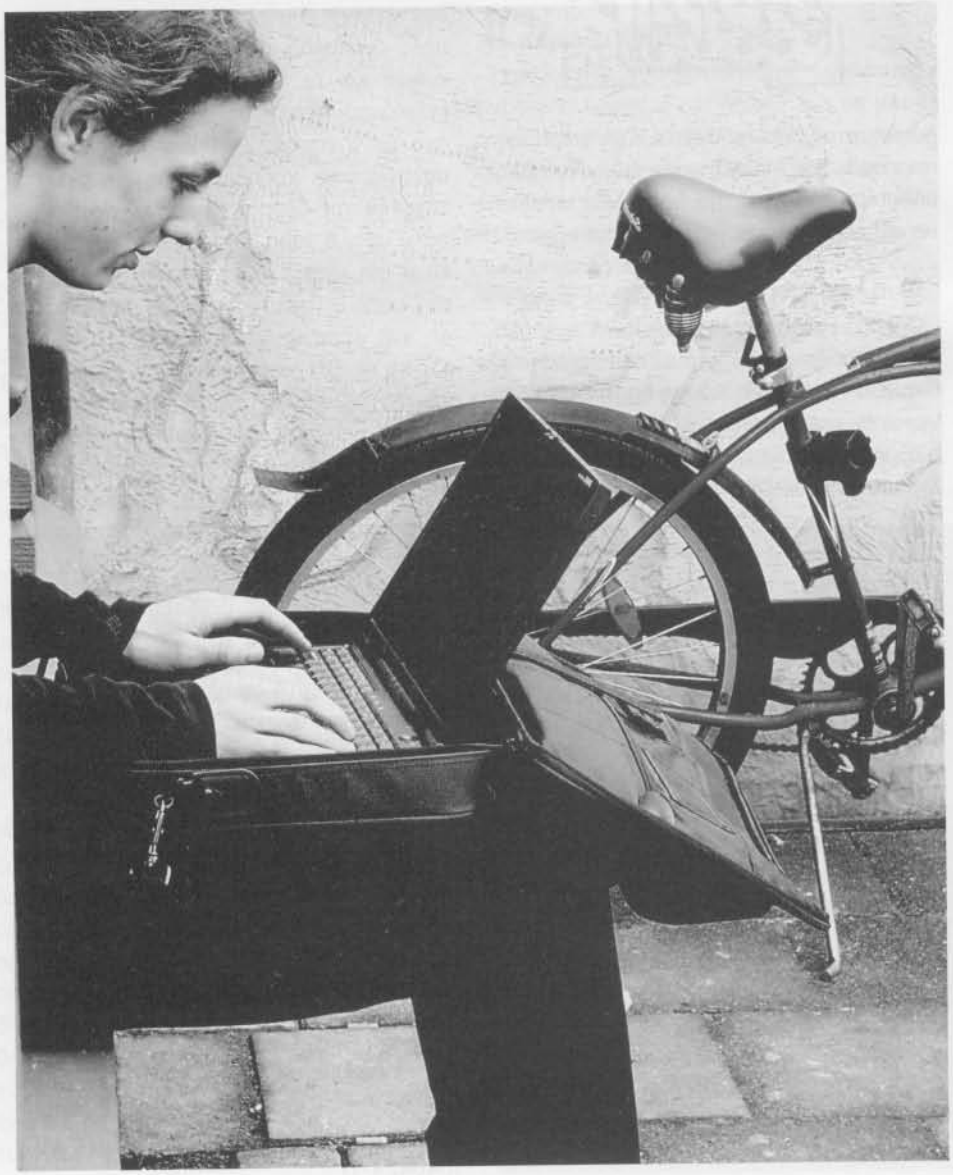
Εξοπλισμός WiFi

Πόσο ασφαλής αποδεικνύεται στις υποκλοπές;

Η τελευταία λέξη στο χώρο των υπολογιστών είναι οι ασύρματες δικτυώσεις. Ετσι λοιπόν, αν θέλετε να είστε 'in', δεν έχετε παρά να προμηθευτείτε μια κάρτα επέκτασης μαζί με ένα Σημείο Πρόσβασης (ή μια εξωτερική μονάδα USB για το φορητό σας) και να αρχίσετε το παιγνίδι. Πως είπατε; Αυτό το έχετε ήδη κάνει; Μη στενοχωριέστε. Σίγουρα δεν είστε οι μοναδικοί!

Από τον Fedde Hettinga



Το τελευταίο χρόνο οι πωλήσεις των μονάδων πρόσβασης σε ασύρματα δίκτυα, γνωστών και σαν Σημεία Πρόσβασης (Access Points), σημείωσαν μια καταπληκτική άνοδο. Και αυτό, όχι μόνο στην πατρίδα του συγγραφέα (Ολλανδία), αλλά και στις υπόλοιπες Ευρωπαϊκές (και μη) χώρες. Γιατί συνέβη αυτό; Απλά, διότι με τη βοήθειά τους η υλοποίηση ενός δικτύου πραγματοποιείται χωρίς κόπο εξασφαλίζοντας παράλληλα υψηλές ταχύτητες διαμεταγωγής δεδομένων. Οι προϋποθέσεις αυτές θεωρούνται πως είναι οι σημαντικότερες από όλους σχεδόν τους χρήστες δικτύων και γενικά από όλους όσους ασχολούνται με τους υπολογιστές.

