ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΜΣ: "Προηγμένα Τηλεπικοινωνιακά Συστήματα και Δίκτυα"

Μάθημα: Ασφάλεια Τηλεπικοινωνιακών Συστημάτων
Κωδικός DIT 114

ΣΤΑΥΡΟΣ Ν. ΝΙΚΟΛΟΠΟΥΛΟΣ

Ηλεκτρολόγος Μηχανικός και Μηχανικός Η/Υ ΕΜΠ

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Η/Υ ΕΜΠ

Μεταδιδακτορικός Υπότροφος Université Pierre et Marie CURIE (UPMC)-FRANCE

ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΕΝΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ
Τηλεφωνικό δίκτυο
Οπτικές Ίνες
Καλωδιακή Τηλεόραση
Δομημένη καλωδίωση
Σηματοδοσία
Δίκτυο Πόλης

ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ
Ασύρματες ζεύξεις (radio links)
Ασύρματη τηλεφωνία
Κινητή Τηλεφωνία
TETRA
Ραδιοφωνία - Τηλεόραση

ΔΟΡΥΦΟΡΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ
Τηλεφωνία
Ραδιοφωνία – Τηλεόραση
Σηματοδοσία
Δίκτυα Επικοινωνιών
GPS
Γαλιλαίος

ΔΙΑΔΙΚΤΥΟ
VoIP
oIP

ΑΣΦΑΛΕΙΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

ΑΣΦΑΛΕΙΑ ΛΕΙΤΟΥΡΓΙΑΣ
ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΟΥ
ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΩΝ
ΑΣΦΑΛΕΙΑ ΧΡΗΣΤΩΝ
ΕΝΕΡΓΕΙΑΚΟ ΑΠΟΤΥΠΩΜΑ
ΟΙΚΟΝΟΜΙΚΟ ΑΠΟΤΥΠΩΜΑ

ΕΝΝΟΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΠΛΗΡΟΦΟΡΙΑ: είναι κάθε γνώση η οποία έχει συγκεκριμένη πρακτική χρησιμότητα, έχει αξία και μπορεί να αποδώσει συγκεκριμένο έργο.

Έχει σαφές και υπολογίσιμο οικονομικό αποτύπωμα.

Έχει διάρκεια ζωής

ΠΑΡΑΔΕΙΓΜΑΤΑ

- ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ
- ΔΗΜΟΓΡΑΦΙΚΑ ΔΕΔΟΜΕΝΑ
- ΓΕΩΓΡΑΦΙΚΑ ΔΕΔΟΜΕΝΑ
- ΠΝΕΥΜΑΤΙΚΟ ΕΡΓΟ

ΠΑΡΑΔΕΙΓΜΑΤΑ (2)

- ΕΜΠΕΙΡΙΑ ΘΕΜΑΤΙΚΟΥ ΠΕΔΙΟΥ
- ΤΕΧΝΟΓΝΩΣΙΑ ΘΕΜΑΤΙΚΟΥ ΠΕΔΙΟΥ
- ΕΠΙΣΤΗΜΟΝΙΚΗ ΓΝΩΣΗ – ΕΞΕΙΔΙΚΕΥΣΗ
- ΣΧΕΔΙΑ ΒΙΟΜΗΧΑΝΙΚΩΝ ΠΡΟΤΥΠΩΝ (Blueprints)

ΠΑΡΑΔΕΙΓΜΑΤΑ (3)

- ΜΟΧΛΕΥΣΗ ΤΥΧΕΡΩΝ ΠΑΙΓΝΙΩΝ
- ΜΟΧΛΕΥΣΗ ΟΙΚΟΝΟΜΙΑΣ
- ΤΡΑΠΕΖΙΚΑ ΔΕΔΟΜΕΝΑ
- ΕΤΑΙΡΙΚΑ ΔΕΔΟΜΕΝΑ

ΠΑΡΑΔΕΙΓΜΑΤΑ (4)

- ΣΧΕΔΙΑ ΕΚΤΑΚΤΟΥ ΑΝΑΓΚΗΣ
- ΣΧΕΔΙΑ ΑΣΦΑΛΕΙΑΣ
- ΣΧΕΔΙΑ ΑΜΥΝΑΣ
- ΒΙΟΜΗΧΑΝΙΚΑ ΜΥΣΤΙΚΑ - ΑΠΟΡΡΗΤΑ
- ΚΡΑΤΙΚΑ ΜΥΣΤΙΚΑ - ΑΠΟΡΡΗΤΑ

ΚΑΝΟΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

ΒΙΟΜΗΧΑΝΙΚΑ ΜΥΣΤΙΚΑ – ΑΠΟΡΡΗΤΑ ΕΚΒΑ

ΚΡΑΤΙΚΑ ΜΥΣΤΙΚΑ – ΑΠΟΡΡΗΤΑ ΕΚΑ

ΟΙΚΟΝΟΜΙΚΟ ΑΠΟΤΥΠΩΜΑ

- ΚΟΣΤΟΣ ΑΠΟΚΤΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
- ΚΟΣΤΟΣ ΔΙΑΤΗΡΗΣΗΣ
- ΚΟΣΤΟΣ ΕΠΙΚΑΙΡΟΠΟΙΗΣΗΣ
- ΚΟΣΤΟΣ ΑΠΟΘΗΚΕΥΣΗΣ
- ΚΟΣΤΟΣ ΑΝΑΚΤΗΣΗΣ

ΔΙΑΒΑΘΜΙΣΗ ΠΛΗΡΟΦΟΡΙΑΣ

- ΝΑΤΟΪΚΗ ΔΙΑΒΑΘΜΙΣΗ
- ΕΥΡΩΠΑΪΚΗ ΔΙΑΒΑΘΜΙΣΗ
- ΕΘΝΙΚΗ ΔΙΑΒΑΘΜΙΣΗ
- ΒΙΟΜΗΧΑΝΙΚΗ ΔΙΑΒΑΘΜΙΣΗ
- ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ
- ΔΗΜΟΓΡΑΦΙΚΑ ΔΕΔΟΜΕΝΑ
- ΓΕΩΓΡΑΦΙΚΑ ΔΕΔΟΜΕΝΑ
- ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

