ΤΕΧΝΙΚΟ ΑΡΘΡΟ ΤΩΝ ΛΑΖΑΡΟΥ ΜΕΡΑΚΟΥ ΚΑΙ ΧΡΗΣΤΟΥ ΞΕΝΑΚΗ

Πόσο ασφαλή είναι τα δίκτυα κινητής τηλεφωνίας;

Το σύστημα GSM είναι σήμερα το πιο διαδεδομένο σύστημα κινητής τηλεφωνίας στον κόσμο, με περισσότερους από 1,5 δισεκατομμύριο συνδρομητές σε περισσότερες από 200 χώρες, και η ασφάλειά του αποτελεί σημαντικό ζήτημα.

Ένα ερώτημα που διατυπώνεται συχνά από πολλούς συνδρομητές GSM αφορά στο βαθμό ασφάλειας που προσφέρει το σύστημα στους χρήστες του και στα αδύνατα σημεία του συστήματος που θα μπορούσαν γίνουν αντικείμενο εκμετάλλευσης. Σε αυτό το άρθρο επιχειρούμε να απαντήσουμε στο παραπάνω ερώτημα. Στο σχετικό ενημερωτικό πλαίσιο οι αναγνώστες μπορούν να βρουν μια σύντομη περιγραφή της βασικής αρχιτεκτονικής του συστήματος GSM, ώστε στη συνέχεια να είναι πιο κατανοητή η ανάλυση σχετικά με τις πιθανές επιθέσεις που μπορούν εκμεταλλευτούν τις αδυναμίες του συστήματος.

Ασφάλεια στο δίκτυο GSM

Η ασφάλεια στα δίκτυα κινητών επικοινωνιών απαιτεί το συνυπολογισμό διαφόρων παραγόντων, όπως είναι η ασύρματη πρόσβαση, η κινητικότητα των χρηστών, οι καταγεγραμμένες απειλές ασφάλειας, τα είδη των πληροφοριών που πρέπει να προστατευτούν και η πολυπλοκότητα της αρχιτεκτονικής του δικτύου. Η ασύρματη μετάδοση είναι από τη φύση της περισσότερο ευαίσθητη σε υποκλοπές και απάτες από όσο είναι η ενσύρματη μετάδοση. Η κινητικότητα των χρηστών και η καθολική πρόσβαση στο δίκτυο προκαλούν απειλές κατά της ασφάλειας. Οι διαφορετικοί τύποι των δεδομένων και των πληροφοριών που είτε μεταβιβάζονται μέσα από το κινητό δίκτυο είτε εδρεύουν σε αυτό απαιτούν διαφορετικούς τύπους και επίπεδα προστασίας. Επιπλέον, η σύνθετη τοπολογία του δικτύου και οι ετερογενείς τεχνολογίες που το απαρτίζουν αυξάνουν την ανάγκη για διασφάλιση της αξιοπιστίας.

Το μοντέλο ασφάλειας που χρησιμοποιείται στην τεχνολογία GSM βασίζεται κυρίως σε ένα μυστικό κλειδί (128bit), το Ki, και στους αλγορίθμους A3, A8 και A5. Το κλειδί Ki και οι αλγόριθμοι A3 και A8, που χρησιμοποιούνται για τον έλεγχο της αυθεντικότητας του χρήστη και τη δημιουργία κλειδιών κρυπτογράφησης βρίσκονται στην κάρτα SIM του συνδρομητή και στο AuC του παροχέα στον οποίο είναι εγγεγραμμένος ο χρήστης. Ο αλγόριθμος A5, ο οποίος χρησιμοποιείται για κρυπτογράφηση, υλοποιείται στο MS και στα BTS που εξυπηρετούν το χρήστη. Οι υπηρεσίες ασφάλειας που παρέχει η τεχνολογία GSM είναι οι ακόλουθες:

1. Προστασία της ταυτότητας του συνδρομητή.
2. Έλεγχος της αυθεντικότητας της ταυτότητας του συνδρομητή.
3. Προστασία των δεδομένων του χρήστη και της σηματοδοσίας μεταξύ του MS και του BTS.