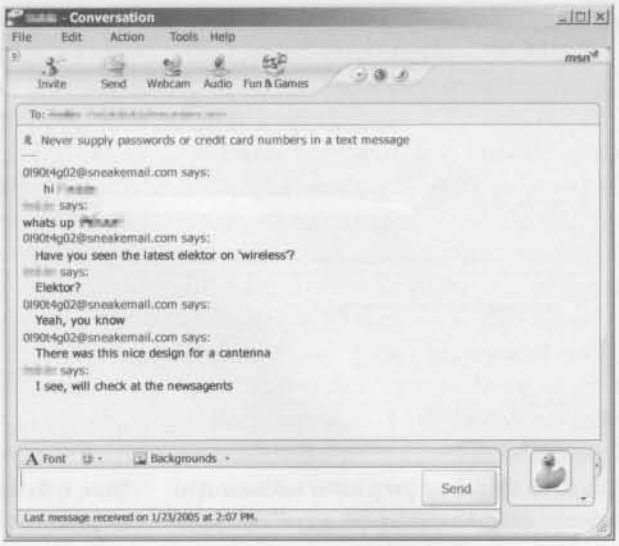
Όμως, τα ασύρματα δίκτυα, τουλάχιστον στην απλούστερη μορφής τους είναι ευάλωτα στις υποκλοπές και στις πάσης φύσεως πειρατικές επεμβάσεις. Έτσι λοιπόν, αν έχετε αφήσει το δικό σας ασύρματο δίκτυο στο έλεος των εργοστασιακών ρυθμίσεών του, είναι σχεδόν βέβαιο πως ο γείτονάς σας που έχει 'στήσει' και αυτός ένα αντίστοιχο δίκτυο, απολαμβάνει τις υπηρεσίες Διαδικτύου που πληρώνετε εσείς για λογαριασμό σας. Αυτό όμως είναι το λιγότερο ενοχλητικό. Αν ο γείτονάς σας είναι ένας από τους γνωστούς 'χάκερ' της περιοχής, τότε εκτός από τις δωρεάν υπηρεσίες Διαδικτύου που του προσφέρετε, 'ψαχουλεύει' ταυτόχρονα τον υπολογιστή σας αναζητώντας ευαίσθητα προσωπικά σας στοιχεία (από έγγραφα μέχρι και κωδικούς πιστωτικών καρτών) και προγράμματα. Αυτό

είναι κάτι που για τους περισσότερους αποτελεί μια ενοχλητική πραγματικότητα, αναγκάζοντας τους να 'θωρακίζουν' τα Σημεία Πρόσβασης μέσω των οποίων πραγματοποιείται η ανταλλαγή δεδομένων. Μόνο με τις κατάλληλες ρυθμίσεις είναι δυνατόν να αποφύγουν τις εισβολές και κατά συνέπεια την απώλεια ή τη δημοσιοποίηση των στοιχείων που φιλοξενούνται στους υπολογιστές τους.

Δεν είναι όμως απαραίτητο όλα τα ασύρματα δίκτυα να προστατεύονται με πολύπλοκους συνδυασμούς υλικού / λογισμικού. Τα Internet cafe, οι χρηματιστηριακές εταιρίες, τα αεροδρόμια αλλά και πολλά άλλα μέρη που συχνάζει πολύ κόσμος, έχουν τις περισσότερες φορές τα δίκτυα τους 'ανοικτά' σε κάθε ενδιαφερόμενο (δίκτυα γνωστά με το όνομα 'hotspots'). Οποιοσδήποτε διαθέτει ένα φορητό υπολογιστή με κάρτα WiFi, μπορεί π.χ. να μάθει πότε φεύγει η πτήση του ή να στείλει e-mail στην οικογένεια του και στους φίλους του. Αρκεί μια απλή ασύρματη σύνδεση με το υπάρχον (ασύρματο) δίκτυο και όλα αποδεικνύονται θέμα μερικών δευτερολέπτων. Για αυτού του είδους τις εφαρμογές δεν τίθεται θέμα ασφάλειας, μιας που οι ζημιές που ενδεχομένως θα προκληθούν στο κεντρικό σύστημα είναι από ελάχιστες έως μηδενικές.

Πως όμως καταφέρνει ο επίδοξος 'λαθρακουστής' να παρακολουθεί τις δραστηριότητές σας; Ανάμεσα στο φορητό υπολογιστή που χρησιμοποιείτε σαν τερματικό και στο Σημείο Πρόσβασης του δικτύου που είστε πελάτης μεσολαβεί μόνο ο αέρας. Για την σύνδεση επομένως, των δύο αυτών συσκευών χρησιμοποιούνται ηλεκτρομαγνητικά κύματα, παρόμοια με αυτά μιας συνηθισμένης δορυφορικής ζεύξης. Είναι λοιπόν απόλυτα εφικτό σε κάποιον που διαθέτει τον κατάλληλο δέκτη (έναν υπολογιστή με κάρτα WiFi, δηλαδή) να 'πιάσει' τα e-mail σας καθώς ταξιδεύουν στον άερα ή, απλά, να παρακολουθεί και να καταγράφει τους δικτυακούς τόπους που επισκέπτεστε. Με λίγα λόγια, το να χρησιμοποιείτε ένα τέτοιο δίκτυο, είναι το ίδιο με το να μιλάτε έντονα με ένα φίλο σας στο μέσον μιας πλατείας. Όλοι οι περαστικοί είτε το θέλουν είτε όχι, σας ακούν. Υπάρχουν όμως και περιπτώσεις που θέλετε η παρουσία σας μέσα στο δίκτυο να είναι περισσότερο διακριτική. Να μην σας 'ακούν' όλοι. Σε μια τέτοια περίπτωση θα πρέπει να αποταθείτε σε κάποιον 'Ειδικό'.