ΔΙΑΡΚΕΙΑ ΖΩΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

- ΔΙΑΤΗΡΗΣΗ
- ΕΠΙΚΑΙΡΟΠΟΙΗΣΗ
- ΑΠΟΘΗΚΕΥΣΗ
- ΑΝΑΚΤΗΣΗ
- ΚΑΤΑΣΤΡΟΦΗ
- ΑΣΦΑΛΗΣ ΔΙΑΓΡΑΦΗ
- ΔΙΚΑΙΩΜΑ ΣΤΗ ΛΗΘΗ

ΚΆΘΕ ΠΛΗΡΟΦΟΡΙΑ ΑΠΟΤΕΛΕΙ ΈΝΑ ΣΑΦΩΣ ΚΟΣΤΟΛΟΓΗΜΕΝΟ ΠΕΡΙΟΥΣΙΑΚΟ ΣΤΟΙΧΕΙΟ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

Ασφάλεια πληροφοριών είναι η προστασία των **επεξεργαζόμενων**, **αποθηκευμένων** ή **διαβιβαζομένων** πληροφοριών από μη εξουσιοδοτημένη απόκτηση, επεξεργασία, τροποποίηση και διαγραφή, ή άρνηση εξυπηρέτησης.

Ερώτηση:

Ποιός είναι ο κύριος στόχος της ασφάλειας πληροφοριών σε έναν Οργανισμό;

Απάντηση:

Να βοηθήσει τον Οργανισμό να επιτύχει τους στόχους του

ΠΑΡΑΤΗΡΗΣΗ 1η

- Η ανθρώπινη βλακεία είναι άπειρη*

(* A. Einstein)

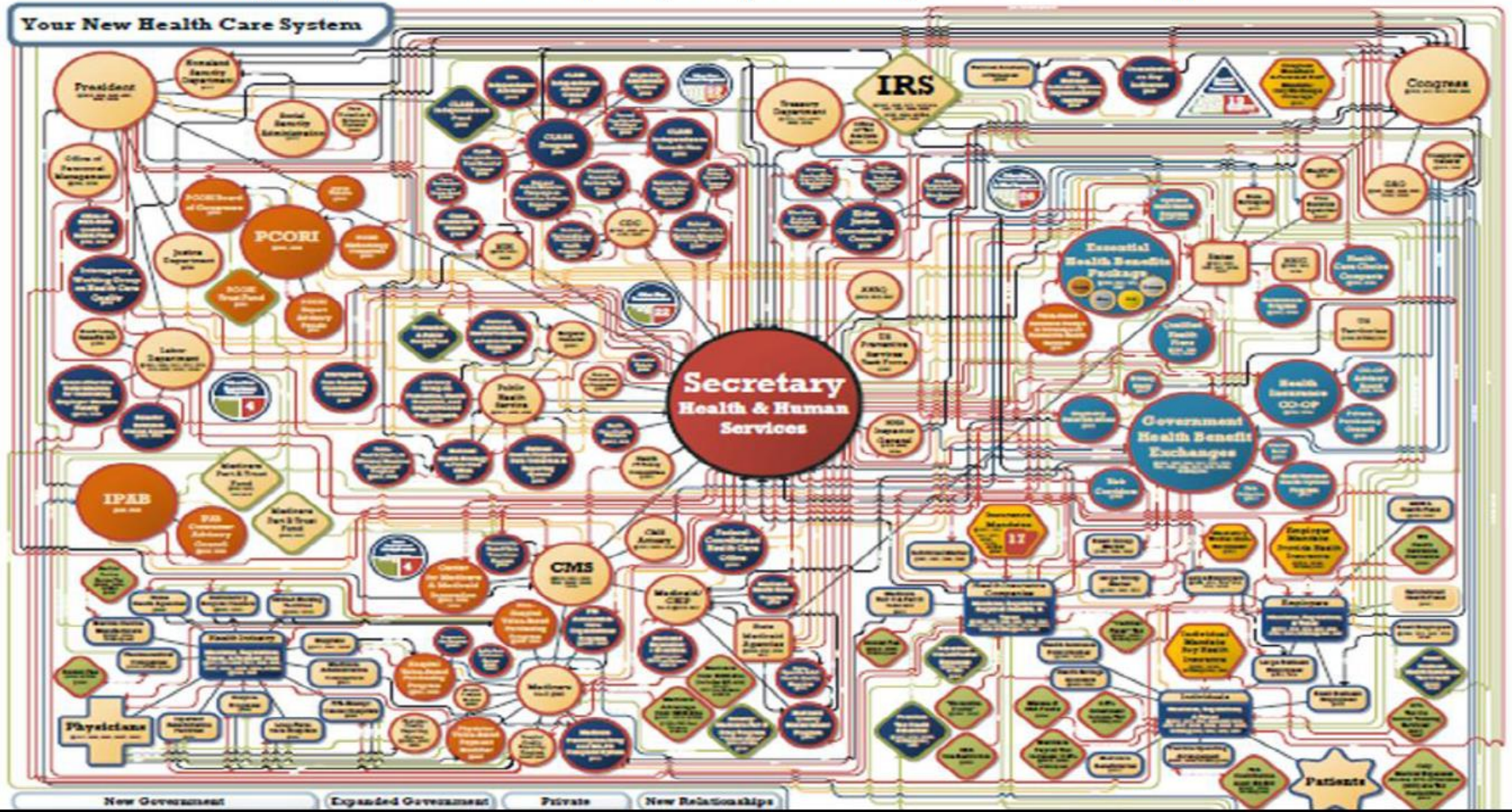
ΒΛΑΚΕΙΑ: Η ενέργεια που βασίζεται κυρίως στον συναισθηματικό αντίκτυπο του περιβάλλοντος παρά στην ορθολογιστική στάθμιση των δεδομένων.

ΝΕΥΡΟΕΠΙΣΤΗΜΗ: Το 95% των ενεργειών μας είναι συναισθηματικές.

ΝΕΥΡΟΕΠΙΣΤΗΜΗ 2: 100% των ενεργειών μας σε πανικό ή πίεση είναι συναισθηματικές.

