνση προορισμού τη διεύθυνση MAC της διεπαφής του κόμβου Β.

Από τα παραπάνω, προκύπτει πως θα πρέπει να υπάρχει μια αντιστοίχιση μεταξύ των IP διευθύνσεων των κόμβων και των διευθύνσεων MAC των διεπαφών τους. Για να δημιουργηθεί κα να τηρηθεί η αντιστοίχιση αυτή, ενημερώνονται πίνακες στους οποίους μια διεύθυνση IP αντιστοιχίζεται με μια διεύθυνση MAC. Οι πίνακες αυτοί ονομάζονται πίνακες ARP και το πρωτόκολλο που καθορίζει τον τρόπο δημιουργίας και διαχείρισής τους ονομάζεται Address Resolution Protocol (ARP). Το πρωτόκολλο ARP περιγράφεται στο RFC 826.

Το Επίπεδο Δικτύου: ARP

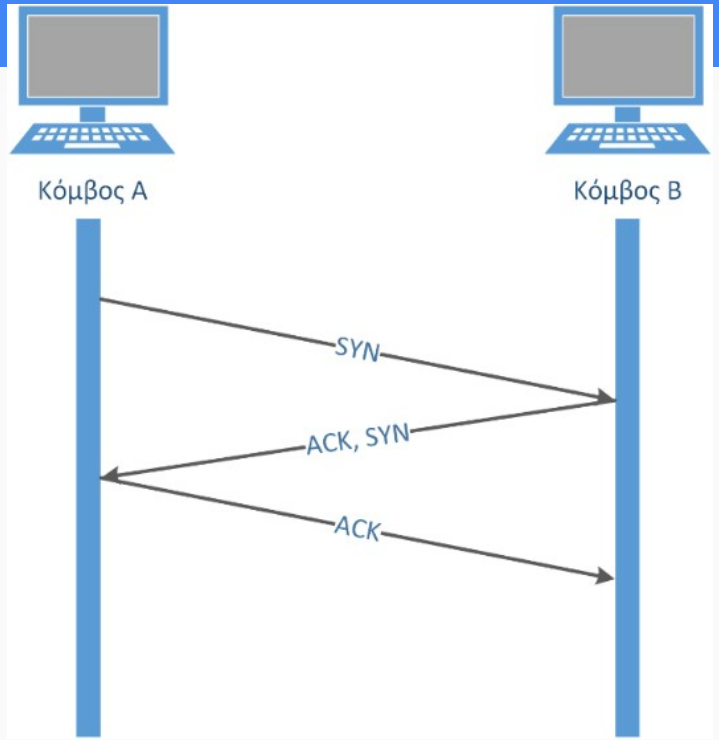


Το επίπεδο Μεταφοράς

Στο επίπεδο δικτύου, λαμβάνεται μέριμνα για τη διασύνδεση δυο κόμβων δικτύου, έστω Α και Β. Το επόμενο επίπεδο, το επίπεδο μεταφοράς, υλοποιείται από πρωτόκολλα τα οποία αναλαμβάνουν την επικοινωνία μεταξύ δυο εργασιών των κόμβων Α και Β, μέσω μιας διαδικασίας πολύπλεξης – αποπολύπλεξης με χρήση των 65535 διαθέσιμων θυρών. Συγκεκριμένα, κάθε διεργασία χρησιμοποιεί μια θύρα για να δημιουργήσει μια σύνδεση και να στείλει ή να λάβει δεδομένα. Ο συνδυασμός διεύθυνσης IP και αριθμού πόρτας (port) ονομάζεται socket.

Στο επίπεδο μεταφοράς συναντάμε δυο βασικά πρωτόκολλα. Το User Datagram Protocol (UDP) και το Transport Control Protocol (TCP).

Το επίπεδο Μεταφοράς: Το πρωτόκολλο TCP



Το πρωτόκολλο TCP, που περιγράφεται στο RFC793, είναι ένα προσανατολισμένο στη σύνδεση (connection oriented) πρωτόκολλο, δηλαδή απαιτείται αρχικά η εδραίωση μιας σύνδεσης μετά από μια διαδικασία τρίδρομης χειραψίας (three-way handshake).

