ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μέτρα Αυτοπροστασίας σε κινητές, σταθερές και ασύρματες επικοινωνίες

Παναγιώτης Θ. Τρακάδας, Ph.D.

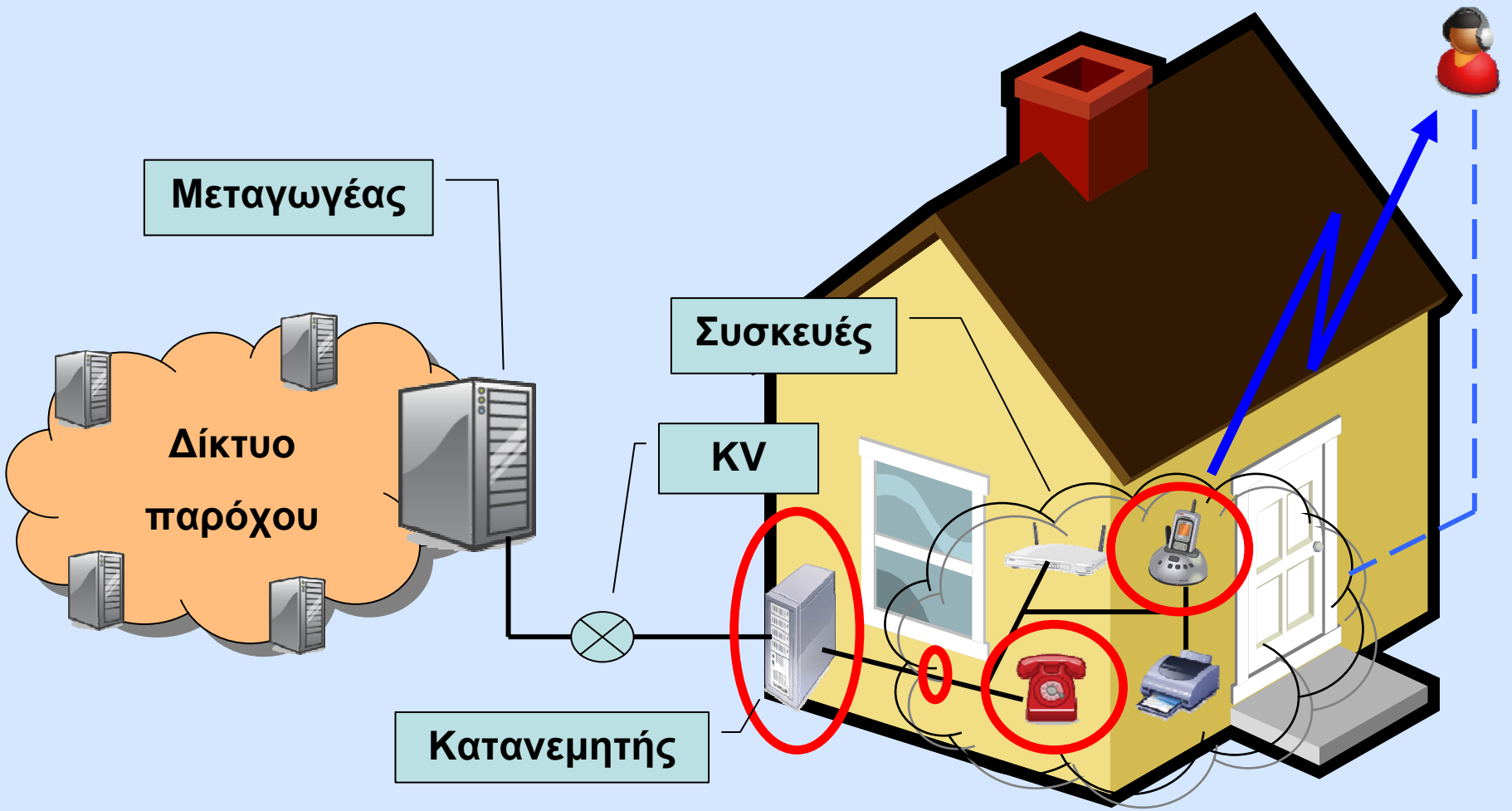
Ε.Ε.Π./Α.Δ.Α.Ε.