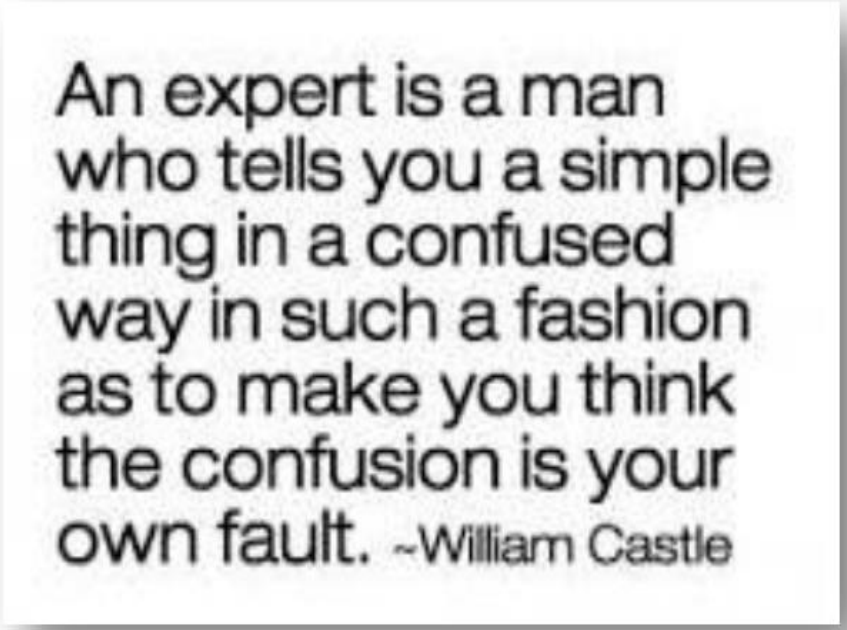
ΠΑΡΑΤΗΡΗΣΗ 2η

- Η πολυπλοκότητα σκοτώνει την ασφάλεια
  - Π.χ. Βρείτε αδυναμίες σε μια υπηρεσία του Δημοσίου



ΠΑΡΑΤΗΡΗΣΗ 3η

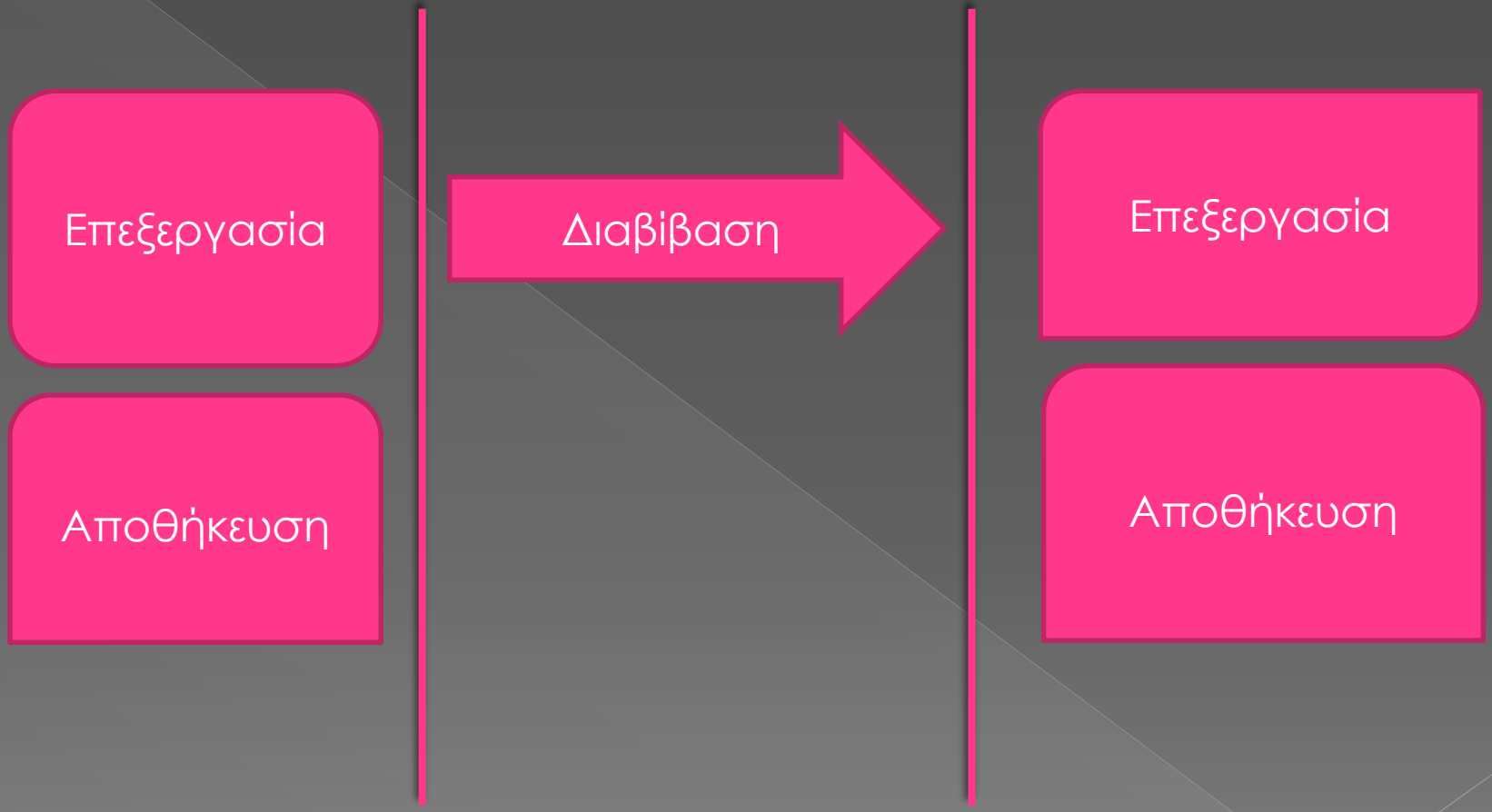
- *ΔΕΝ* υπάρχουν "ειδικοί" στην ασφάλεια πληροφοριών



