ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Διαχείριση Ασφαλείας (Ι)

Απειλές Ασφαλείας

Συμμετρική & Μη-Συμμετρική Κρυπτογραφία

Β. Μάγκλαρης

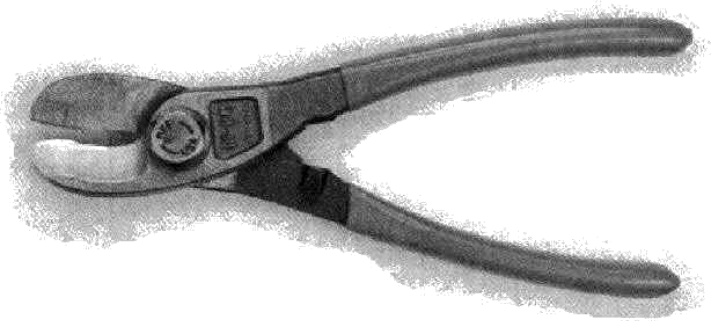
maglaris@netmode.ntua.gr

www.netmode.ntua.gr

13/11/2017

ΘΕΜΑΤΙΚΕΣ ΠΕΡΙΟΧΕΣ ΑΣΦΑΛΕΙΑΣ

- Είδη Απειλών και Επιθέσεων
- Προστασία
  - Πολιτικές
  - Αρχιτεκτονικές Ελέγχου Πρόσβασης (**Authentication & Authorization Infrastructures - AAI**) & Διαχείρισης Δημοσίων Κλειδιών (**Public Key Infrastructures - PKI**)
  - Εργαλεία (**Access Control Lists – ACLs, Firewalls**)
  - Συστήματα Εντοπισμού Επιθέσεων (**Intrusion Detection Systems – IDS**) & Ανωμαλιών (**Anomaly Detection Systems**)
- Κρυπτογραφία
- Η ***σίγουρη*** μέθοδος εξασφάλισης ενός δικτύου:



ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

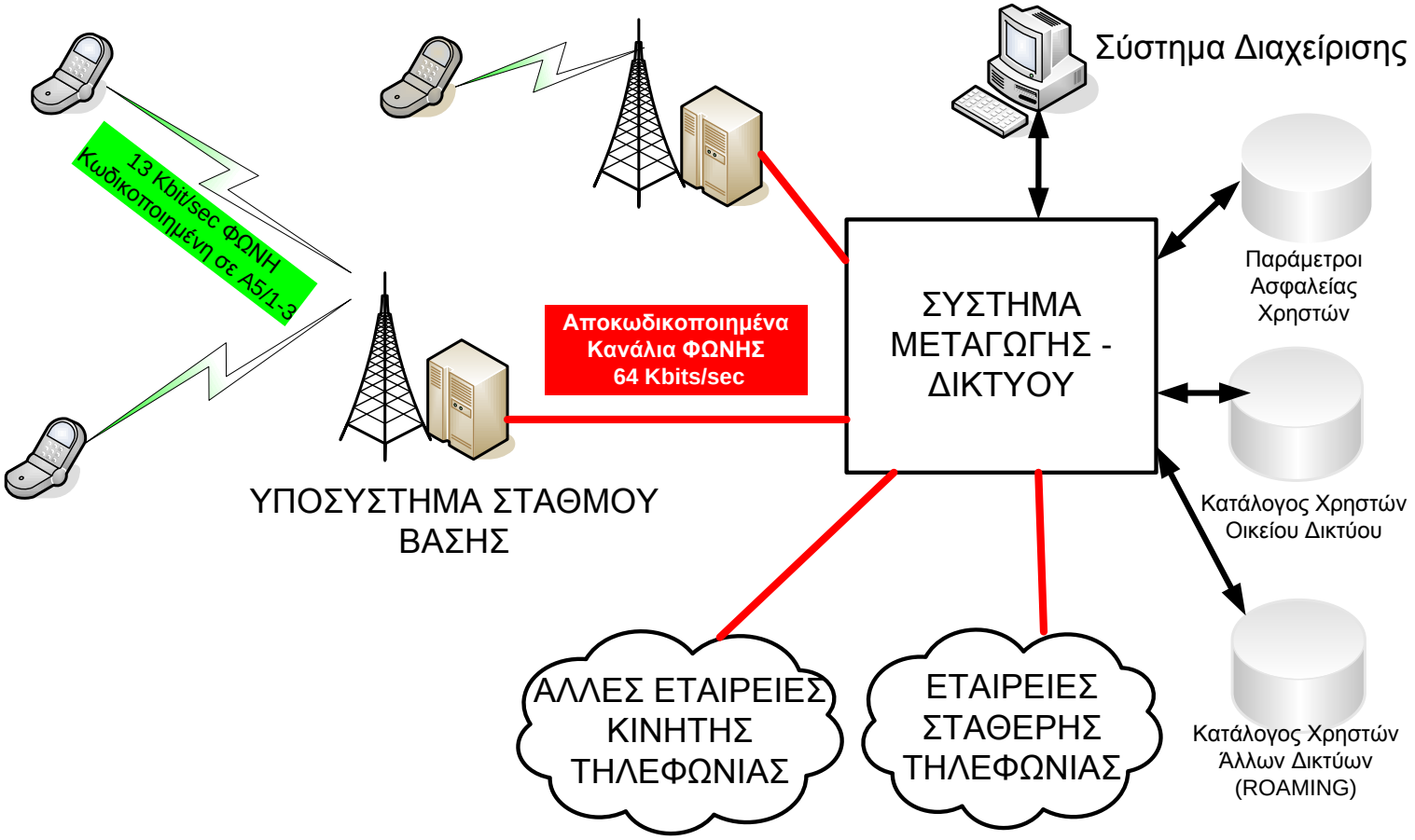
- **Απόκτηση πληροφοριών για το σύστημα:**
  - Port Scanning
  - Fingerprinting
- **Μη εξουσιοδοτημένη πρόσβαση**
  - Υποκλοπή κωδικών
  - Λάθος διαμορφώσεις (ανοικτά συστήματα)
  - Από μη εξουσιοδοτημένα σημεία (π.χ. ανοιχτά σημεία ασύρματης πρόσβασης)
- **Επιθέσεις Άρνησης Υπηρεσίας** (Denial of Service Attacks - DoS)
- **Υποκλοπή και παραποίηση επικοινωνιών**
  - Packet sniffing
  - "Man-in-the-Middle" attacks
- **Κακόβουλο λογισμικό** (malware)
  - Ιοί, Δούρειοι ίπποι (trojans)
  - Αυτόματα διαδιδόμενοι ιοί (worms)