Ο 'Ειδικός' είναι ένας πρωτοετής φοιτητής του τομέα Τεχνητής Νοημοσύνης. Ασχολήθηκε κατ' αρχήν με το αντικείμενο των ασύρματων επικοινωνιών WiFi και, αμέσως μετά, με το κατά πόσο αυτές μπορούν να βελτισοποιηθούν σε ότι αφορά την ασφάλειά τους. Το συμπέρασμα που κατέληξε ήταν θετικό για την έρευνά του. Στη συνέχεια παραθέτονται οι τρόποι και οι μέθοδοι που πρέπει να ακολουθηθούν.



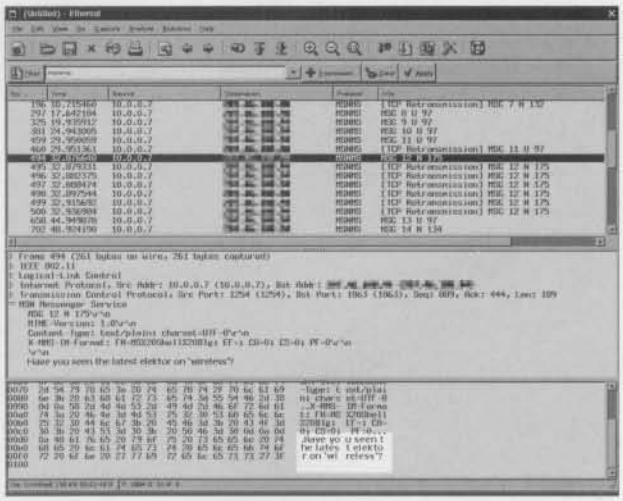
Σχ. 1. Τα περιεχόμενα της συζήτησης ενός ανυποψίαστου χρήστη.

Λίγη θεωρία

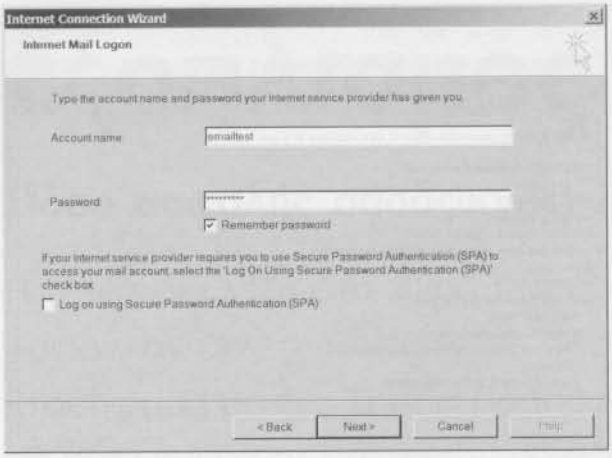
Ένα ασύρματο δίκτυο επιτρέπει σε ένα σύνολο υπολογιστών να επικοινωνούν μεταξύ τους χωρίς τη χρήση καλωδίων ή άλλων αγωγών. Τα περισσότερα ασύρματα δίκτυα που είναι εγκαταστημένα σήμερα είναι συμβατά με το πρωτόκολλο 802.11, γνωστό στους περισσότερους με το όνομα WiFi (Wireless Fidelity, Ασύρματη Πιστότητα). Η εμβέλεια ενός τέτοιου δικτύου φθάνει τα 100 μέτρα σε εσωτερικούς χώρους ή τα 300 μέτρα σε ανοικτούς (ιδανικές περιπτώσεις μετάδοσης). Σε ότι αφορά στο υλικό του, στην πιο συνηθισμένη οργάνωσή του, απαιτεί την παρουσία ενός Σημείου Πρόσβασης (κεντρικό πομποδέκτη του δικτύου) και ενός ή περισσότερων 'ασυρμάτων πελατών' (υπολογιστών με ενσωματωμένη ή εξωτερική (τύπου USB) κάρτα WiFi. Σε ένα τέτοιο δίκτυο όλη η κίνηση διεκπεραιώνετε μέσω του Σημείου Πρόσβασης. Όταν ένας 'ασύρματος πελάτης' βρίσκεται εντός εμβέλειας, τότε είναι σε θέση να επικοινωνεί με όλους τους άλλους πελάτες που 'ακούν' το Σημείο Πρόσβασης. Αν μάλιστα το τελευταίο έχει τη δυνατότητα παροχής υπηρεσιών Διαδικτύου, τότε αυτόματα όλοι οι πελάτες μπορούν να αποκτήσουν πρόσβαση στον Παγκόσμιο Ιστό.

Δεν είναι όμως πάντα απαραίτητη η ύπαρξη ενός Σημείου Πρόσβασης. Ένα ασύρματο δίκτυο φτιάχνετε το ίδιο εύκολα από υπολογιστές (ή συσκευές) εφοδιασμένες με απλές κάρτες WiFi. Τα δίκτυα αυτά χρησιμοποιούνται συνήθως εκεί που υπάρχει ανάγκη περιστασιακής σύνδεσης δύο ή περισσότερων υπολογιστών, που δεν δικαιολογεί το (σχετικά υψηλό) κόστος ενός Σημείου Πρόσβασης.

Ο Επόπτης του δικτύου οφείλει να 'εφοδιάσει' το δίκτυό του με ένα μοναδικό αριθμό - ταυτότητα, που στην ορολογία των υπολογιστών, καλείται Service Set IDentifier ή συντομότερα SSID. Ο αριθμός - ταυτότητα εκπέμπεται ανά τακτά διαστήματα από το Σημείο Πρόσβασης, επιτρέποντας στους ασύρματους πελάτες να γνωρίζουν το πλήθος των δικτύων που μπορούν να συνδεθούν.