Περιεχόμενα

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- **Σταθερά Δίκτυα**
  - **«Ευάλωτα» σημεία**
  - **Μέθοδοι/συσκευές παραβίασης απορρήτου**
  - **Μέτρα αυτοπροστασίας**
- **Κινητά Δίκτυα**
  - **«Ευάλωτα» σημεία**
  - **Μέθοδοι/συσκευές/λογισμικό παραβίασης απορρήτου**
  - **Μέτρα αυτοπροστασίας**

«Ευάλωτα» σημεία σταθερού δικτύου



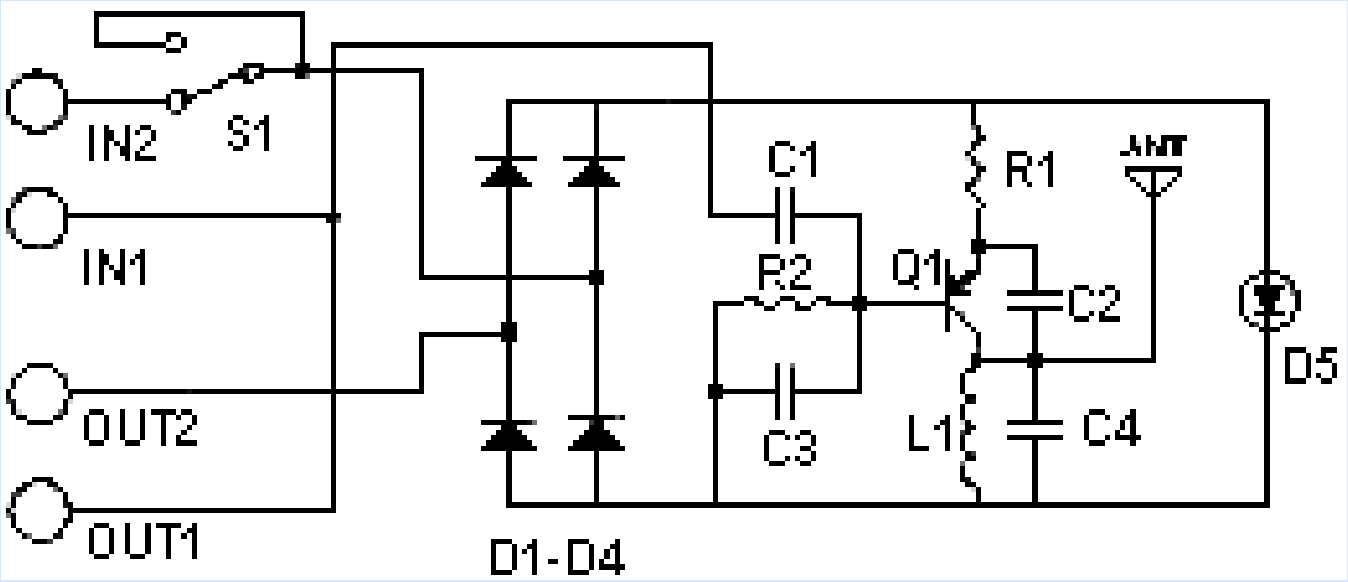
Μέθοδοι παραβίασης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