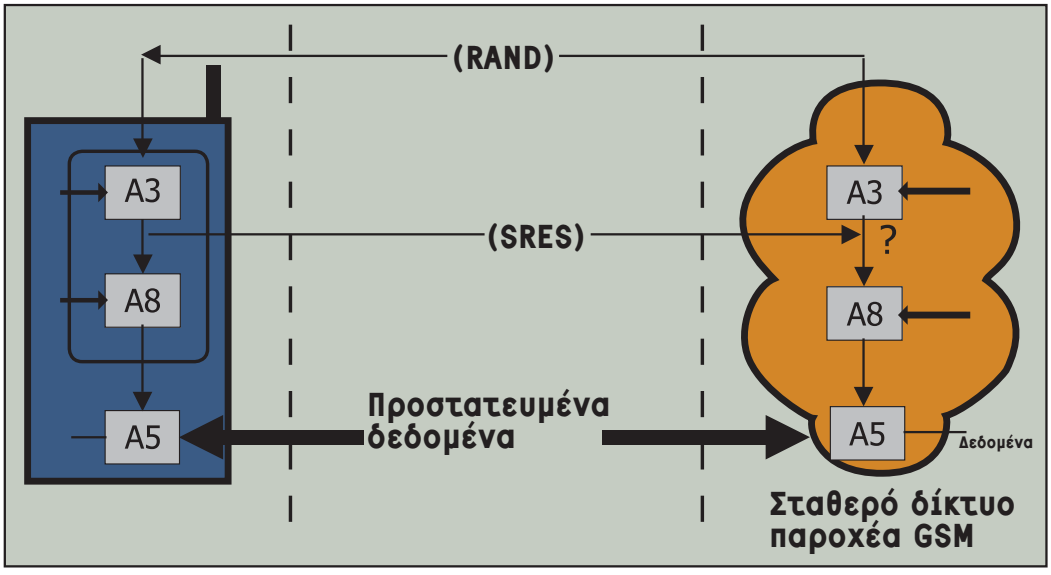
■ Προστασία της ταυτότητας του συνδρομητή

Η προστασία της ταυτότητας του συνδρομητή διασφαλίζει τη μυστικότητα της ταυτότητας IMSI και της θέσης του κινητού χρήστη. Βασίζεται στη χρήση μιας προσωρινής ταυτότητας (TMSI), της οποίας η σχέση με τη μοναδική ταυτότητα IMSI κρατιέται μυστική στον κινητό σταθμό και το δίκτυο. Επίσης, περιλαμβάνει μέτρα τα οποία αποκλείουν τη δυνατότητα να αντληθεί η ταυτότητα του χρήστη, έμμεσα, από την υποκλοπή συγκεκριμένων πληροφοριών στο ασύρματο δίκτυο.

Η προσωρινή ταυτότητα TMSI χρησιμοποιείται για να προσδιορίσει έναν κινητό συνδρομητή στο ευαίσθητο τμήμα του ασύρματου δικτύου. Είναι μια τοπική ταυτότητα και πρέπει να συνοδεύεται από την ταυτότητα της περιοχής δρομολόγησης (Routing Area Identity - RAI) για την αποφυγή πιθανών ασαφειών. Η ανάθεση μιας προσωρινής ταυτότητας TMSI γίνεται από το δίκτυο και μεταφέρεται κρυπτογραφημένη στον κινητό σταθμό. Ο τελευταίος αποθηκεύει την τρέχουσα TMSI μαζί με την ταυτότητα της περιοχής RAI σε μια αμετάβλητη μνήμη, ώστε να μη χάνονται όταν κλείνει το τερματικό. Για να αντιμετωπιστούν πιθανά προβλήματα δυσλειτουργίας, π.χ. από μια αποτυχία του λογισμικού, το δίκτυο έχει τη δυνατότητα να απαιτήσει τον προσδιορισμό ενός κινητού σταθμού με βάση τη μόνιμη ταυτότητα IMSI. Η διαδικασία αυτή αποτελεί παραβίαση των κανόνων εξυπηρέτησης και ασφάλειας και πρέπει να χρησιμοποιείται σε εξαιρετικές περιπτώσεις μόνο όταν είναι απολύτως αναγκαία.