Σχ. 2. Τα ίδιο περιεχόμενα όπως τα κατέγραψε το Kismet.



Σχ. 3. Το όνομα χρήστη και ο κωδικός πρόσβασης ενός λογαριασμού e-mail.

Προστασία

Η προστασία των ασύρματων δικτύων πραγματοποιείται με δύο τρόπους. Ο πρώτος αφορά στον επιλεκτικό περιορισμό και στην απόκρυψη του δικτύου, ενώ ο δεύτερος στην κρυπτογράφηση των διακινούμενων δεδομένων. Ας τους δούμε αναλυτικά.

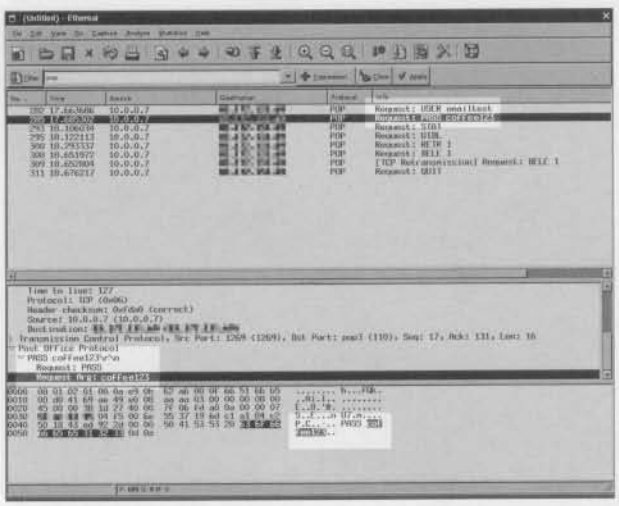
Αν ζητήσουμε από το Σημείο Πρόσβασης τη διακοπή της εκπομπής του αριθμού - ταυτότητας SSID, τότε το δίκτυο μένει 'αόρατο' σε όλους τους 'ασύρματους πελάτες του δικτύου. Μόνο όσοι από αυτούς γνωρίζουν εκ των προτέρων το SSID μπορούν να αποκτήσουν πρόσβαση στο δίκτυο. Επιπρόσθετα, το ίδιο το Σημείο Πρόσβασης μπορεί να αρνηθεί τις υπηρεσίες του σε έναν ή περισσότερους χρήστες ελέγχοντας τον αριθμό MAC της κάρτας δικτύου που χρησιμοποιούν.

Οι παραπάνω τακτικές όμως, κάθε άλλο παρά επαρκώς ασφαλείς μπορούν να θεωρηθούν. Μια άλλη, περισσότερο αποδοτική τακτική, επιτρέπει σε όλους την πρόσβαση, μόνο που για να έχουν νόημα αυτά που 'βλέπουν' στις οθόνες τους θα πρέπει να διαθέτουν το κατάλληλο 'κλειδί'. Η μέθοδος κρυπτογράφησης WEP (Wired Equivalent Privacy) φροντίζει να κωδικοποιεί όλα τα διακινούμενα δεδομένα με τη βοήθεια κλειδιών, η άγνοια των οποίων οδηγεί στη λήψη ακατάληπτων μηνυμάτων.

Η κατακλυσμιαία αύξηση των δικτύων WiFi, όπως είπαμε και προηγουμένως, οφείλεται στις ευκολίες που παρέχουν. Τις περισσότερες φορές αρκεί να ανοίξουμε το κουτί με το δικτυακό εξοπλισμό, να τοποθετήσουμε τις επιμέρους μονάδες στους υπολογιστές και να αφήσουμε το λογισμικό να κάνει όλα τα υπόλοιπα. Η ευκολία και η άνεση όμως, έρχεται σε άμεση σύγκρουση με την ασφάλεια. Οι εταιρίες κατασκευής δικτυακού εξοπλισμού προκειμένου να εξασφαλίσουν την γρηγορότερη και εντυπωσιακότερη λειτουργία του δικτύου, αφήνουν επίτηδες 'ανοικτές όλες τις πόρτες' κάνοντας το ευάλωτο σε εισβολές. Είναι δική μας υποχρέωση να προστατεύσουμε το δίκτυό μας!

Η απότομη αύξηση των ασύρματων δικτύων

Όταν πριν από μερικά χρόνια ο συγγραφέας του άρθρου έκανε μια βόλτα με το φορητό του στα κανάλια του Άμστερνταμ, ανακάλυψε δεκάδες ασύρματα δίκτυα στα οποία κατάφερε, χωρίς ιδιαίτερο κόπο, να συνδεθεί. Σήμερα, μια παρόμοια βόλτα φέρνει στην επιφάνεια αρκετές εκατοντάδες δίκτυα WiFi αποδεικνύοντας τη ραγδαία αύξηση των δικτύων αυτού του τύπου.



Σχ. 4. Τα ίδια στοιχεία όπως εμφανίζονται μέσα στο αρχείο καταγραφής.

Ανεξάρτητα όμως από το πόσο πολλά ή λίγα είναι σήμερα τα εγκαταστημένα δίκτυα, ο λόγος των απροστάτευτων σε σχέση με τα προστατευμένα μένει πάντα ο ίδιος (1:1 περίπου). Το ποσοστό αυτό προσδιορίζει χωρίς περιθώρια λάθους το πόση σημασία δίνουν στην ασφάλεια οι χρήστες των ασύρματων δικτύων.