ΥΠΟΚΛΟΠΗ & ΠΑΡΑΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

- **Packet sniffing**
  - Μπορεί να συμβεί σε δίκτυα με Hub, μη ασφαλισμένα ασύρματα δίκτυα ή σε περιπτώσεις υπερφόρτωσης του MAC Table ενός Switch
  - Κάθε πληροφορία που κυκλοφορεί μη κρυπτογραφημένη είναι διαθέσιμη σε αυτόν που παρακολουθεί
    - *Telnet passwords*
    - *Web passwords*
    - *Οικονομικά και προσωπικά στοιχεία (π.χ. προσωπικά email, αριθμοί πιστωτικών καρτών κ.λπ.)*
- **"Man-in-the-Middle" attacks**
  - Κάποιος μπορεί να παρεμβληθεί σε μια επικοινωνία και είτε να υποκλέψει τα στοιχεία είτε να "υποκριθεί" ότι είναι κάποιος τρίτος φορέας
    - *ARP "poisoning"*
    - *TCP "session hijacking"*
    - *DNS "poisoning" – URL redirection*
    - *Υποκλοπή περιεχομένου κλήσεων κινητής τηλεφωνίας GSM*

ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

GSM (1/11)



ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

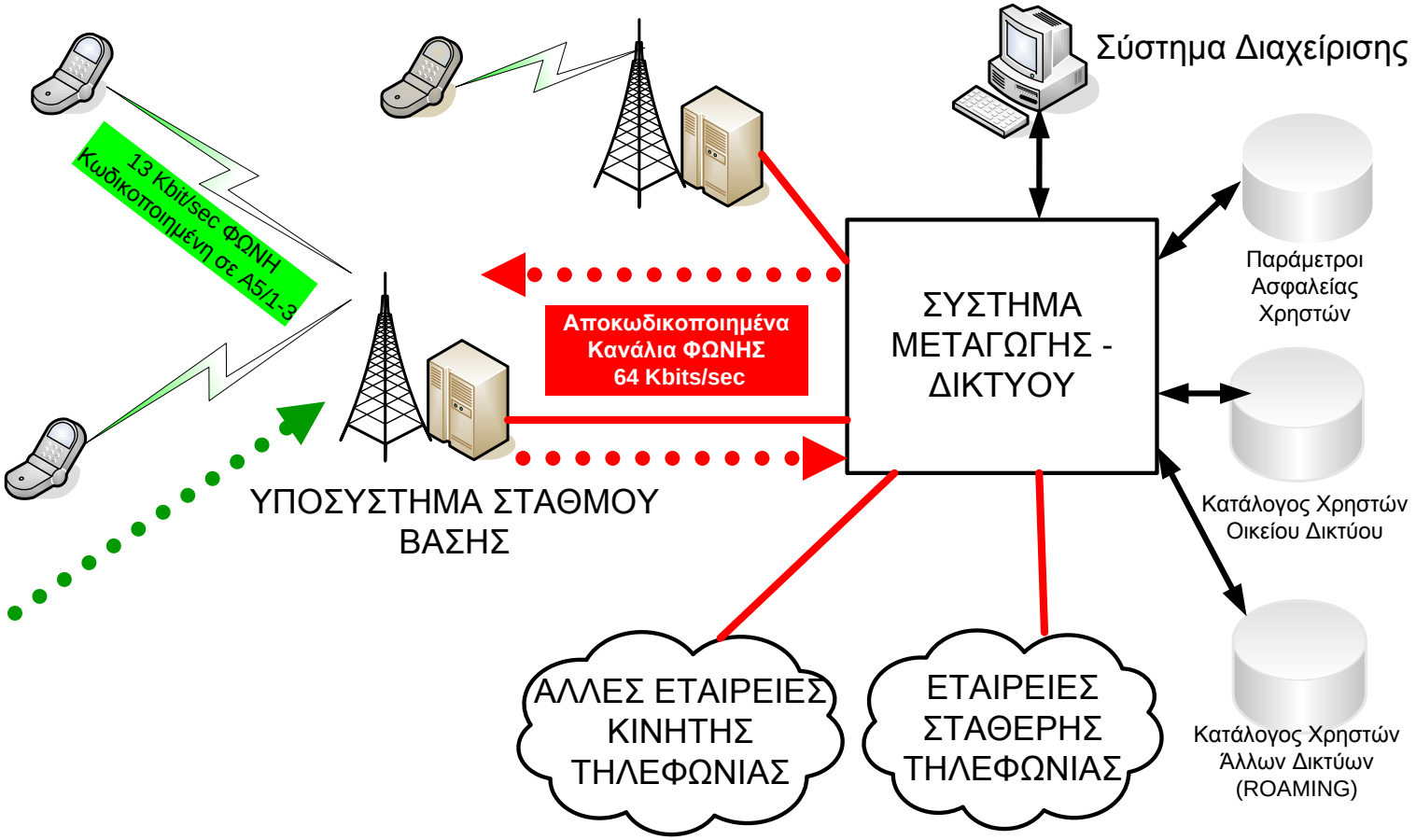
GSM (2/11)

ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

GSM (3/11)