■ Έλεγχος της αυθεντικότητας της ταυτότητας του χρήστη

Ένας συνδρομητής GSM πρέπει να αποδείξει την ταυτότητά του, προκειμένου να του επιτραπεί η πρόσβαση στο δίκτυο. Ο έλεγχος της αυθεντικότητας προστατεύει το δίκτυο από ενδεχόμενη απατηλή χρήση και εξασφαλίζει την ορθή τιμολόγηση. Το δίκτυο διανέμει πρώτα στον κινητό σταθμό έναν τυχαίο αριθμό RAND (βλ. σχήμα 2), ο οποίος είναι αποτέλεσμα μιας γεννήτριας μη προβλέψιμων, τυχαίων αριθμών. Ο κινητός σταθμός κρυπτογραφεί τον αριθμό RAND χρησιμοποιώντας τον αλγόριθμο A3 και το κλειδί Ki. Στη συνέχεια στέλνει την υπογεγραμμένη απάντηση (signed response - SRES) πίσω στο δίκτυο. Με βάση την απάντηση, το δίκτυο ε-



Σχήμα 2: Διαδικασία ελέγχου της αυθεντικότητας του χρήστη

λέγχει αν ο κινητός σταθμός έχει το σωστό κλειδί Ki. Μόλις διαπιστωθεί η κατοχή του κλειδιού, ο συνδρομητής αναγνωρίζεται ως εξουσιοδοτημένος χρήστης, διαφορετικά το δίκτυο απορρίπτει την αίτηση πρόσβασης. Τμήμα του κρυπτογραφημένου αποτελέσματος (από τον αλγόριθμο A3) μαζί με το κλειδί Ki χρησιμοποιούνται από τον αλγόριθμο A8 για την παραγωγή του κλειδιού κρυπτογράφησης Kc.

■ **Προστασία των δεδομένων του χρήστη και της σηματοδοσίας**

Η προστασία των δεδομένων του χρήστη και της σηματοδοσίας πάνω από το ευαίσθητο τμήμα του ασύρματου δικτύου (μεταξύ του MS και του BTS) βασίζεται στον αλγόριθμο κρυπτογράφησης A5. Ο A5 είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ροής (symmetric stream cipher algorithm), που επιλέγεται κάθε φορά από το σύνολο των αλγορίθμων που υποστηρίζει ο κινητός σταθμός. Ο κινητός σταθμός διαφημίζει στο δίκτυο τους αλγορίθμους που υποστηρίζει, κατά τη διάρκεια της διαδικασίας ελέγχου της αυθεντικότητας της ταυτότητας του χρήστη. Δεδομένου του ότι ο αλγόριθμος A5 απαιτεί σχετικά υψηλές δυνατότητες επεξεργασίας, η κινητή συσκευή (όχι η κάρτα SIM) εκτελεί την κρυπτογράφηση χρησιμοποιώντας το κλειδί Kc. Το κλειδί αυτό έχει μήκος 64bits, παράγεται κατά τη διαδικασία ελέγχου της αυθεντικότητας της ταυτότητας του χρήστη και δεν μεταφέρεται ποτέ πάνω από την ασύρματη διεπαφή.