Πληροφορίες από τον αέρα

Δύο είναι οι σημαντικότεροι από τους λόγους που ένας εισβολέας 'επιτίθεται' σε ένα απροστάτευτο ασύρματο δίκτυο. Ο πρώτος, και προφανέστερος, είναι η απόκτηση (τζάμπα) πρόσβασης στο Διαδίκτυο, χωρίς αυτό να αποκλείει το 'ψαχούλεμα' των πόρων του δικτύου. Ο δεύτερος, αν και λιγότερο προφανής, είναι το ίδιο ενοχλητικός και επικίνδυνος: η υποκλοπή ευαίσθητων πληροφοριών (π.χ. ονομάτων χρηστών και κωδικών πρόσβασης e-mail) ή ακόμα και η παρακολούθηση ολόκληρων συζητήσεων που πραγματοποιούνται μέσω του MSN. Τους εισβολείς της πρώτης κατηγορίας είναι σχετικά εύκολο να τους εντοπίσουμε και να τους εκδιώξουμε. Για τους εισβολείς της δεύτερης τα πράγματα είναι δυσκολότερα, αφού κανείς δεν μπορεί να απαγορεύσει στα ηλεκτρομαγνητικά κύματα που μεταφέρουν τα δεδομένα του δικτύου να φθάσουν και στους δικούς τους υπολογιστές - δέκτες. Μια τέτοια εισβολή, ονομάζεται από τους ειδικούς των ασύρματων δικτύων 'Παθητική Επίθεση' (Passive Attack).

Και με τα προστατευμένα, όμως, δίκτυα τα πράγματα δεν είναι τόσο καλά όσο θα θέλαμε. Υπάρχει φυσικά η κρυπτογράφηση WEP που κάνει τα δεδομένα να μοιάζουν με ένα κακόγουστο συρφετό χαρακτήρων σε όποιον δεν έχει το κλειδί, αλλά πόσο εύκολα μπορεί ένας εισβολέας να αποκτήσει ένα τέτοιο κλειδί; Κάθε ένας χρήστης του δικτύου δικαιούται να ζητήσει (και να λάβει) ένα κλειδί για να αποκτήσει πρόσβαση στις επιθυμητές υπηρεσίες. Το κακό είναι ότι το ίδιο κλειδί, δίδεται και σε όλους τους άλλους πελάτες του δικτύου για τον ίδιο ακριβώς σκοπό. Μήπως λοιπόν είναι πολύ πιο εύκολο απ' ότι φαντάζεται κάποιος, ένας πελάτης να 'στήνει αυτί' στις δραστηριότητες του άλλου;

Παθητική επίθεση

Λίγες παραγράφους πιο πάνω αναφέραμε πως κάθε μια κάρτα δικτύου χαρακτηρίζεται από ένα μοναδικό αριθμό - ταυτότητα, γνωστό σαν MAC. Το ίδιο ισχύει και για κάθε μια κάρτα ασύρματης δικτύωσης WiFi. Τα δεδομένα που μετακινούνται μέσα από ένα ασύρματο δίκτυο είναι εκ των προτέ-

ρων 'σπασμένα' σε πακέτα bytes, κάθε ένα από τα οποία συνοδεύεται από τους αριθμούς MAC του πομπού (αποστολέα) και του επιθυμητού δέκτη (παραλήπτη). Τα δεδομένα σίγουρα εκπέμπονται από έναν πομπό, δεν ισχύει όμως το ίδιο και για το δέκτη που τα λαμβάνει. Αναμφισβήτητα το κάθε ένα πακέτο συνοδεύεται από την διεύθυνση MAC του επιθυμητού δέκτη, κανείς όμως δεν μπορεί να εμποδίσει και τους υπόλοιπους υπολογιστές - δέκτες που βρίσκονται εντός εμβέλειας να το λάβουν και, ενδεχομένως, να το καταγράψουν. Και αυτό πράγματι συμβαίνει. Φυσικά, μόλις αντιληφθούν ότι δεν αφορά τους ίδιους, το απορρίπτουν, γεγονός που μας κάνει να πιστεύουμε πως, πρακτικά, κάθε ένα μήνυμα λαμβάνεται μόνο από τον επιθυμητό υπολογιστή - δέκτη.

Είναι πολύ εύκολο να επέμβουμε στο λογισμικό μιας κάρτας ασύρματου δικτύου και να την κάνουμε λιγότερο 'διακριτική' στα μηνύματα που φτάνουν στην κεραία της. Ο παραπάνω τρόπος 'αδιάκριτης' λειτουργίας είναι γνωστός με το όνομα 'Monitor mode' (Λειτουργία Παρακολούθησης) και υποστηρίζεται από όλες τις κάρτες ασύρματης δικτύωσης. Σύμφωνα με αυτόν, το λογισμικό αποθηκεύει στον σκληρό δίσκο όλα τα πακέτα που συλλαμβάνει η κάρτα WiFi, επιτρέποντας την κατοπινή επεξεργασία τους.