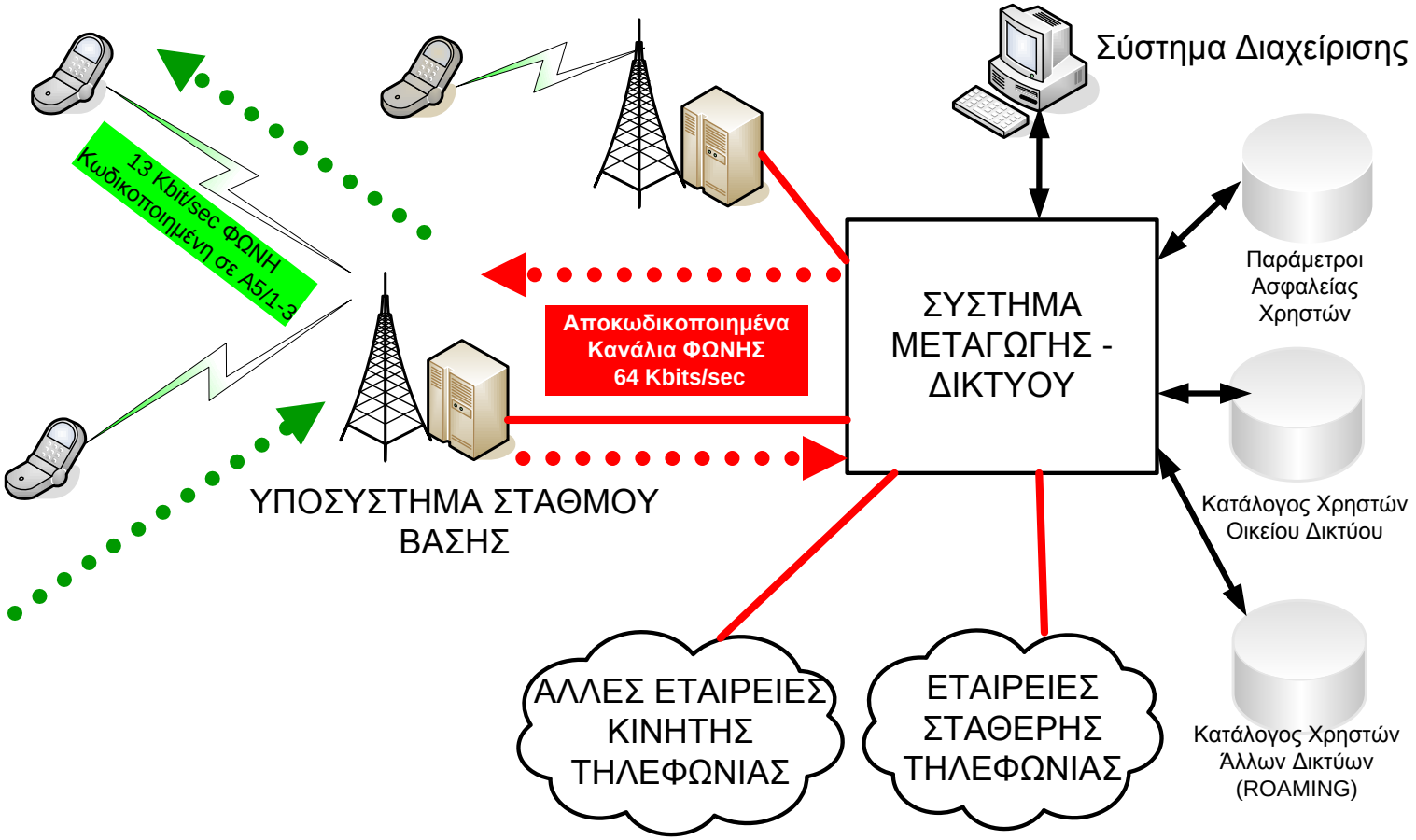
ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

GSM (4/11)