Πιθανές επιθέσεις στο κινητό δίκτυο GSM

Όπως αναφέρθηκε προηγουμένως, η ασφάλεια του συστήματος GSM βασίζεται στο κλειδί Ki και στους αλγορίθμους A3, A8 και A5. Για την υλοποίηση των αλγορίθμων A3 και A8 η πλειονότητα των παροχέων χρησιμοποιεί τον αλγόριθμο COMP 128, ο οποίος κρατήθηκε μυστικός. Παρόμοια, οι υλοποιήσεις του A5 (A5/1 "ισχυρή" έκδοση του αλγορίθμου και A5/2 "ασθενέστερη" έκδοση, η οποία χρησιμοποιείται στις περισσότερες χώρες του κόσμου) δεν δημοσιοποιήθηκαν. Ως συνέπεια, η επιστημονική κοινότητα δεν μελέτησε τους παραπάνω αλγορίθμους, ώστε να αποκαλυφθούν πιθανές ατέλειές τους. Έτσι, η ασφάλεια στο GSM βασίστηκε κυρίως στη μυστικότητά τους και στο μέγεθος των κλειδιών που επιλέχθηκαν, τα οποία με βάση την τότε διαθέσιμη υπολογιστική ισχύ (τέλη του 1980) κρίθηκαν ικανοποιητικά. Όμως, όπως ήταν αναμενόμενο, οι αλγόριθμοι τελικά διέρρευσαν, ενώ παράλληλα η διαθέσιμη υπολογιστική ισχύς έχει αυξηθεί κατά αρκετές τάξεις μεγέθους. Για τους λόγους αυτούς, η βάση ασφάλειας του GSM έχει εξασθενήσει σημαντικά. Στη συνέχεια, θα αναφερθούμε στις επιθέσεις που μπορούν να εκδηλωθούν εναντίον του συστήματος GSM, οι οποίες εκμεταλλεύονται τις αδυναμίες ασφάλειας του συστήματος.

■ **Κλωνοποίηση της κάρτας SIM**

Από τα παραπάνω συμπεραίνουμε ότι η ασφάλεια στο σύστημα GSM βασίζεται σε μεγάλο βαθμό στο μυστικό κλειδί Ki. Στην περίπτωση που κάποιος επιτιθέμενος αποκτήσει αυτό το κλειδί, μπορεί να υποκλέψει παθητικά τα δεδομένα που μεταφέρονται μεταξύ του κινητού σταθμού MS και του σταθμού βάσης BTS ή μπορεί να δημιουργήσει μια κάρτα αντίγραφο της αρχικής ("κλώνο"). Έχοντας μια κάρτα κλώνο, ο επιτιθέμενος μπορεί να συμμετέχει σε συναλλαγές οι οποίες θα χρεώνονται στο νόμιμο συνδρομητή. Η μόνη δικλίδα ασφάλειας που παρέχει το σύστημα GSM είναι ότι δεν επιτρέπει την πρόσβαση του ίδιου χρήστη δύο φορές, ταυτόχρονα. Άρα, θύτης και θύμα δεν μπορούν να είναι ενεργοί συγχρόνως. Στην περίπτωση που κάτι τέτοιο συμβεί, ο λογαριασμός κλειδώνεται και ειδοποιείται ο νόμιμος χρήστης.

■ **Ανάκτηση του κλειδιού Ki**

Το κλειδί Ki κάθε συνδρομητή GSM βρίσκεται αποθηκευμένο σε δύο σημεία: στην κάρτα SIM της συσκευής του και στο HLR του παροχέα στον οποίο είναι εγγεγραμμένος ο χρήστης. Η κάρτα SIM δεν παρέχει κάποιον άμεσο τρόπο ανάκτησης του κλειδιού Ki, ακόμα και σε κάποιον που έχει φυσική πρόσβαση σε αυτή. Παρ' όλα αυτά όμως, ερευνητές ανακάλυψαν μεθόδους με τις οποίες ένας κακόβουλος χρήστης μπορεί να ανακτήσει το κλειδί Ki είτε έχοντας στην κατοχή του μια κάρτα SIM είτε όχι. Αυτές οι μέθοδοι εκμεταλλεύονται κάποιες αδυναμίες του αλγορίθμου COMP 128, ο οποίος χρησιμοποιείται για την υλοποί-