Το λογισμικό

Το καλύτερο δωρεάν διανεμόμενο λογισμικό 'τρέχει' σε λειτουργικό Linux και ονομάζεται Kismet [1]. Ο σκοπός που γράφτηκε ήταν η παρακολούθηση της κίνησης των δικτύων WiFi και γι' αυτό το λόγο, ακόμα και τώρα, αρκετές από τις λειτουργίες βρίσκουν εφαρμογή μόνο σε δίκτυα αυτού του τύπου. Μπορεί π.χ. να εργαστεί στον τρόπο λειτουργίας 'Μεταπήδησης Καναλιών' (Channel Hopping), αναγκάζοντας το δέκτη της κάρτας WiFi να 'ακούει' διαδοχικά το κάθε ένα από τα 13 κανάλια του δικτύου, με ρυθμό 10 μεταπηδήσεων ανά δευτερόλεπτο. Με αυτόν τον τρόπο, σε οποιοδήποτε κανάλι και αν γίνει 'συνομιλία', το Kismet είναι βέβαιο πως θα την εντοπίσει. Το ίδιο πρόγραμμα είναι ακόμα σε θέση να ανιχνεύει κρυμμένα δίκτυα, αναλύοντας απλώς το περιεχόμενο των πακέτων που λαμβάνει. Ανεξάρτητα, λοιπόν, του αν ένα Σημείο Πρόσβασης εκπέμπει ή όχι τον αριθμό SSID είναι το ίδιο ευάλωτο στις διερευνητικές ικανότητες του Kismet.

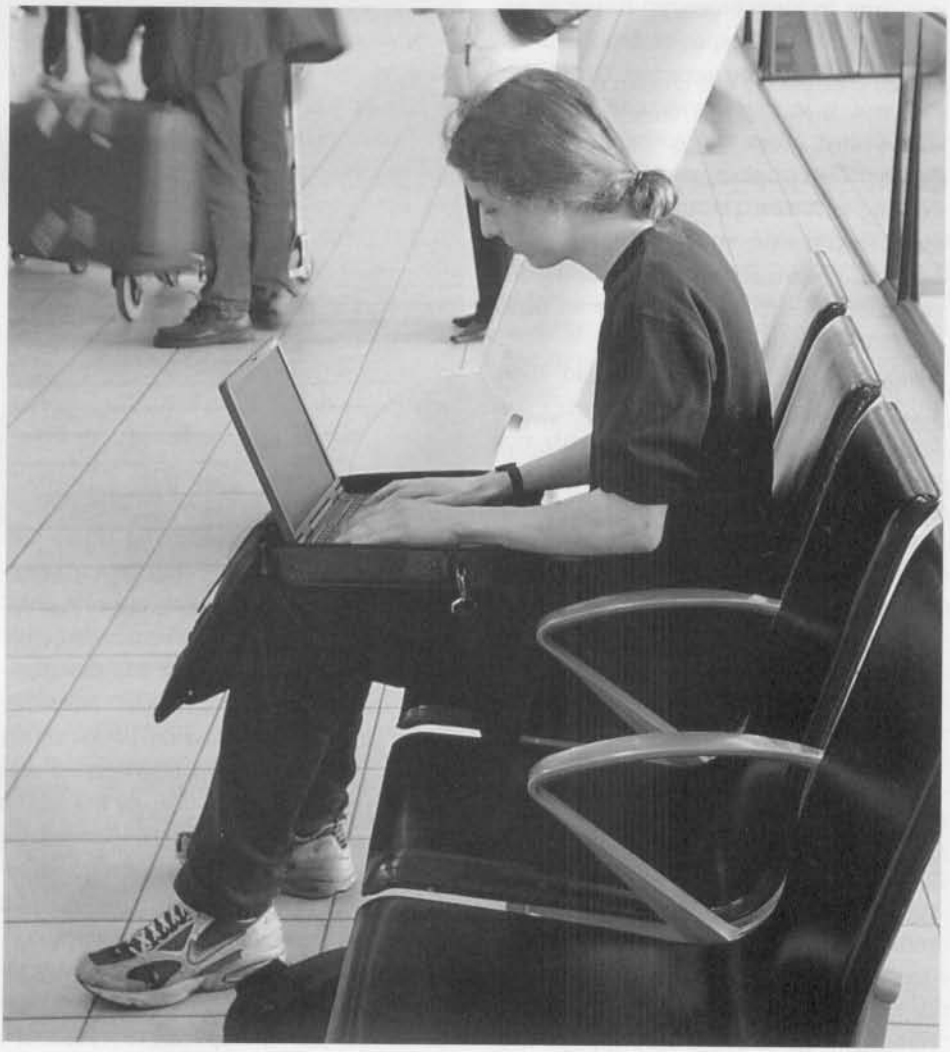
Βέβαια, τις περισσότερες φορές η κίνηση ενός ασύρματου δικτύου είναι τόσο μεγάλη που τα περιεχόμενα των πακέτων εμφανίζονται με τέτοιους ρυθμούς στην οθόνη, που το μάτι αδυνατεί να συλλάβει. Και εδώ όμως οι δημιουργεί του Kismet φρόντισαν να δώσουν λύση. Όλα τα πακέτα καταγράφονται στο σκληρό δίσκο του υπολογιστή με μορφή αρχείου καταγραφής (log file), κάνοντας δυνατή τη μετέπειτα επεξεργασία τους με τη βοήθεια ειδικών προγραμμάτων.

Ένα από τα καλύτερα και δωρεάν διανεμόμενο πρόγραμμα της παραπάνω κατηγορίας είναι το Ethereal [2], που τρέχει' το ίδιο καλά και σε Linux και σε Windows. Κύρια εργασία του είναι η ανάλυση αρχείων καταγραφής, δημιουργημένων από το Kismet ή από άλλα συναφή προγράμματα, με σκοπό την αναζήτηση των πακέτων που περιέχουν στοιχεία λογαριασμών e-mail, συζητήσεις MSN κ.α. Όλα τα παραπάνω πραγματοποιούνται με τη βοήθεια ειδικών φίλτρων κατά τη διάρκεια της ανάλυσης του αρχείου καταγραφής.