Το επίπεδο Μεταφοράς:
Το πρωτόκολλο UDP

Το πρωτόκολλο UDP, που περιγράφεται από το RFC 7683, είναι, σε αντίθεση με το TCP, ένα πρωτόκολλο ασυνδεσμικής (connectionless) μεταφοράς. Αυτό σημαίνει ότι δεν απαιτείται η εδραίωση σύνδεσης πριν την αποστολή δεδομένων, ενώ δεν παρέχεται κάποιος μηχανισμός αξιόπιστης μεταφοράς ή ελέγχου ροής.
Το πρωτόκολλο UDP είναι ουσιαστικά ένα best effort πρωτόκολλο με μοναδικό (προαιρετικό) έλεγχο το άθροισμα ελέγχου.

Το επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής είναι αυτό στο οποίο, για παράδειγμα, εκτελούνται οι διαδικτυακές εφαρμογές που χρησιμοποιούμε καθημερινά. Υπηρεσίες, όπως ο παγκόσμιος ιστός, η ηλεκτρονική αλληλογραφία, η ονοματοδοσία και πολλές ακόμη άλλες, χρησιμοποιούν για τη λειτουργία τους πρωτόκολλα του επιπέδου εφαρμογής.

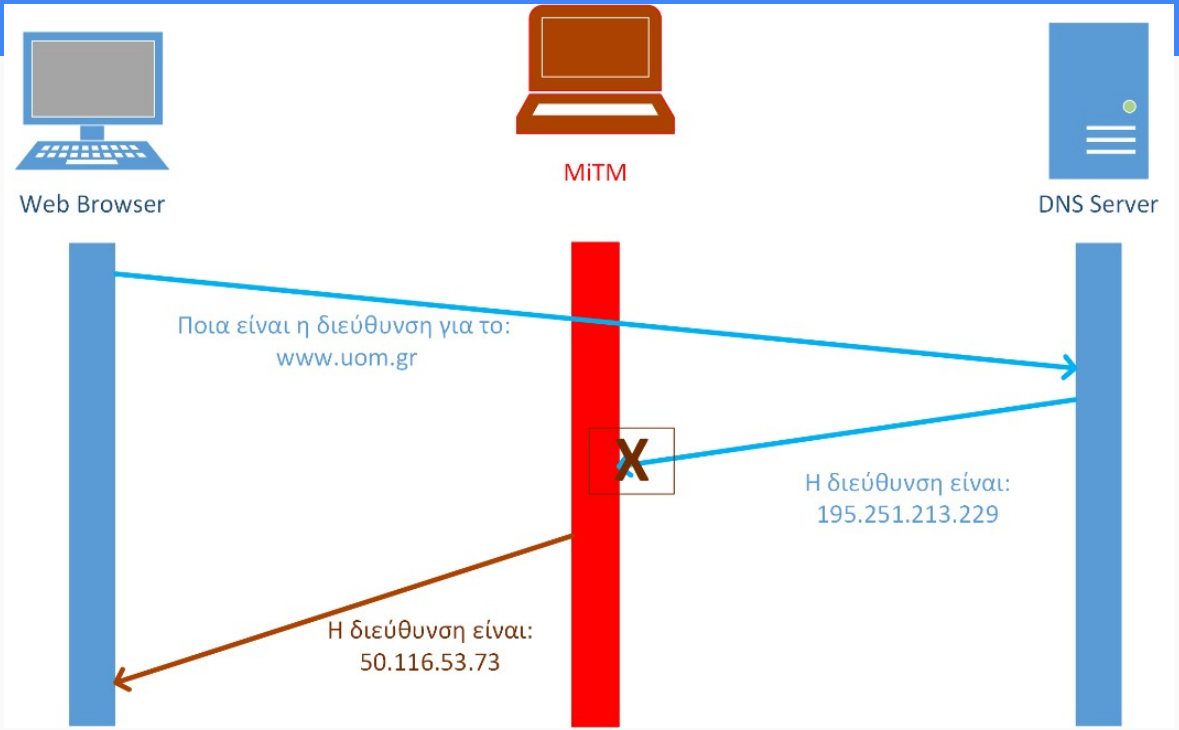
Στο επίπεδο εφαρμογής, ιδιαίτερο ρόλο επιτελεί ο ανθρώπινος παράγοντας, είτε με το ρόλο του κατασκευαστή είτε με το ρόλο του χρήστη. Σε πολλές περιπτώσεις, εντοπίζονται ευπάθειες προερχόμενες από αστοχίες και παραλείψεις κατά την ανάπτυξη των διαδικτυακών εφαρμογών (Web applications), οι οποίες συνήθως διορθώνονται με αναβαθμίσεις (ενημερώσεις) του λογισμικού εφαρμογών ή/και του λογισμικού συστήματος.