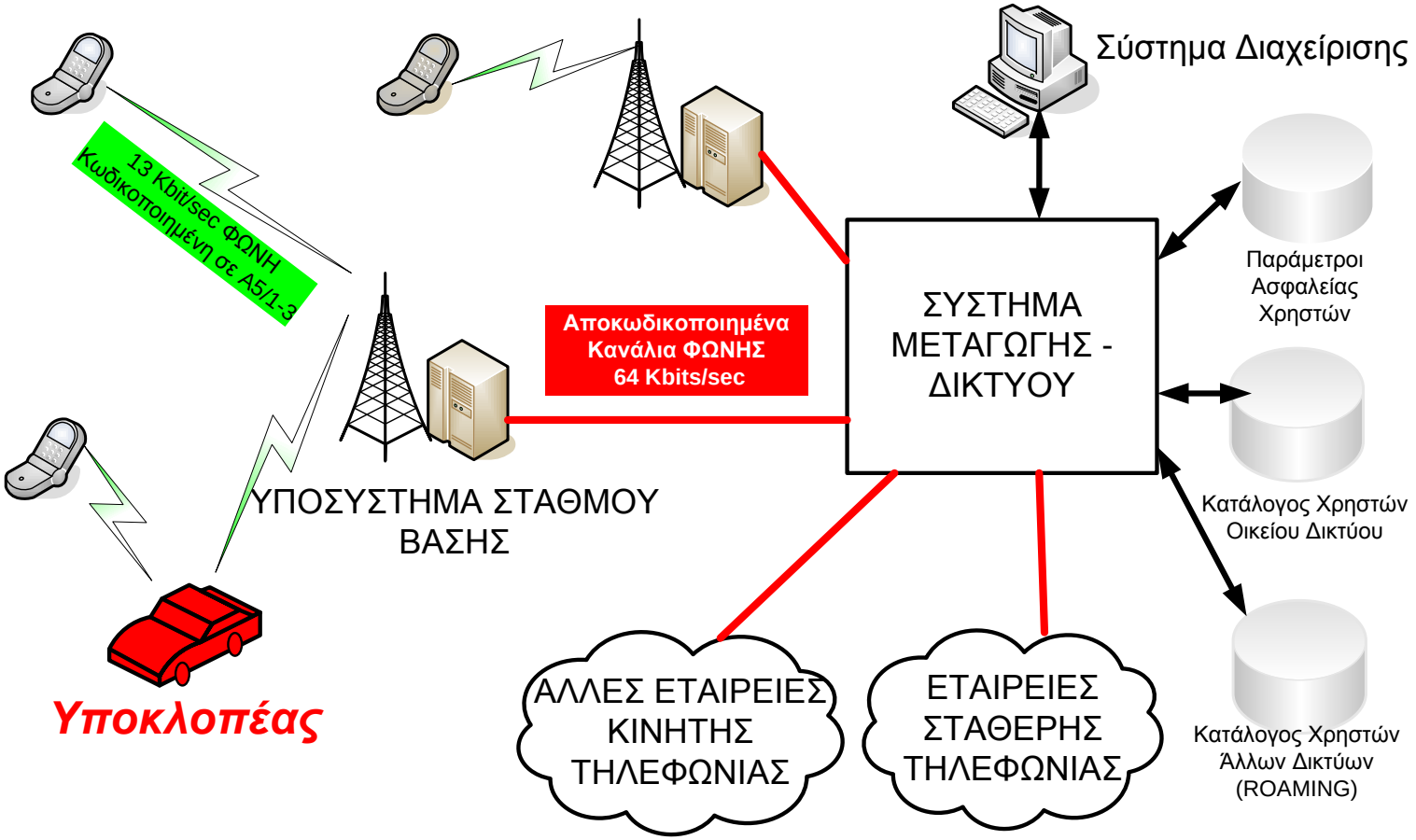


ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

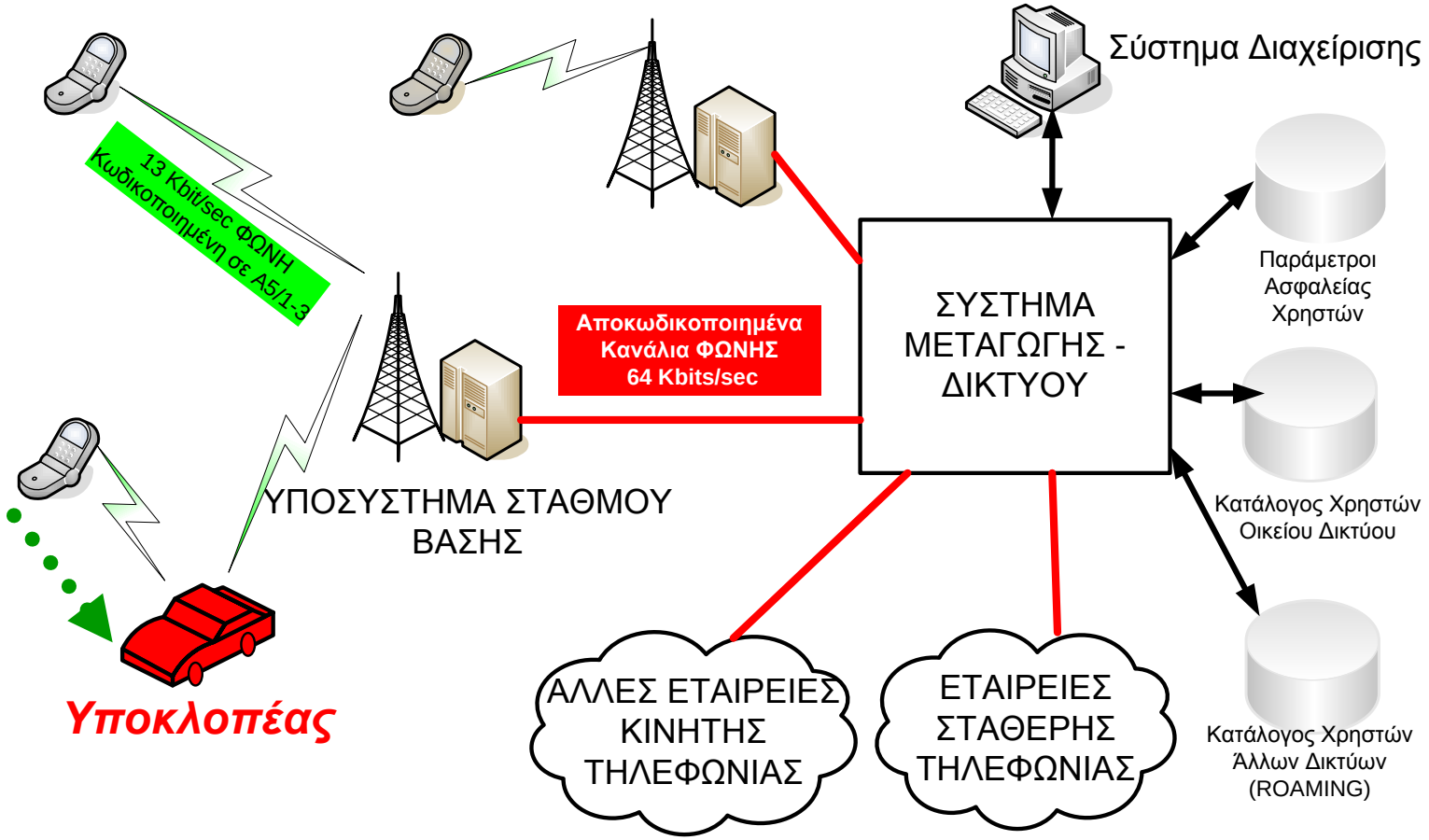
GSM (5/11)