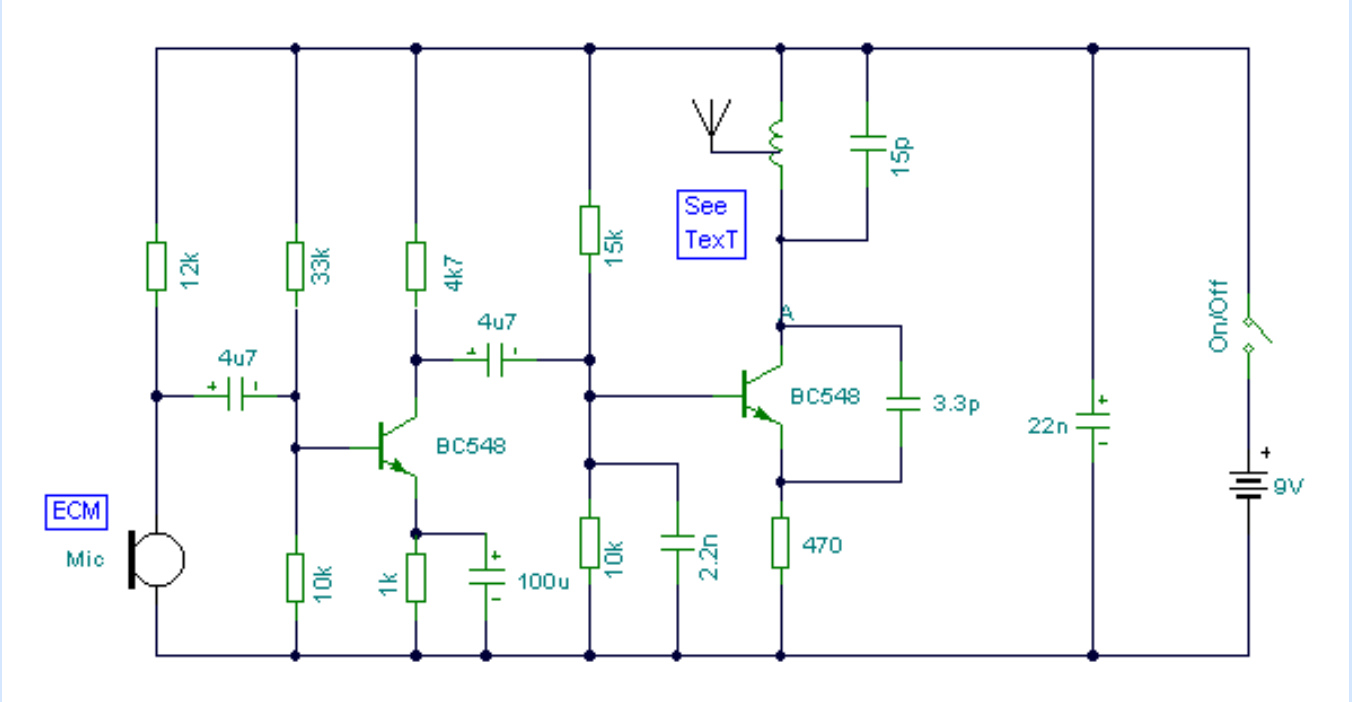
Οι μέθοδοι παραβίασης χωρίζονται σε τέσσερις κύριες κατηγορίες:

- **Hard Wiretap: Παραλληλισμός τηλεφωνικού καλωδίου (προϋποθέτει φυσική πρόσβαση στο καλώδιο).**
- **Soft Wiretap ή Translation Tap: Μέθοδος παραβίασης η οποία βασίζεται στην κατάλληλη τροποποίηση του λογισμικού στο τηλεφωνικό κέντρο (PBX).**
- **Record Wiretap: Η μέθοδος αυτή είναι όμοια με τη μέθοδο Hard Wiretap με τη διαφορά της χρήσης μαγνητοφώνου.**
- **Transmit Wiretap: Η πλέον διαδεδομένη μέθοδος παραβίασης. Πομπός RF που συνδέεται στο τηλεφωνικό καλώδιο.**