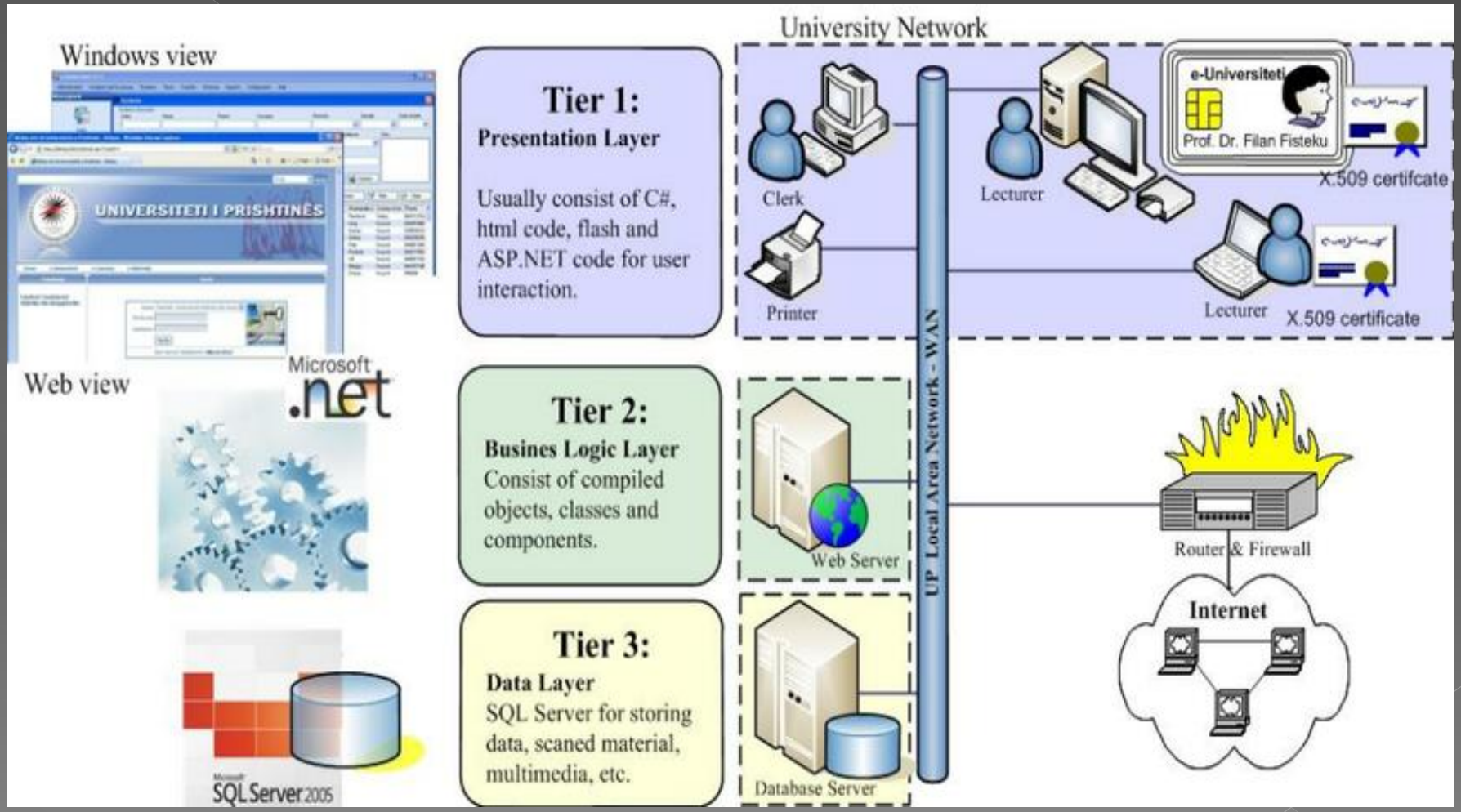
Επικοινωνία Πληροφορίας

- Πληροφοριακό Σύστημα επικοινωνιών
- **Επεξεργασία** (προσαρμογή της πληροφορίας ώστε να είναι διαβιβάσιμη)
- **Αποθήκευση** (της πληροφορίας, μετά-δεδομένων)
- **Διαβίβαση** (της πληροφορίας και των μετά-δεδομένων)