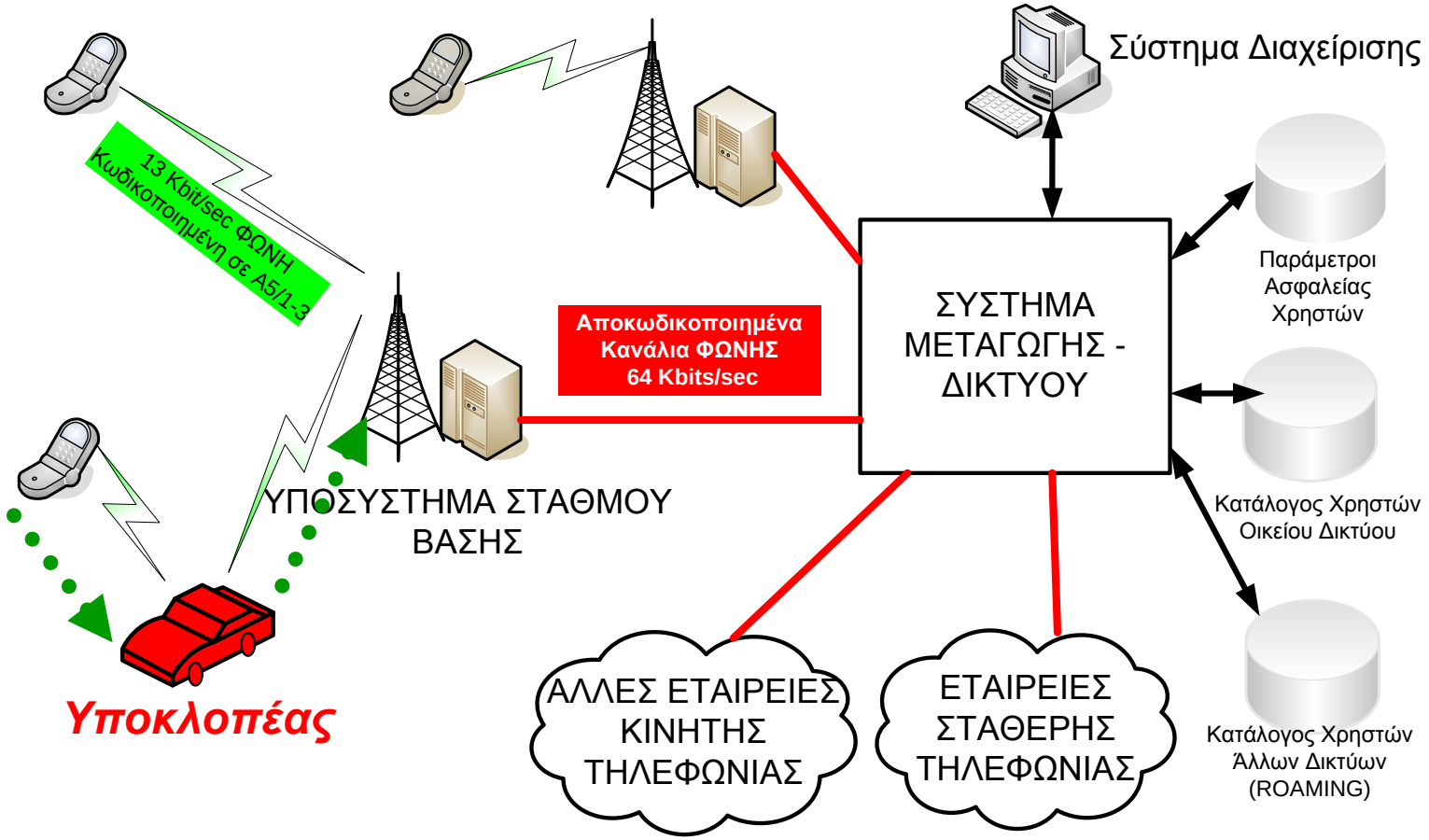
ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ
GSM (6/11)



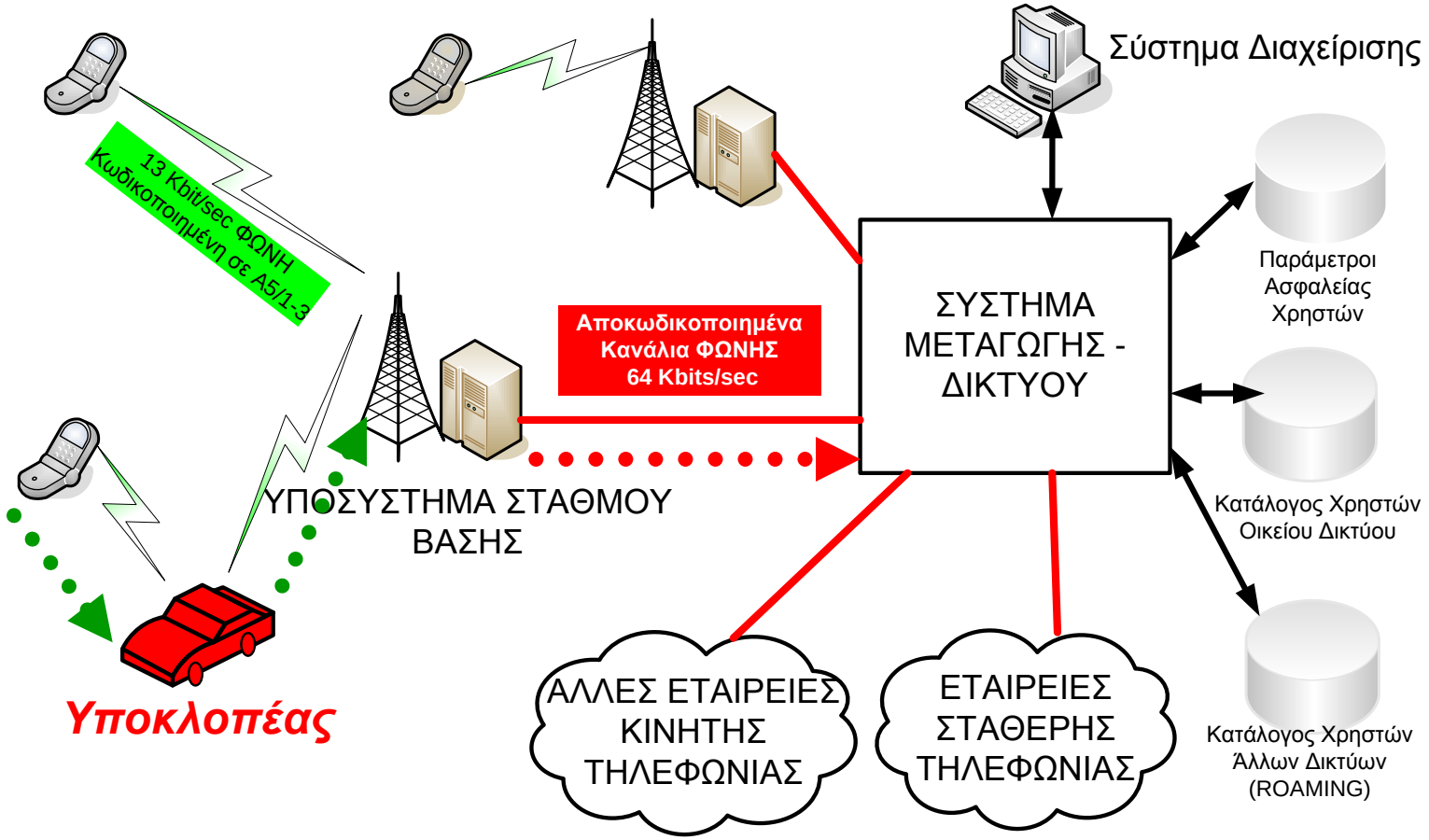
ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ
GSM (7/11)



ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ
GSM (8/11)

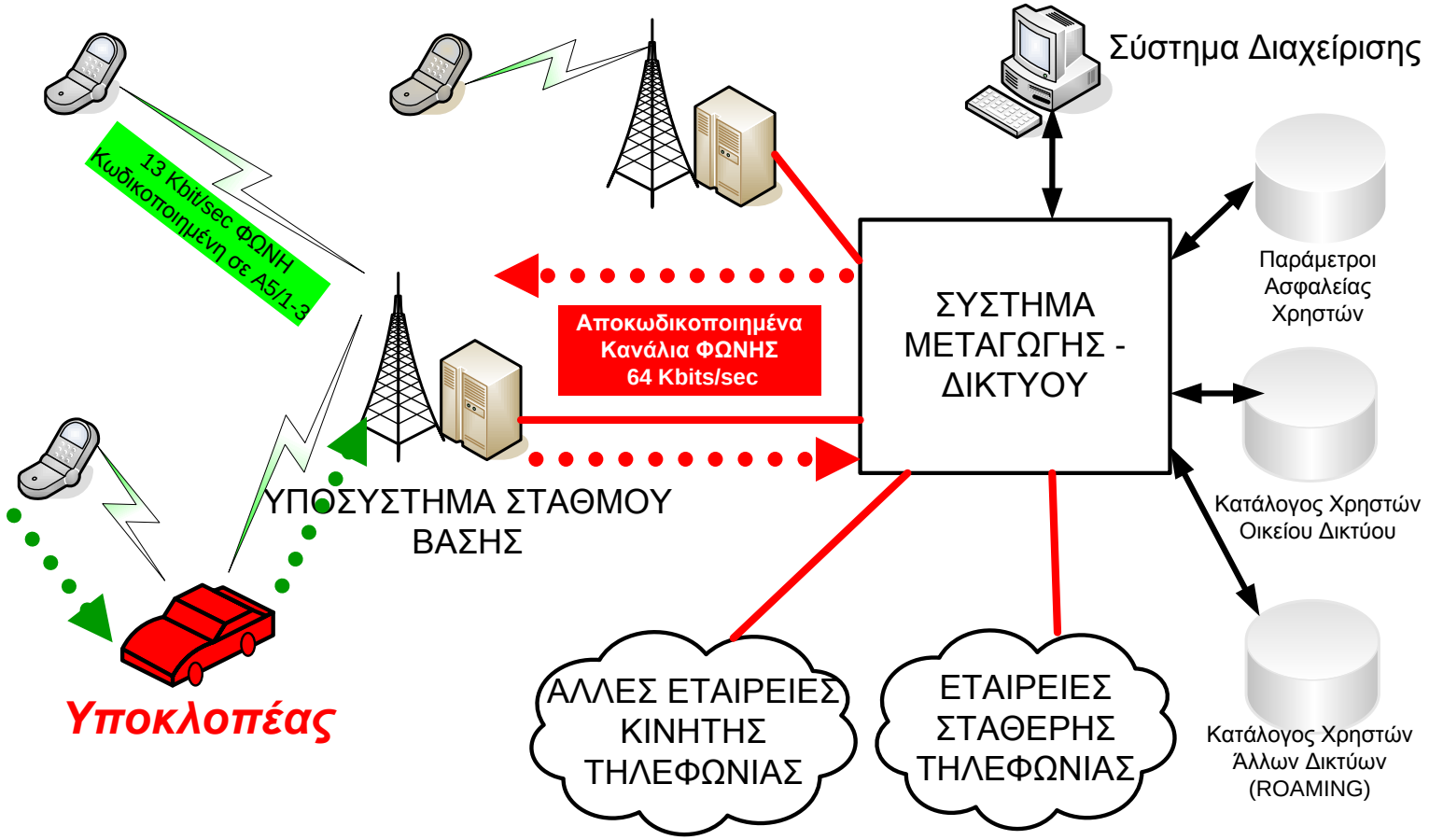


ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ
GSM (9/11)