Στην πράξη

Θα ήταν παράλειψη μας, έχοντας γράψει τόσα πράγματα για το WiFi, να μην σπεύσουμε να τα τεκμηριώσουμε. Για το λόγο αυτό στήσαμε μια υποτυπώδη διάταξη μετρήσεων, αποτελούμενη από δύο φορητούς υπολογιστές. Ο πρώτος συνδεόταν με το Διαδίκτυο μέσω ενός απομακρυσμένου Σημείου Πρόσβασης ενώ ο δεύτερος ήταν ρυθμισμένος ώστε να εργάζεται σε τρόπο Παρακολούθησης (monitor mode). Διαπιστώσαμε εκ των υστέρων, πως όλες οι συνομιλίες MSN που πραγματοποιήσαμε με τον πρώτο φορητό είχαν αποθηκευτεί στο αρχείο καταγραφής του Kismet που 'έτρεχε' στο δεύτερο φορητό. Οι αποδείξεις φαίνονται στα **σχ. 1** και **σχ. 2**.

Μια δεύτερη δοκιμή που κάναμε με την ίδια διάταξη υπολογιστών αφορούσε στην ασφάλεια των διακινούμενων e-mail. Χωρίς να πούμε τίποτα για τους σκοπούς μας,



ζητήσαμε από ένα ανύποπτο συνεργάτη μας να 'πάρει' τα e-mail του χρησιμοποιώντας τον πρώτο φορητό. Ο δεύτερος, κατά τα γνωστά, κατέγραψε όλη την κίνηση. Όταν αργότερα αναλύσαμε το αρχείο που καταγράψαμε, μέσω του φίλτρου POP3, είδαμε κυριολεκτικά τα πάντα: το όνομα χρήστη, τον κωδικό πρόσβασης και φυσικά τα περιεχόμενα των μηνυμάτων του. Και όλα αυτά μέσα σε μερικά δευτερόλεπτα. Τα **σχ. 3** και **σχ. 4** επιβεβαιώνουν του λόγου το αληθές.

Κατά τη διάρκεια των πειραμάτων μας αποδείχθηκε και κάτι ακόμα, όχι υποχρεωτικά καλό ή κακό. Από το αρχείο καταγραφής του Kismet είχαν ξεφύγει μερικά πακέτα! Αναζητώντας την αιτία, επιβεβαιώσαμε ότι όλες οι μεταδόσεις δεδομένων μεταξύ του πρώτου φορητού και του Σημείου Πρόσβασης πραγματοποιούνταν μέσα από ένα μόνο κανάλι, ενώ ο δεύτερος φορητός 'άκουγε' και τα 13 κανάλια που υποστηρίζει δυνητικά το δίκτυο. Αυτό είχε σαν συνέπεια την αδυναμία καταγραφής δεδομένων όταν το Kismet 'άκουγε' εκείνα τα κανάλια που δεν μετέφεραν τα δεδομένα που διακινούσε ο πρώτος φορητός. Όπως αποδείχθηκε, η λειτουργία 'Μεταπήδησης Καναλιών' είναι εξαιρετικά χρήσιμη όταν αναζητούμε δίκτυα, αλλά μάλλον άβολη όταν έχοντας εντοπίσει ένα από αυτά, θέλουμε να καταγράψουμε την κίνησή του. Αυτό οφείλετε στο ότι μόνο το 1/13 του συνολικού χρόνου λειτουργίας του Kismet αφιερώνεται στο επιθυμητό δίκτυο.

Υπάρχει, όμως, και για αυτό μια λύση. Έχοντας ξεκαθαρίσει ποιο δίκτυο μας ενδιαφέρει και γνωρίζοντας το κανάλι που χρησιμοποιεί, μπορούμε να πούμε στο 'Kismet' να παρακολουθεί μόνο αυτό! Αρκεί να επιλέξουμε το κανάλι και να πιέσουμε Shift+L. Για όλο το χρονικό διάστημα που θα ακολουθήσει μέχρι να πιέσουμε Shift + H, το Kismet θα παρακολουθεί μόνο το συγκεκριμένο κανάλι. Αμέσως μετά θα ξαναπεράσει στην παρακολούθηση όλων των ασύρματων φορέων.

Μια βόλτα στην πόλη

Ας ξαναγυρίσουμε όμως και πάλι στον πραγματικό κόσμο. Εφοδιασμένοι με ένα τυπικό εξοπλισμό δικτυακού ωτακουστή (μια τσάντα με ένα φορητό) ξεκινήσαμε τη βόλτα μας στην πόλη. Τα δεδομένα που αλιεύσαμε ήταν πολλά και διαφορετικά. Τα Σημεία Πρόσβασης με τα οποία συνδεθήκαμε ήταν αρκετές εκατοντάδες, εκ των οποίων τα μισά δεν είχαν καμία απολύτως προστασία. Συνειδητοποιείτε, χωρίς δεύτερη κουβέντα, τον όγκο των αφύλακτων προσωπικών δεδομένων που έκοβε βόλτες στον αέρα. Επιχειρώντας μια σύντομη ανάλυσή τους διαπιστώσαμε πως προερχόντουσαν από περιηγήσεις στο Διαδίκτυο (HTTP), από την ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου (POP3 και SMTP), όπως επίσης και από ατέλειωτες συζητήσεις μέσω του MSN. Αυτό βέβαια που είχε το μεγαλύτερο ενδιαφέρον δεν ήταν ο ατέλειωτος κατάλογος των δικτυακών τόπων που επισκέπτονταν οι διάφοροι χρήστες, αλλά η κίνηση του ηλεκτρονικού ταχυδρομείου τους. Και αυτό όχι τόσο για το περιεχόμενο των μηνυμάτων τους, όσο για την σκανδαλιστική δημοσιοποίηση των ονομάτων χρήστη και των κωδικών πρόσβασης, που φιγουράριζαν φαρδιά - πλατιά στην οθόνη του φορητού μας. Το ίδιο ενδιαφέρον θα έκρινε κάποιος και το περιεχόμενο των συζητήσεων MSN, αν το αντικείμενο τους άγγιζε το δικό του πεδίο ενδιαφερόντων.