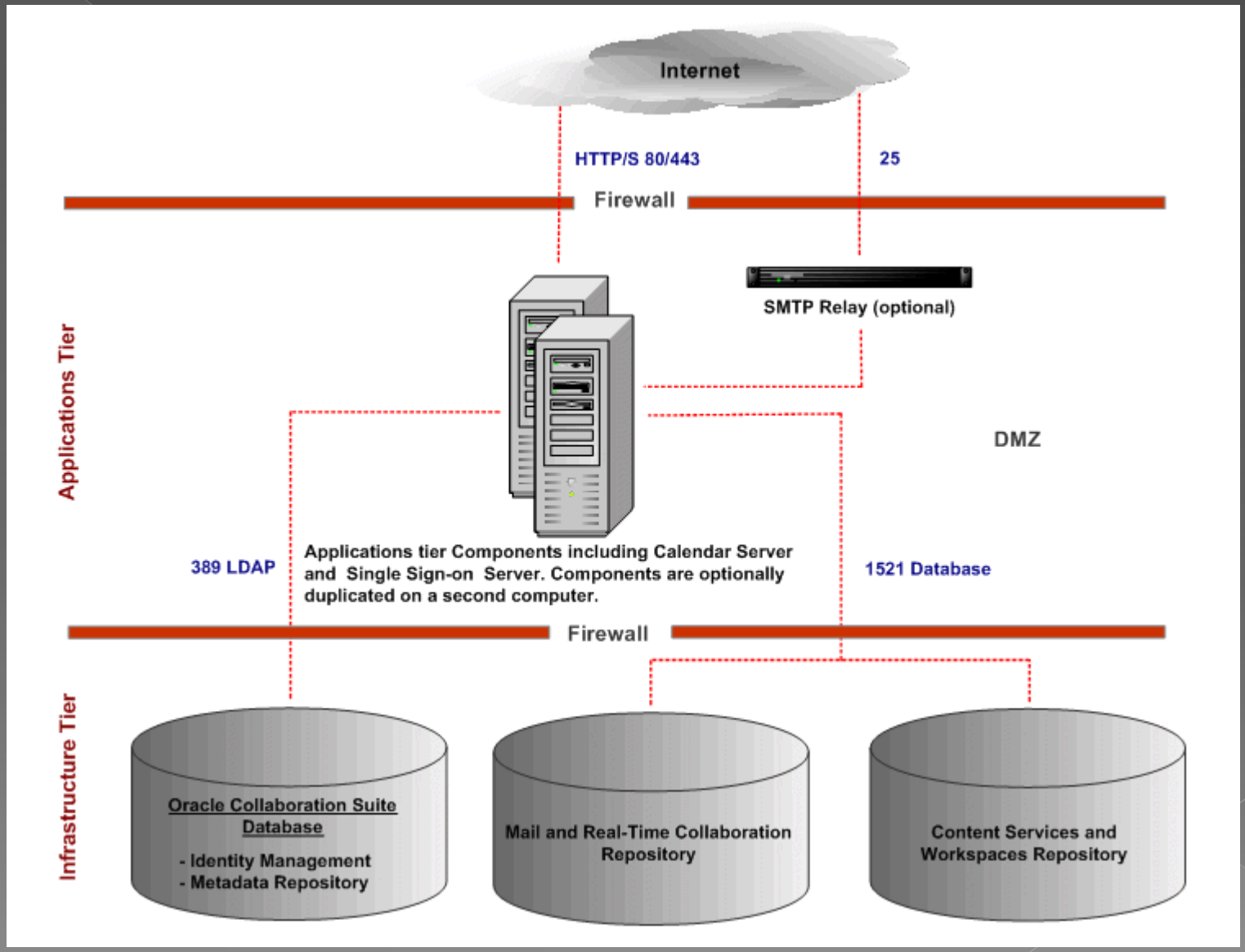
Καθορισμός Ορίων Ευθύνης



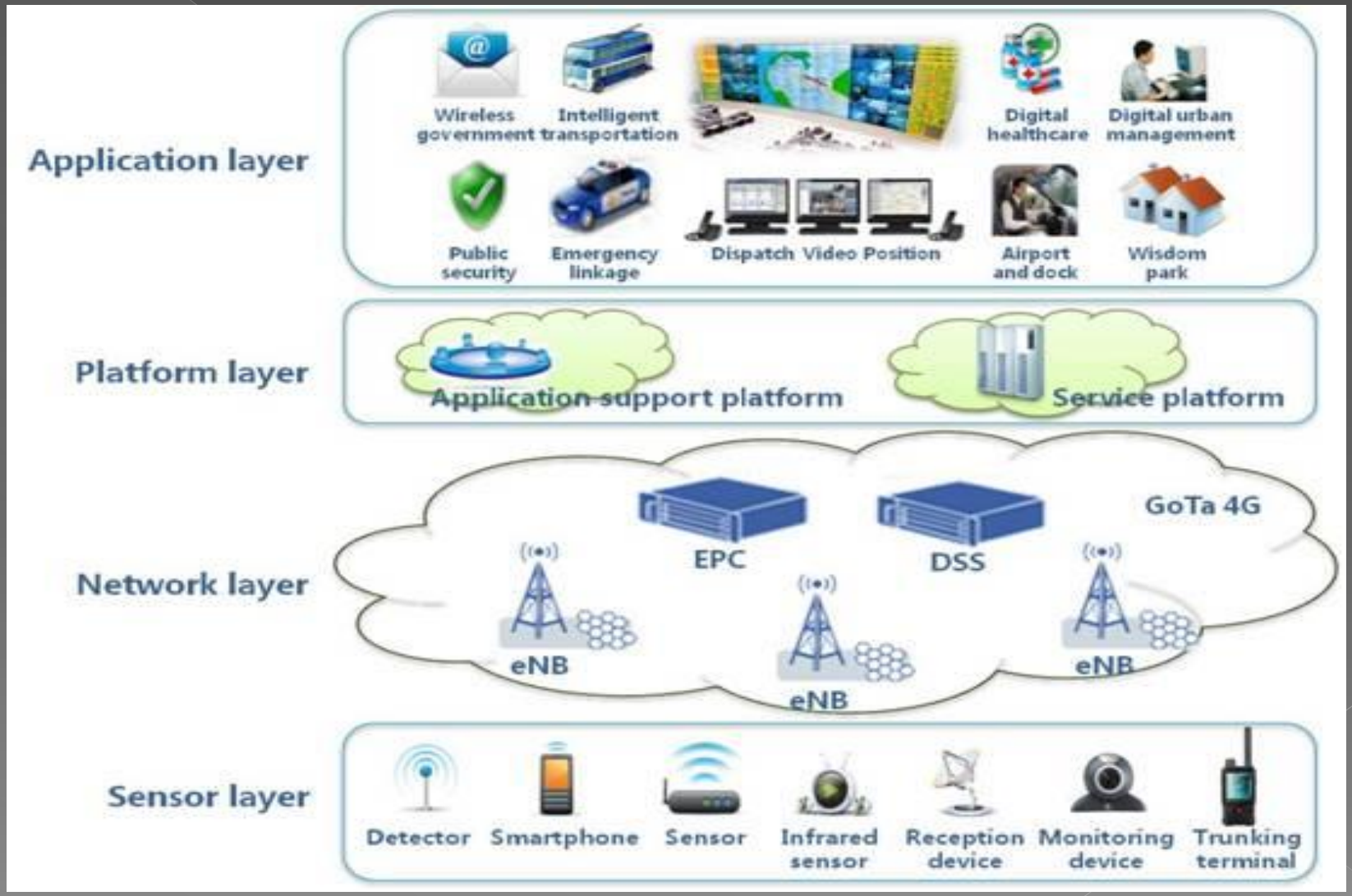
Καθορισμός Ορίων Ευθύνης



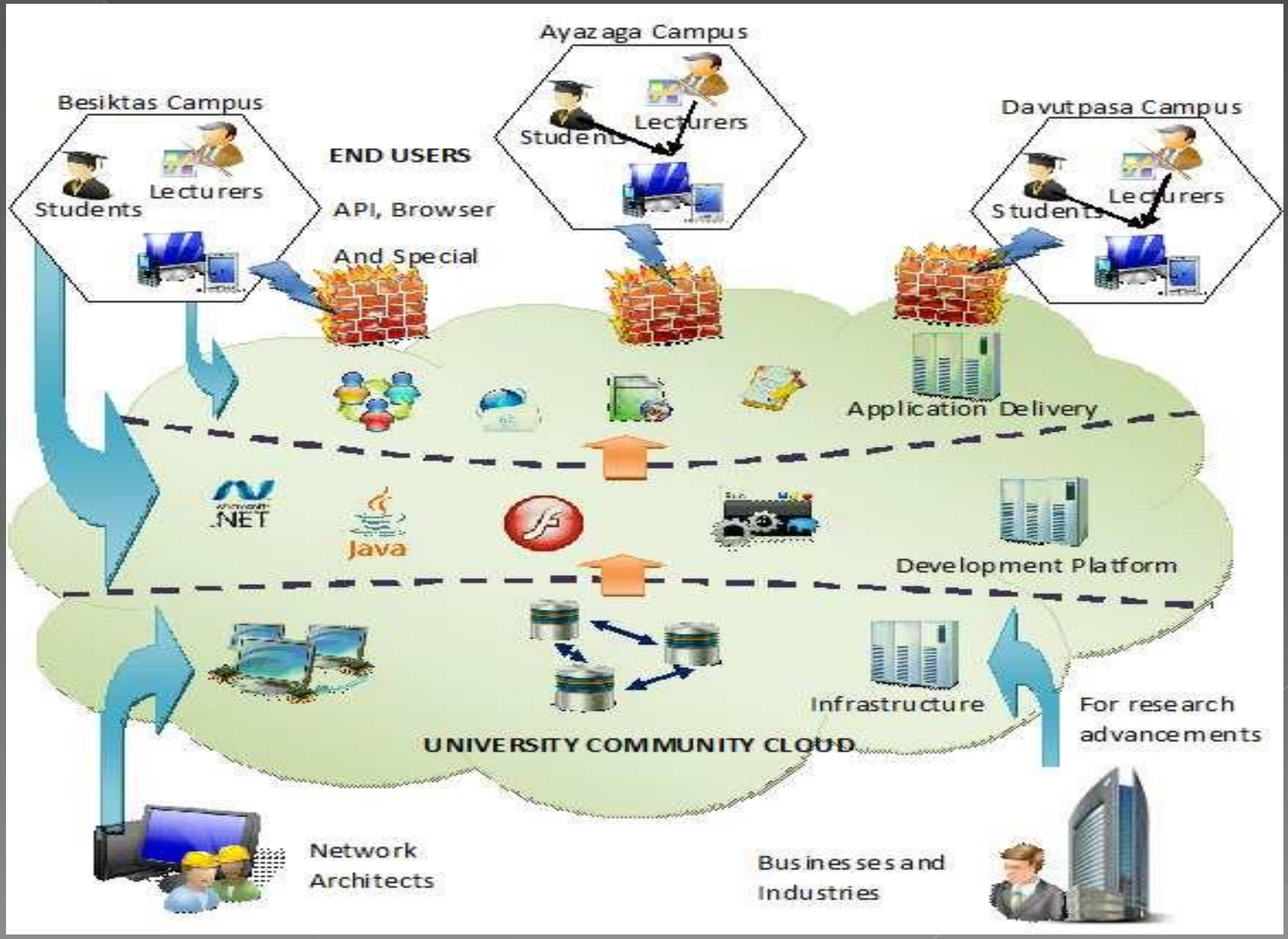
Καθορισμός Ορίων Ευθύνης



Καθορισμός Ορίων Ευθύνης

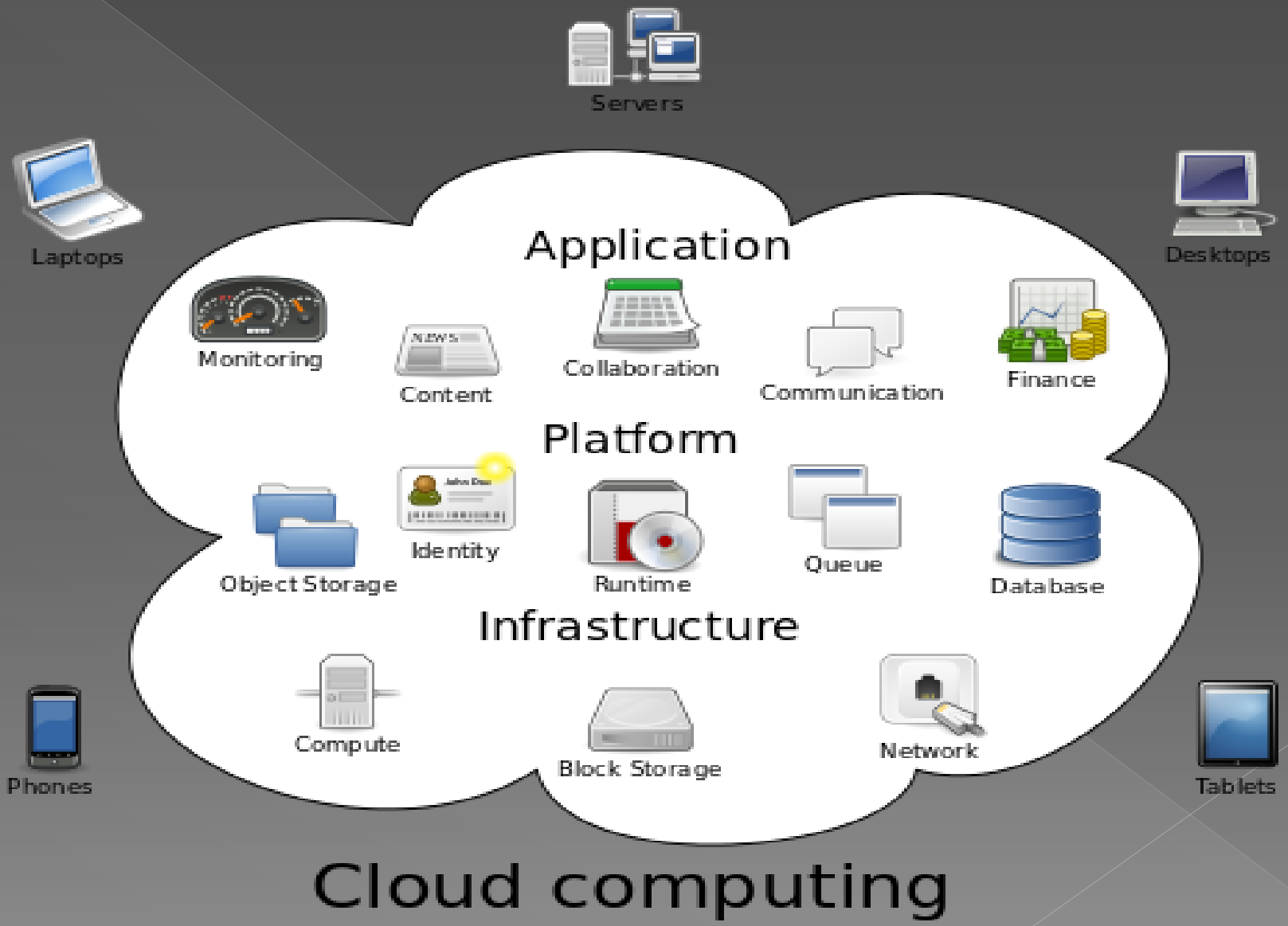


Καθορισμός Ορίων Ευθύνης



Καθορισμός Ορίων Ευθύνης

Καθορισμός Ορίων Ευθύνης



ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

-Εμπιστευτικότητα (Confidentiality)
-Ακεραιότητα (Integrity)
-Αυθεντικότητα (Authentication)
-Διαθεσιμότητα (Availability)
-Μη απάρνηση (Non repudiation)

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

- **Εμπιστευτικότητα (Confidentiality)**