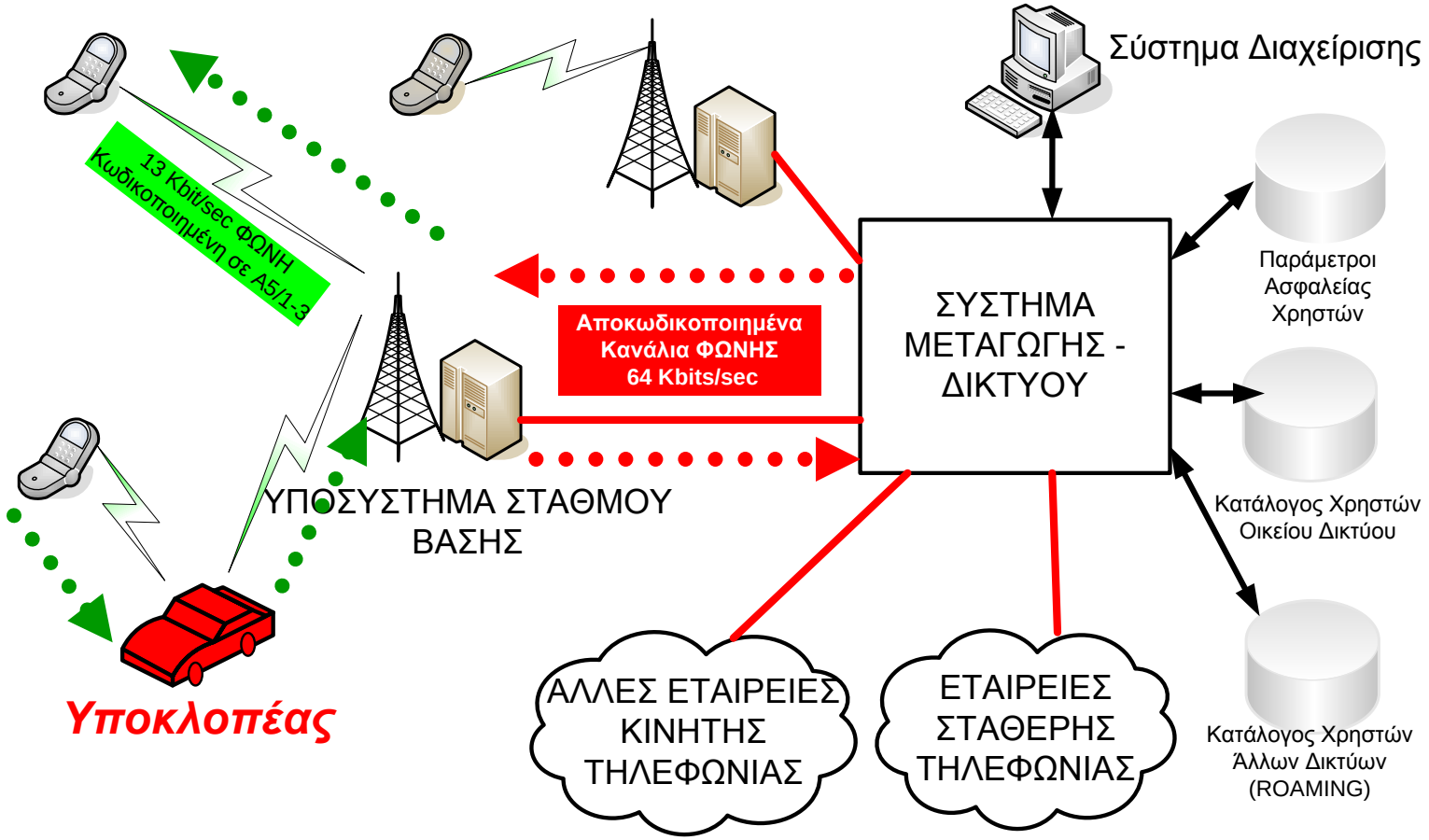


ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

GSM (10/11)



ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ
GSM (11/11)



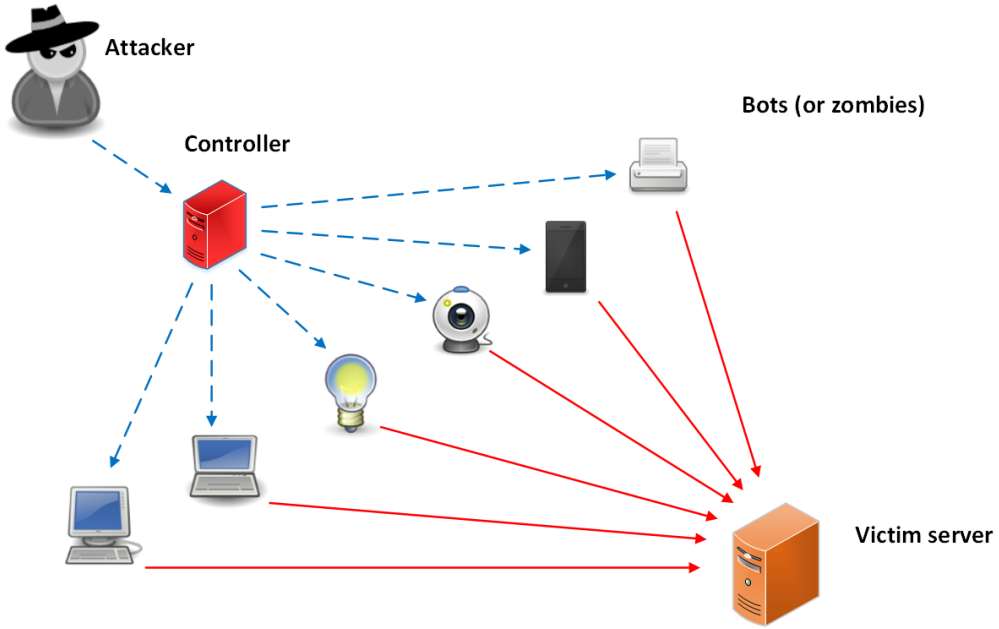
ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ (malware)

- **Αυτόματα Διαδιδόμενοι Ιοί** (**worms**)
  - *Εκμεταλλεύονται συνήθως άγνοια του τελικού χρήστη ή προβλήματα λογισμικού* (**vulnerabilities**) *σε Λειτουργικά Συστήματα ή εφαρμογές για να μεταδοθούν στο* **Internet**
  - *Διαδίδονται σε υπολογιστές με γειτονικές διευθύνσεις* **IP** *και το ίδιο πρόβλημα ή από προκαθορισμένη λίστα διευθύνσεων*
  - *Σε ορισμένες περιπτώσεις χρησιμοποιούνται παραπλανητικά μηνύματα* **e-mail** *που παρασύρουν το χρήστη στο να εκτελέσει συγκεκριμένες ενέργειες στον υπολογιστή του*
  - *Εφόσον χρησιμοποιήσουν ιδιαίτερα διαδεδομένο πρόβλημα είναι δυνατόν να εξαπλωθούν με μεγάλη ταχύτητα σε ολόκληρο το* **Internet**