Το επίπεδο Εφαρμογής

Τρία βασικά πρωτόκολλα του επιπέδου εφαρμογής:

- Το DNS, που έχει θεμελιώδη σημασία στον κόσμο του Internet, καθώς αποτελεί τον απαραίτητο «τηλεφωνικό κατάλογό» του.
- Το SMTP, που είναι το βασικό στοιχείο λειτουργίας του e-mail («ταχυδρομείου» στο Internet).
- Το HTTP, το οποίο είναι το πιο συχνά χρησιμοποιούμενο από τις διαδικτυακές εφαρμογές πρωτόκολλο.

Το επίπεδο Εφαρμογής:
Επιθέσεις επιπέδου εφαρμογής



Packet Interception

Το επίπεδο Εφαρμογής:
Επιθέσεις επιπέδου εφαρμογής

Betrayal by Trusted Server

Ουσιαστικά, αποτελεί μια επίθεση ενδιάμεσου (man-in-the-middle), με τη διαφορά πως ο ενδιάμεσος είναι ένας κανονικός DNS server, ο οποίος θεωρείται έμπιστος από τον επιλύτη (resolver). Πολλές φορές, κατά την αυτόματη απόδοση παραμέτρων δικτύου σε ένα host, ο χρήστης αποδέχεται (πέρα από τη διεύθυνση IP που του αποδίδεται) και παραμέτρους, όπως οι διακομιστές ονοματοδοσίας (DNS servers). Είναι δυνατό, ένας από τους αποδιδόμενους διακομιστές, για κάποιο λόγο, να υποδεικνύει (μέσω των απαντήσεών του) στον επιλύτη σκόπιμα λανθασμένες τοποθεσίες.

Το επίπεδο Εφαρμογής:
Επιθέσεις επιπέδου εφαρμογής

Distributed Denial of Service

Μια κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS) έχει ως σκοπό τον κατακλυσμό ενός εξυπηρετητή από πακέτα με συχνότητα μεγαλύτερη από εκείνη με την οποία ο τελευταίος μπορεί να ανταποκριθεί. Τα πακέτα αυτά είναι συνήθως:

- Πακέτα τύπου ICMP.
- Πακέτα ερωτημάτων (queries).

Σε κάθε περίπτωση, η αναχαίτιση επιθέσεων DDoS είναι εφικτή με χρήση κατάλληλου φιλτραρίσματος πακέτων.