- Προστασία έναντι της διάθεσης ή αποκάλυψης διαβαθμισμένων πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα.
-
- Τεχνικές:
  - Κρυπτογραφία
  - Έλεγχος πρόσβασης
- Η ανίχνευση της παραβίασης της εμπιστευτικότητας είναι σχεδόν αδύνατη στις ψηφιακές επικοινωνίες

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

- Ακεραιότητα (Integrity) :
- Προστασία έναντι της τροποποίησης ή αλλοίωσης των πληροφοριών.

Ακεραιότητα (Integrity) :

- "Αποτροπή μη εξουσιοδοτημένων αλλαγών στα δεδομένα του συστήματος"

- **Τεχνικές**:
  - Κρυπτογραφία (crypto checksums).
  - Κώδικες ανίχνευσης/διόρθωσης σφαλμάτων
  - Διαδικασίες για τη διαχείριση, συντήρηση και λειτουργία του συστήματος.

- Η ανίχνευση της παραβίασης της ακεραιότητας είναι κατά κανόνα εφικτή.

Defacement: avg.com @ 8/10/13

avg.com

Hello World

We Are Here To Deliver Tow Messages

First one:

we want to tell you that there is a land called Palestine on the earth
this land has been stolen by Zionist
do you know it ?
Palestinian people has the right to live in peace
Deserve to liberate their land and release all prisoners from israeli jails
we want peace

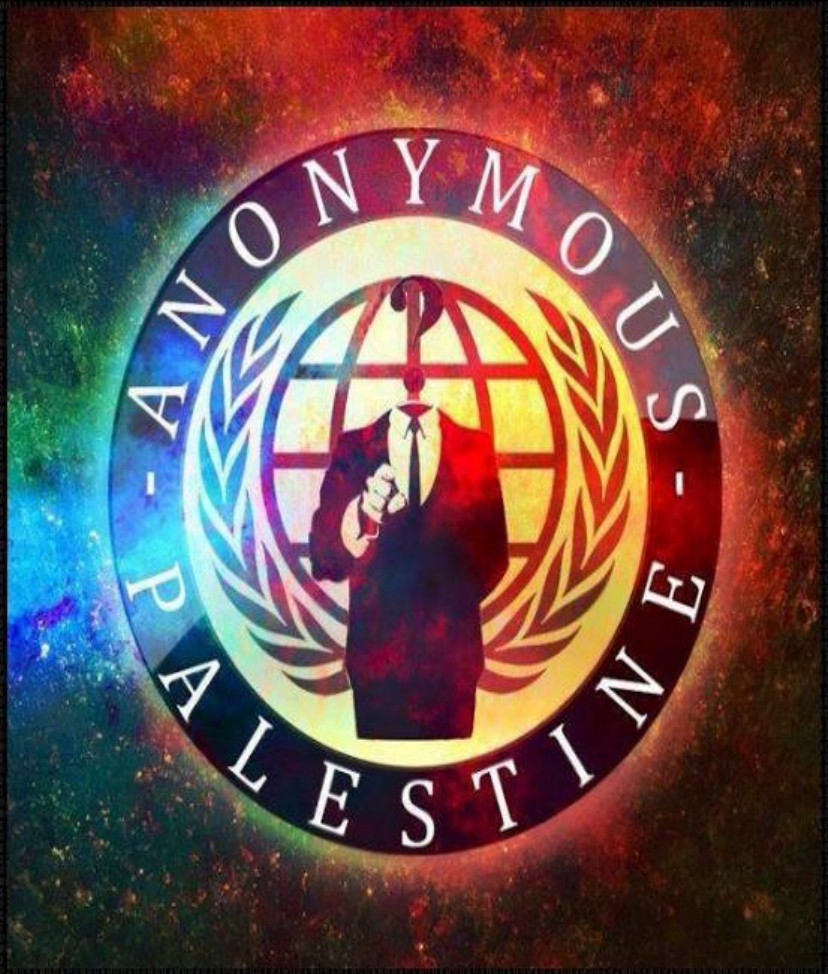
long live Palestine

Defacement: avira.com @ 8/10/13

www.avira.com

Second Message:

There Is No Full Security
We Can Catch You !



ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

- **Αυθεντικότητα (Authentication) :**

- Προστασία έναντι της δημιουργίας παραπλανητικών πληροφοριών καθώς και η εξασφάλιση της αυθεντικότητας των χρηστών

ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ

"Δυνατότητα εξακρίβωσης της αυθεντικότητας μιας **οντότητας**"

- οντότητες: χρήστες, στοιχεία δικτύου, δεδομένα (μηνύματα)

ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ ΧΡΗΣΤΗ

ΤΡΕΙΣ (3) ΠΑΡΑΓΟΝΤΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

- Αυτό που γνωρίζουμε. PIN,passwords,passphrases,etc.
- Αυτό που κατέχουμε. badges, smart cards, tokens.
- Αυτό που είμαστε βιομετρία

τι γνωρίζουμε

Τι κατέχουμε

Τι είμαστε

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Διαθεσιμότητα (Availability) :

Εξασφάλιση της απρόσκοπτης διάθεσης των πληροφοριών.

ΔΙΑΘΕΣΙΜΟΤΗΤΑ

"Εξασφάλιση της πρόσβασης στο σύστημα από εξουσιοδοτημένους χρήστες".

- Τεχνικές:
  - Περίσσεια πόρων (redundancy).
  - Σύστημα ανοχής σφαλμάτων (fault tolerance system design).
  - Κατηγορία επιθέσεων Άρνησης Υπηρεσίας: 'Denial of Service' (DoS).
- Η **υψηλή διαθεσιμότητα** χαρακτηρίζεται από το **υψηλό κόστος**.

Εργαλεία (D)DoS

- Low Orbit Ion Cannon (LOIC)
- High Orbit Ion Cannon (HOIC)
- Slowloris

Slowloris is a piece of software written by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.[

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Μη αποποίηση (Non repudiation) :

Προστασία έναντι της άρνησης χειρισμού (επεξεργασία, διαβίβαση, αποθήκευση) των πληροφοριών. (καταλογισμός ευθυνών)

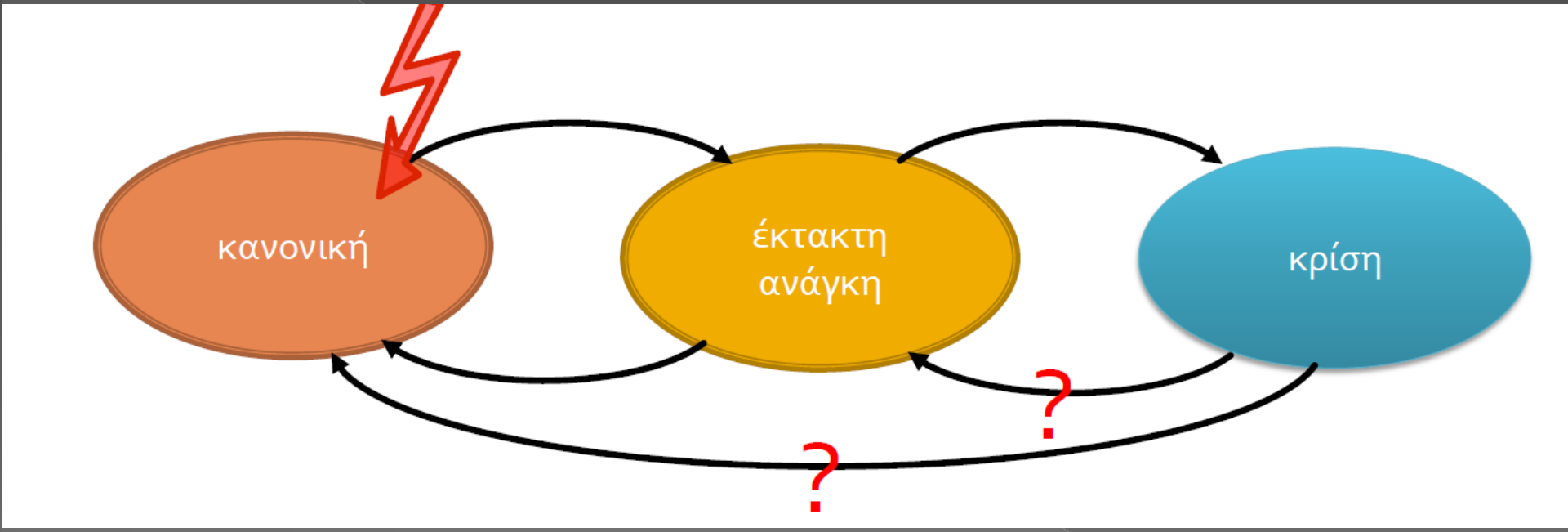
ΜΗ ΑΠΟΠΟΙΗΣΗ

"Δεν είναι δυνατόν ο χρήστης να αρνηθεί εκ των υστέρων κάποια πράξη του"

- Μη αποποίηση **προέλευσης**
  Ο αποστολέας αποδέχεται ότι έστειλε το μήνυμα
- Μη αποποίηση **παράδοσης**
  Ο παραλήπτης αποδέχεται ότι παρέλαβε το μήνυμα

▪**Τεχνικές**
κρυπτογραφία (Υποδομές Δημοσίου Κλειδιού)
Στεγανογραφία (watermarks, μυστική σήμανση αρχείων (ηλεκτρονικών και εντύπων))

ΑΝΑΓΝΩΡΙΣΗ ΤΗΣ ΚΑΤΑΣΤΑΣΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ



- Ανάγκη για εις βάθος άμυνα (Defense In Depth)
- Ει δυνατόν, ελαχιστοποίηση (μεγιστοποίηση) της ανθρώπινης παρέμβασης για Ε.Α. (κρίση)

ΕΜΠΕΙΡΙΑ ΑΝΤΙΛΗΨΗ ΚΑΙ ΛΑΘΟΣ ΕΚΤΙΜΗΣΗ

ΕΜΠΕΙΡΙΑ ΑΝΤΙΛΗΨΗ ΚΑΙ ΛΑΘΟΣ ΕΚΤΙΜΗΣΗ