Για να επιβεβαιώσουμε όμως την (αν)ασφάλεια των ασύρματων δικτύων έπρεπε να έχουμε ένα πληρέστερο στατιστικό δείγμα. Έτσι λοιπόν, ορίσαμε σαν επόμενο στόχο μας την αίθουσα αναμονής των επιβατών της θέσης Bussiness του αεροδρομίου Schiphol του Άμστερνταμ. Οι επιχειρηματίες φαίνεται να έχουν τα δικά τους ωράρια και συνήθειες μιας που ο 'αέρας' ήταν ανεξήγητα σιωπηλός. Το ίδιο σιωπηλά (ή σχεδόν σιωπηλά) αποδείχθηκαν και πολλά άλλα σημεία ελεύθερης πρόσβασης στο αεροδρόμιο που επισκεφθήκαμε αμέσως μετά. Ποιος, όμως, ήταν εκείνος ο χρήστης με το όνομα 'Butch102' που έστειλε το μήνυμα 'μόλις βρω μια άλλη εταιρία θα φύγω από αυτή που είμαι τώρα'; Είχε πράγματι σκοπό να παραιτηθεί ή εννοούσε κάτι άλλο; Μετά από μια μικρή έρευνα ανακαλύψαμε πως ο 'Butch102' ήταν ένας από τους πολλούς παίκτες του 'EVE Online' που περνούσε ευχάριστα την ώρα του μπροστά από τον υπολογιστή του. Το συμπέρασμα από όλα τα παραπάνω ήταν πως, αν θέλαμε να 'κρυφακούσουμε' τις ασύρματες συνομιλίες των επιχειρηματιών και να μάθουμε περισσότερο για τα παιγνίδια που παίζουν, θα έπρεπε να έχουμε έρθει λίγο νωρίτερα.

Επόμενος σταθμός μας ήταν τα εστιατόρια και οι καφετέριες των αριστοκρατικών συνοικιών του Άμστερνταμ, την ώρα του μεσημεριανού φαγητού. Σε μια από τις πιο 'γεμάτες' καφετέριες, οι θαμώνες συνομιλούσαν μεγαλόφωνα μεταξύ τους, αλλά κανείς τους δεν ασχολιόταν με το Διαδίκτυο. Απογοητευθήκαμε διαπιστώνοντας πως αν θέλαμε να μάθουμε κάτι από τις δραστηριότητες της 'καλής κοινωνίας' θα ήταν καλύτερο αντί να κοιτάμε την οθόνη του φορητού μας, να (κρυφ)ακούμε απλώς τις συνομιλίες στα γειτονικά τραπέζια.

Στο δρόμο του γυρισμού εντοπίσαμε, τυχαία, έντονη δικτυακή δραστηριότητα έξω από μια καφετερία. Και εκεί όπως προηγουμένως, τα πακέτα που λαμβάναμε αφορούσαν συζητήσεις MSN και περιήγηση δικτυακών σελίδων.

Μη ψάχνετε λοιπόν να βρείτε 'μυστικά' σε εξεζητημένα μέρη. Οι γειτονιές της πόλης έχουν πάντα την περισσότερη κίνηση. Όλες σχεδόν οι οικογένειες που διαθέτουν συστήματα WiFi είναι βέβαιο πως θα παίρνουν το ταχυδρομείο τους από τον αέρα.

Δοκιμάστε και εσείς

Αν οι απόψεις σας σχετικά με την πειθαρχία και το σεβασμό στους νόμους είναι μάλλον χαλαρές, τότε μπορείτε να δοκιμάσετε να δικτυωθείτε κρυφά με τους υπολογιστές των γειτόνων σας. Για να καταγράψετε τα πακέτα που ανταλλάσσουν μεταξύ τους ή με το Διαδίκτυο, θα χρειαστείτε έναν υπολογιστή φορτωμένο με Linux, που θα 'τρέχει' το Kismet και το Ethereal. Για τους αναγνώστες που δεν είναι εξοικειωμένοι με την εγκατάσταση του Linux, υπάρχει πάντα η λύση της εκτέλεσης του λειτουργικού κατ' ευθείαν από ένα CD. Αναζητήστε λοιπόν την διανομή Auditor [3], 'κατεβάστε' το αρχείο που την περιέχει, αποσυμπιέστε την (μέσω του WinZip) και 'κάψτε' την σε ένα CD (μέσω του Nero, επιλογές: 'File' / 'Burn Image'). Στη συνέχεια τοποθετήστε το CD στον αντίστοιχο μηχανισμό του φορητού σας, μπείτε μέσα στο BIOS Setup για να ορίσετε σαν πρώτο μηχανισμό εκκίνησης το CD-ROM και αφήστε τον φορητο σας να ξεκινήσει. Το λειτουργικό που θα εμφανιστεί μπροστά σας θα είναι το Linux.

(050083-1)

Χρήσιμες διευθύνσεις:

[1] www.kismetwireless.net
[2] www.ethereal.com
[3] www.remote-exploit.org