Κυκλωματικό διάγραμμα 1



Κυκλωματικό διάγραμμα 2



Τύποι συσκευών

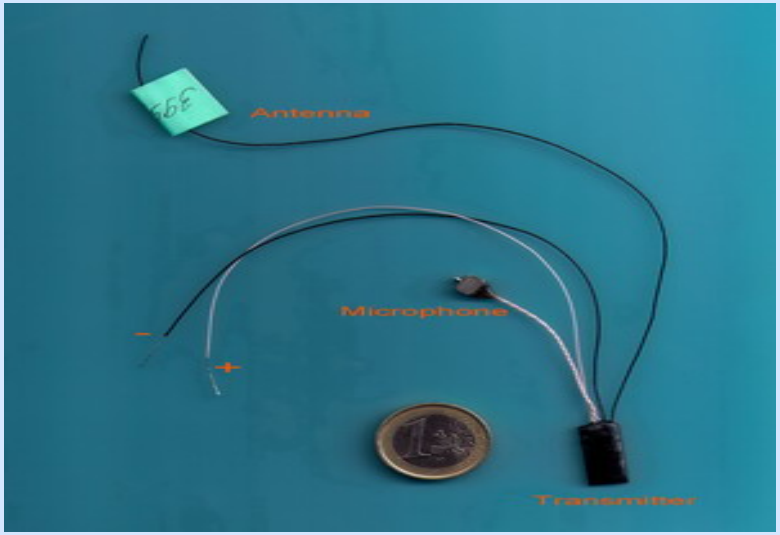
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- **Πομπός RF**
  Ο πιο διαδεδομένος τύπος συσκευής. Εκπέμπει το σήμα σε μεγάλες αποστάσεις. Τροφοδοτείται από την τηλεφωνική γραμμή ή από μπαταρία. Είναι δυνατό να τοποθετηθεί σε διάφορα σημεία (καλώδιο, τηλεφωνική συσκευή, κλπ).
- **Infinity Transmitter ή Harmonica Bug**
  Παλαιού τύπου συσκευές που συνδέονται στο τηλέφωνο και δίνουν τη δυνατότητα ακρόασης των συνομιλιών στο χώρο, χωρίς να χτυπήσει το τηλέφωνο.
- **Hook-switch Bypass**
  Μέθοδος μόνιμης ενεργοποίησης του μικροφώνου του ακουστικού. Απαιτείται τροποποίηση του κυκλώματος της τηλεφωνικής συσκευής. Με τον τρόπο αυτό είναι δυνατό να ακούγονται όλες οι συνομιλίες στο χώρο.

Συσκευές παραβίασης (1/3)

- Πομπός UHF τηλεφωνικού σήματος, ο οποίος συνδέεται σε οποιοδήποτε σημείο της διαδρομής του καλωδίου (συσκευή ή κατανεμητής). Ο πομπός τροφοδοτείται από την τηλεφωνική γραμμή. Το εκπεμπόμενο σήμα μπορεί να ληφθεί σε απόσταση έως 1km (line of sight).

- Πομπός ακουστικού σήματος UHF με απόσταση λήψης σήματος σε απόσταση 500-700 μέτρα.



Συσκευές παραβίασης (2/3)

- **Πομπός UHF τηλεφωνικού σήματος ενσωματωμένος σε τηλεφωνική πρίζα. Τροφοδοτείται από την τηλεφωνική γραμμή και παρέχει τη δυνατότητα καταγραφής των εισερχομένων και εξερχομένων κλήσεων. Η απόσταση λήψης είναι περίπου έως 600 μέτρα.**

- **Πομπός ενσωματωμένος σε τηλεφωνικό καλώδιο.**

Συσκευές παραβίασης (3/3)

- **Πομπός FM τηλεφωνικού σήματος, ενσωματωμένος σε τηλεφωνική πρίζα.**

- **Συνδέεται στην τηλεφωνική γραμμή και εκπέμπει τη συνομιλία στη ζώνη συχνοτήτων AM/FM**

Μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Να ελέγχετε σε τακτά χρονικά διαστήματα τη συσκευή σας για σημάδια πιθανής παραβίασης και ενδεχόμενης τοποθέτησης συσκευών παρακολούθησης.
- Αν χρησιμοποιείτε ασύρματη συσκευή (DECT), θα πρέπει να ελέγχετε αρχικά εάν είναι πιστοποιημένη αναφορικά με τις χρησιμοποιούμενες συχνότητες για το σκοπό αυτό. Επιπλέον, δεν θα πρέπει να γίνεται χρήση της συσκευής σε πολύ απομακρυσμένα σημεία από το σταθμό βάσης διότι είναι πιθανό να υπάρχουν παρεμβολές από ασύρματες συσκευές γειτονικών οικιών.
- Το κουτί διανομής (box) και ο πίνακας διανομής (εσκαλίτ) στα οποία τερματίζει το δημόσιο τηλεπικοινωνιακό δίκτυο, θα πρέπει να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα. Επίσης, θα πρέπει να ελέγχετε τα σημεία αυτά σε τακτά χρονικά διαστήματα για πιθανή παραβίασή τους.
- Δοκιμή με συμβατικό ραδιόφωνο.

Συσκευές προστασίας (1/2)

- **Αναλυτής τηλεφωνικής γραμμής**
  Συνδέεται στην τηλεφωνική γραμμή και δίνει τη δυνατότητα ανίχνευσης συσκευών παραβίασης του απορρήτου.