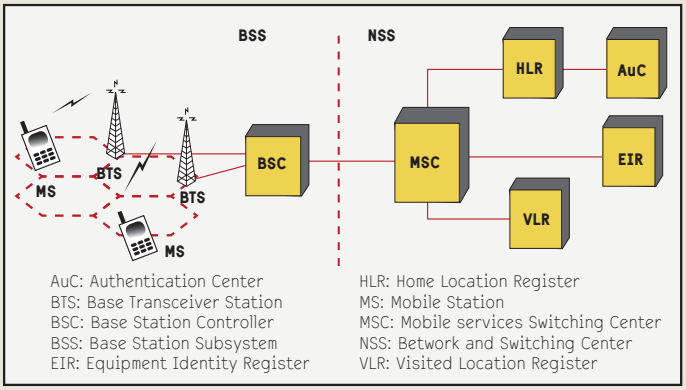
Αρχιτεκτονική του δικτύου GSM

ΤΗΝ ΑΡΧΙΤΕΚΤΟΝΙΚΗ του δικτύου GSM (βλ. σχήμα 1) απαρτίζουν τρία βασικά λειτουργικά μέρη: ο κινητός σταθμός (Mobile Station, MS), το υποσύστημα σταθμού βάσης (Base Station Subsystem, BSS) και το υποσύστημα δικτύου και μεταγωγής (Network and Switching Subsystem, NSS).

Ο κινητός σταθμός MS αποτελεί την τερματική συσκευή του χρήστη και περιλαμβάνει μία αποσπώμενη έξυπνη κάρτα (smart card), η οποία ονομάζεται κάρτα SIM (Subscriber Identity Module). Η κάρτα SIM αποθηκεύει τη διεθνή ταυτότητα του συνδρομητή (International Mobile Subscriber Identity, IMSI), το μυστικό κλειδί Ki στο οποίο βασίζονται η διαδικασία ελέγχου της αυθεντικότητας του κινητού χρήστη και η κρυπτογράφηση των δεδομένων, καθώς και τους αλγορίθμους A3 και A8 που σχετίζονται με τις παραπάνω διαδικασίες. Εκτός από τα παραπάνω, η κάρτα SIM αποθηκεύει την προσωρινή ταυτότητα του χρήστη (Temporal Mobile Subscriber Identity, TMSI), η οποία αντικαθιστά το IMSI, ώστε αυτό να μην εκπέμπεται στον αέρα αποκαλύπτοντας την πραγματική ταυτότητα του χρήστη.

Ο ρόλος του BSS είναι ο έλεγχος της ασύρματης ζεύξης με τους συνδρομητές και η σύνδεσή τους με το σταθερό δίκτυο του παροχέα. Αποτελείται από κάποιους σταθμούς εκπομπής/λήψης (Base Transceiver Stations, BTSs) και τον ελεγκτή του σταθμού (Base Station Controller, BSC), ο οποίος διαχειρίζεται θέματα διασύνδεσης των συνδρομητών με τα BTS που ελέγχει, όπως, για παράδειγμα, το πότε ένας χρήστης πρέπει να εξυπηρετηθεί από άλλο BTS και ποιο κανάλι θα χρησιμοποιήσει.