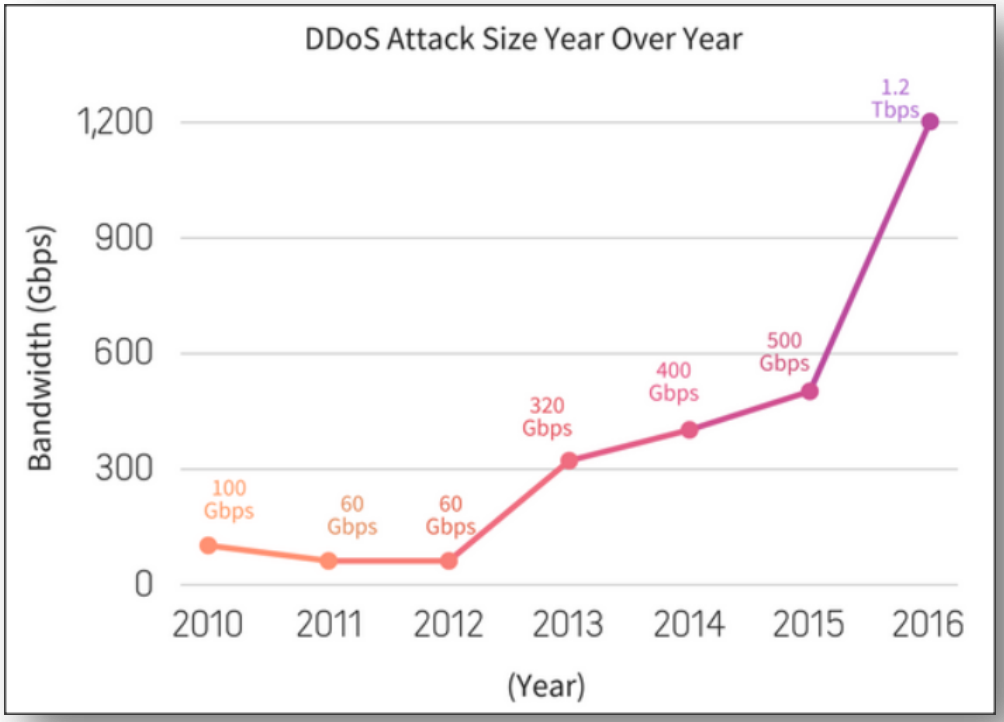
- **Δούρειοι Ίπποι** (**trojans** – executable προγράμματα "σε απόκρυψη")
  - *Έχουν συνήθως αργή μετάδοση, προσκείμενοι σε εκτελέσιμα προγράμματα*
  - *Συνήθεις τρόποι διάδοσης: Εγκατάσταση/εκτέλεση λογισμικού από* **USB Flash**, *δικτυακά με* **e-mail attachments**

DISTRIBUTED DENIAL OF SERVICE ATTACKS
DDoS Attacks

- **Bots ή Zombies**: *Μολυσμένοι* (π.χ. μέσω **worms** ή **Trojans**) *κόμβοι στο* **Internet** *(υπολογιστές - smart phones - sensors…) που ενεργοποιούνται σε ορισμένη χρονική στιγμή σαν* **bots** *ή* **zombie** *μαζικών Επιθέσεων Άρνησης Υπηρεσίας* (**Distributed Denial of Service Attacks, DDoS**)
- *Δρομολογείται μεγάλος όγκος κίνησης προς ένα θύμα με στόχο την κατασπατάληση του εύρους ζώνης της σύνδεσης του θύματος ή των πόρων του (επεξεργαστική ισχύς, μνήμη) ώστε να παρεμποδίζεται η όποια παρεχόμενη υπηρεσία*



ΕΞΕΛΙΞΗ ΕΠΙΘΕΣΕΩΝ DDoS



https://blogs.haltdos.com/wp-content/uploads/2017/02/2015.png

21 Οκτωβρίου 2016: Επίθεση DDoS στη Dyn, πάροχο DNS

- Μέγεθος κίνησης: **1.2 Tbps**
- Πηγή της επίθεσης **100.000** παραβιασμένες συσκευές Internet of Things
- Αδυναμία πρόσβασης μεγάλου αριθμού χρηστών σε σημαντικές υπηρεσίες επιχειρήσεων: **Amazon, CNN, Twitter, PayPal, Visa, GitHub, Spotify, Netflix,…**

ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

- Συμμετρική (Ιδιωτικού Κλειδιού, **Private Key Cryptography**)
  - *Χρήση μοναδικού κλειδιού και από τα δύο μέρη*
  - *Κρυπτογράφηση με συγκεκριμένου μήκους κομμάτια κειμένου* (**block cipher**) *ή ανά bit σε συνεχή ροή δεδομένων* (**stream cipher**)
  - *Αλγόριθμοι κρυπτογράφησης:* **DES, triple DES, RC2, RC4, RC5, IDEA, AES**
  - *Γρήγορη άλλα έχει προβλήματα στην ασφάλεια διανομής του κλειδιού*
  - *Έχει πολλαπλή χρήση:* **Encryption, authentication, non-repudiation**

- Μη Συμμετρική (Δημόσιου Κλειδιού, **Public Key Cryptography**)
  - *Κάθε μέρος έχει ιδιωτικό και δημόσιο κλειδί. Διανέμει το τελευταίο ελεύθερα*
  - *Αλγόριθμοι κρυπτογράφησης:* **RSA, Diffie-Hellman**
  - *Αλγόριθμοι κατακερματισμού (hash functions) για εξαγωγή περίληψης μέρους ή του συνόλου ενός μηνύματος:* **SHA & SHA-1, MD2, MD4, MD5**
  - *Ισχυρά σημεία:*
    - *Δεν διανέμονται ιδιωτικά κλειδιά – μόνο τα δημόσια κλειδιά*
  - *Αδύνατα σημεία:*
    - *Αργή στην εκτέλεση*
    - *Αμφισβήτηση εμπιστοσύνης στα δημόσια κλειδιά: γι' αυτό συνιστάται η εγκατάσταση Αρχών Πιστοποίησης* (**Certification Authorities, CA**) *και οργανωμένων υποδομών Δημοσίου Κλειδιού* (**Public Key Infrastructures, PKI**)
  - *Έχει πολλαπλή χρήση:* **Encryption, authentication, non-repudiation**