- **Non-Linear Junction Detector**
  Εντοπίζει συσκευές παραβίασης του απορρήτου, με τη λήψη σήματος που προέρχεται από την 3η αρμονική κυκλωματικών στοιχείων του κυκλώματος (διόδους, τρανζίστορ, κλπ) με μη-γραμμική συμπεριφορά.

Συσκευές προστασίας (2/2)

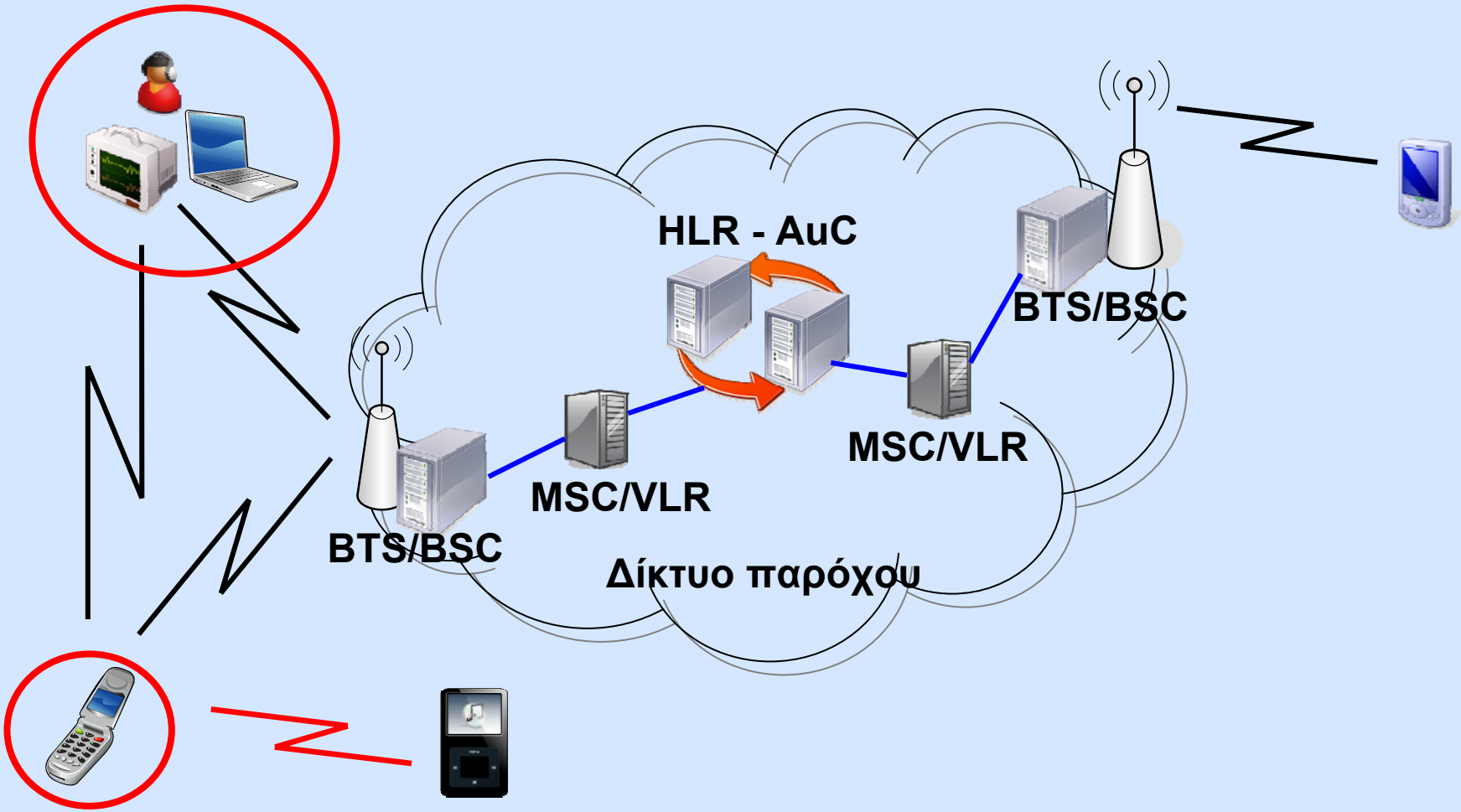
- **Αναλυτής φάσματος**

  Εποπτεύει το φάσμα για εκπομπές και αναλύει τα χαρακτηριστικά των σημάτων. Χρησιμοποιείται για την ανίχνευση πομπών RF.