Το επίπεδο Εφαρμογής:
Επιθέσεις επιπέδου εφαρμογής

Cache Poisoning

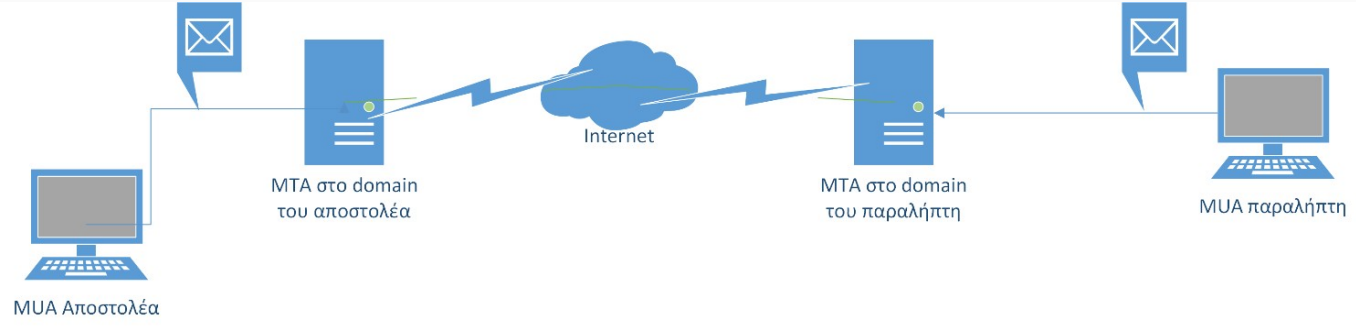
Το σύστημα DNS έχει ιεραρχική δομή οργάνωσης. Έτσι, ο κάθε επιλύτης (resolver) απευθύνει το ερώτημά του σε ένα DNS διακομιστή (server). Εάν ο server αυτός δεν τηρεί αρχείο ζώνης (μια ζώνη αποτελεί ένα τμήμα του χώρου ονομάτων DNS) για το domain του ερωτήματος, θα πρέπει να απευθύνει το ερώτημα σε ένα server που βρίσκεται υψηλότερα στην ιεραρχία. Όταν τελικά λάβει απάντηση, πέρα από το να την προωθήσει στον επιλύτη, την αποθηκεύει σε μια μνήμη (cache), έτσι ώστε αν ερωτηθεί ξανά στο μέλλον, να μπορεί να απαντήσει άμεσα.

Το επίπεδο Εφαρμογής:
Το πρωτόκολλο HTTP

Το HTTP είναι το πρωτόκολλο πάνω στο οποίο βασίζεται η λειτουργία του World Wide Web (WWW). Είναι ένα stateless πρωτόκολλο που χρησιμοποιεί το πρωτόκολλο μεταφοράς TCP. Ο όρος stateless αφορά τη λειτουργία του πρωτοκόλλου και συγκεκριμένα ότι χειρίζεται κάθε δοσοληψία (transaction) ξεχωριστά. Έτσι, μια σύνοδος ξεκινά με ένα αίτημα από τον πελάτη προς το διακομιστή και τερματίζεται με την απάντηση από το διακομιστή προς τον πελάτη. Η απάντηση περιλαμβάνει ένα ή περισσότερα αντικείμενα, χωρίς να τηρούνται κάπου πληροφορίες συνόδου.

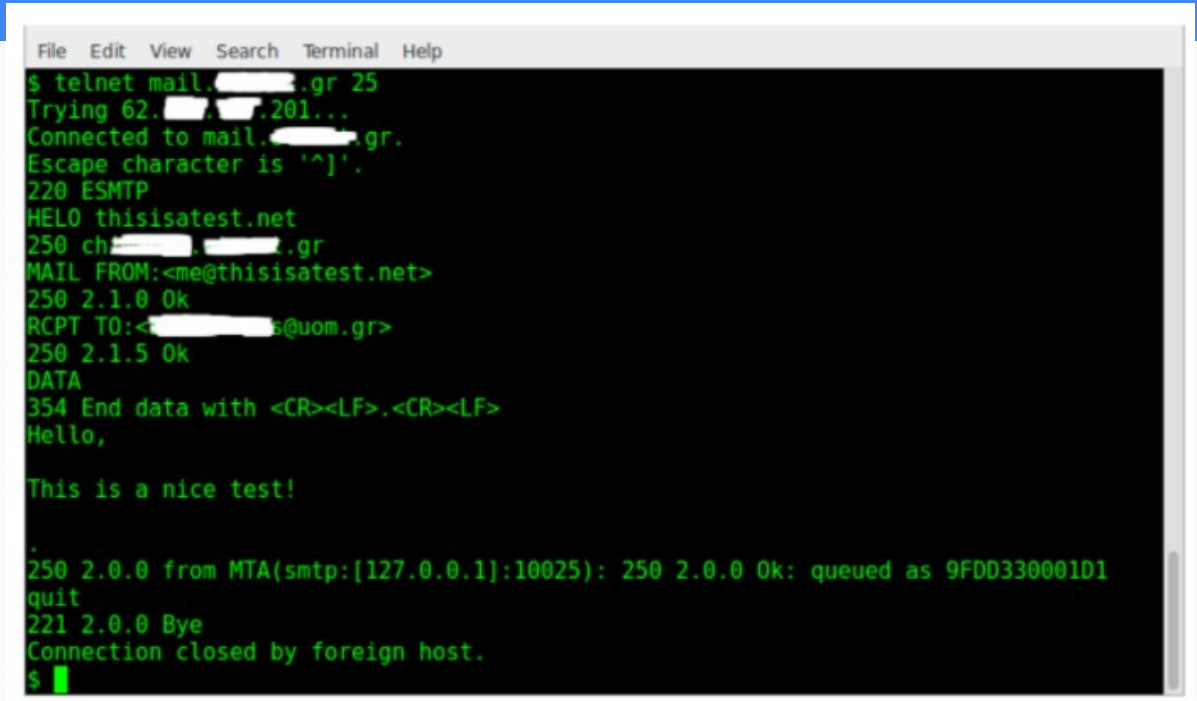
Το επίπεδο Εφαρμογής: Ηλεκτρονική αλληλογραφία

Η ηλεκτρονική αλληλογραφία ή ηλεκτρονικό ταχυδρομείο (e-mail) είναι μια από τις δημοφιλέστερες υπηρεσίες του Internet. Η υπηρεσία αυτή βασίζεται στο πρωτόκολλο SMTP (Simple Mail Transfer Protocol), το οποίο περιγράφεται στο RFC 2821 και είναι ένα από τα παλιότερα πρωτόκολλα του Internet (εμφανίστηκε πολύ πριν το HTTP).



Το επίπεδο Εφαρμογής: Ηλεκτρονική αλληλογραφία

Για την επικοινωνία του MUA του αποστολέα με τον MTA και την παράδοση μηνύματος προς αποστολή, ο MUA χρησιμοποιεί SMTP commands.



Το επίπεδο Εφαρμογής: Ηλεκτρονική αλληλογραφία

Παρατηρούμε ότι η αλληλογραφία μεταφέρεται ως απλό κείμενο (plaintext), δηλαδή χωρίς κρυπτογράφηση. Το SMTP έχει σχεδιαστεί για να μεταφέρει δεδομένα ASCII 7-bit. Σήμερα, μπορούμε να παρατηρήσουμε, ότι μέσω ηλεκτρονικού ταχυδρομείου μεταφέρονται αρχεία εικόνας, ήχου, λογιστικά φύλλα κοκ. Θα αναρωτηθεί κανείς, πώς γίνεται να χρησιμοποιείται για τη μεταφορά δεδομένων διαφόρων μορφότυπων ένα πρωτόκολλο σχεδιασμένο να μεταφέρει ASCII κείμενο; Ο τρόπος με τον οποίο γίνεται αυτό, είναι η μετατροπή όλων των δεδομένων σε μορφή ASCII, κάτι που επιτυγχάνεται με τη χρήση της
κωδικοποίησης Base64.

Άρα, μπορούμε να εντοπίσουμε δυο σημαντικά ζητήματα για την ασφάλεια:

- Δεν υπάρχει έλεγχος της ταυτότητας αποστολέα.
- Τα μηνύματα μεταφέρονται ως απλό κείμενο (plaintext).

Συστήματα Διάχυτου Υπολογισμού

Η ανάπτυξη των δικτύων και κυρίως της ασύρματης δικτύωσης, έχει δώσει σάρκα και οστά στο όραμα του Mark Weiser, ο οποίος πρώτος είχε εισάγει τον όρο της απανταχού παρούσας ή διάχυτης υπολογιστικής (ubiquitous / pervasive computing).

Με τον όρο αυτό, αναφερόμαστε στη διασπορά διασυνδεδεμένων υπολογιστικών συστημάτων στο φυσικό χώρο, χωρίς αυτά να γίνονται ενοχλητικά ή άμεσα αντιληπτά από τους χρήστες με τους οποίους αλληλεπιδρούν.

Η ανάπτυξη των υποδομών στις επικοινωνίες, έχει δώσει τεράστια ώθηση στο διάχυτο υπολογισμό.