- **Παρεμβολέας κινητών τηλεφώνων**

  Κατάλληλος για χρήση σε κλειστούς χώρους όπου δεν επιτρέπεται η χρήση κινητών

«Ευάλωτα» σημεία κινητού δικτύου



Πιθανοί Κίνδυνοι

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Μηνύματα-ιοί, «δούρειοι ίπποι», προγράμματα «απομακρυσμένου» ελέγχου συσκευής.
- Επιθέσεις «άρνησης υπηρεσίας».
- Πραγματοποίηση κλήσεων προς αριθμούς υψηλής χρέωσης.
- Προσπέλαση κακόβουλων ιστοσελίδων (WAP).
- Πρόσβαση σε προσωπικά δεδομένα, αποθηκευμένα στο κινητό (συσκευή, κάρτα μνήμης).
- Παρακολούθηση κλήσεων και μηνυμάτων SMS

Τρόποι εισαγωγής «ιών»

- **Bluetooth**
- **email, instant message, MMS**
- **WAP page**
- **Infrared**

Java J2ME APIs

- MIDP 2.0 API JSR-139
- Location API JSR-179
- Bluetooth API JSR-082
- PDA Optional API JSR-075
- Wireless Messaging API JSR-120

Κίνδυνοι λόγω Bluetooth

- Μεταφορά και εγκατάσταση «εφαρμογής»
- Πρόσβαση σε δεδομένα αποθηκευμένα στη συσκευή
- Πραγματοποίηση κλήσεων ή αποστολής μηνυμάτων

Συσκευές παραβίασης

- **Man-in-the-middle interceptor Εκμεταλλεύεται κενά ασφάλειας του συστήματος GSM 2G. Παρέχει δυνατότητα παρακολούθησης συνομιλιών και λοιπών δεδομένων (SMS, cell ID, κλπ).**

- **Κινητά τηλέφωνα κατάλληλα τροποποιημένα ώστε να λειτουργούν ως μικρόφωνα.**

Μέτρα αυτοπροστασίας (1/2)

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Μην ανακοινώνετε το PIN σε τρίτους. Αλλάξτε το αρχικό PIN και χρησιμοποιείστε κάποιο νέο με όσο το δυνατόν πιο δύσκολο συνδυασμό.
- Μην αφήνετε το κινητό τηλέφωνο εκτεθειμένο σε μη εξουσιοδοτημένη πρόσβαση και προστατεύστε το από το ενδεχόμενο κλοπής.
- Μην εγκαθιστάτε εφαρμογές και μην αποθηκεύετε άγνωστα αρχεία που δέχεστε μέσω Bluetooth, WAP σελίδων, email και MMS.
- Εάν στο κινητό τηλέφωνο είναι εγκατεστημένα ανοιχτά προγράμματα λογισμικού (π.χ. Symbian OS) θα πρέπει να χρησιμοποιείτε κάποιο λογισμικό ανίχνευσης και αντιμετώπισης ιών (antivirus software).
- Να ελέγχετε συστηματικά τους λογαριασμούς σας για τυχόν χρεώσεις σε μηνύματα SMS/MMS που δεν έχετε στείλει ή χρεώσεις για δεδομένα (GPRS/3GWAP, GPRS/3GInternet) που δεν έχετε «κατεβάσει».

Μέτρα αυτοπροστασίας (2/2)

- Όταν το Bluetooth δεν χρησιμοποιείται, να είναι απενεργοποιημένο ή σε «αόρατη/κρυφή» κατάσταση λειτουργίας (hidden mode).
- Να αποφεύγετε την πραγματοποίηση «συζεύξεων» (pairs) με άγνωστες συσκευές ή σε χώρους με πολλά ενεργοποιημένα Bluetooth.
- Να καταργείτε τις συζεύξεις με συσκευές τρίτων ή παλαιότερες συζεύξεις που δεν χρησιμοποιείτε πια, εφόσον έχουν εξυπηρετήσει το σκοπό τους.
- Όταν «αναβοσβήνει» συχνά η ένδειξη σύνδεσης του Bluetooth χωρίς προφανή λόγο, θα πρέπει να το απενεργοποιείτε.
- Χρήση κρυπτογράφησης end-to-end.