Στο σταθερό τμήμα του δικτύου (NSS) βρίσκεται το Mobile services Switching Center (MSC), το οποίο είναι υπεύθυνο για τις λειτουργίες μεταγωγής στο δίκτυο και την επικοινωνία με τα υπόλοιπα τηλεφωνικά δίκτυα (σταθερά ή κινητά). Το MSC υλοποιεί βασικές λειτουργίες του δικτύου, όπως ο έλεγχος της αυθεντικότητας της ταυτότητας των χρηστών και η δρομολόγηση των κλήσεων. Άλλες οντότητες που απαρτίζουν το NSS και παρέχουν πληροφορίες στο MSC είναι το Authentication Center (AuC), το Home Location Register (HLR), το Visitor Location Register (VLR) και το Equipment Identity Register (EIR). Το AuC διατηρεί πληροφορίες σχετικά με την ταυτότητα των συνδρομητών και παράγει τα κλειδιά ελέγχου αυθεντικότητας και κρυπτογράφησης. Για το λόγο αυτό αποτελεί μία από τις πιο ευαίσθητες οντότητες που απαρτίζουν το NSS από πλευράς ασφάλειας. Το HLR είναι μια βάση δεδομένων που χρησιμοποιείται για τη διαχείριση των πληροφοριών στο κινητό δίκτυο. Όλα τα μόνιμα στοιχεία των συνδρομητών αποθηκεύονται εκεί. Μια εγγραφή του HLR αποτελείται από τρεις τύπους πληροφοριών: πληροφορίες σχετικές με τον κινητό σταθμό, πληροφορίες που αφορούν στη θέση του κινητού, καθώς και πληροφορίες που αναφέρονται στις υπηρεσίες. Το VLR είναι μια βάση δεδομένων της περιοχής που επισκέπτονται οι κινητοί σταθμοί και περιέχει όλα τα στοιχεία ενός χρήστη που απαιτούνται για την παροχή υπηρεσιών. Τέλος, το EIR διατηρεί πληροφορίες ασφάλειας σχετικά με τον εξοπλισμό.



Σχήμα 1: Αρχιτεκτονική του δικτύου GSM

ηση του A3.

Συγκεκριμένα, η πρώτη μέθοδος, η οποία δεν προϋποθέτει την κατοχή της κάρτας SIM, βασίζεται στην τροφοδότηση επιλεγμένων τυχαίων αριθμών RAND (το πλήθος τους ποικίλλει από 11.000 έως 150.000, ανάλογα με την επίθεση) στην κάρτα SIM ενός κινητού χρήστη. Από την επεξεργασία των απαντήσεων που θα αποστείλει η κάρτα SIM (ή το κινητό του χρήστη) στον επιτιθέμενο, εκείνος μπορεί να ανακτήσει το μυστικό κλειδί Ki. Ένας άλλος τύπος επιθέσεων αναφέρεται ως "side-channel attacks" και βασίζεται στην παρατήρηση της εκτέλεσης του αλγορίθμου COMP 128 στην κάρτα SIM. Από την παρατήρηση μπορεί να εξαχθεί χρήσιμη πληροφορία, η οποία τελικά οδηγεί στην ανάκτηση του μυστικού κλειδιού Ki. Μια βελτιωμένη εκδοχή αυτής της επίθεσης ονομάζεται "partitioning attack". Η επίθεση βασίζεται στην παρατήρηση της εκτέλεσης του αλγορίθμου COMP 128, ο οποίος ενεργοποιείται είτε από 1.000 τυχαίους αριθμούς RAND, είτε από 255 επιλεγμένους αριθμούς, είτε από μόνο 8 προσαρμοζόμενους αριθμούς. Πρακτικά αυτό σημαίνει ότι κάποιος που έχει στην κατοχή του την κάρτα SIM ενός χρήστη για περίπου ένα λεπτό μπορεί να κλέψει το μυστικό κλειδί Ki.

Μία επιπλέον αδυναμία του GSM, η οποία μπορεί να οδηγήσει στην ανάκτηση του μυστικού κλειδιού Ki, είναι η ανάγκη γνώσης του κλειδιού από τον παροχέα. Το AuC πρέπει να γνωρίζει τα μυστικά κλειδιά των συνδρομητών του δικτύου, προκειμένου να παράγει τις παραμέτρους ελέγχου της αυθεντικότητας και της κρυπτογράφησης. Εφόσον τα κλειδιά αυτά αποθηκεύονται σε μια βάση δεδομένων του παροχέα, ο επιτιθέμενος θα μπορούσε να έχει πρόσβαση σε αυτά είτε εκ των έσω μέσω κάποιου εργαζομένου στην εταιρεία είτε παραβιάζοντας την ασφάλεια των συστημάτων του παροχέα και αποκτώντας έτσι πρόσβαση στη βάση.

Ο Λάζαρος Μεράκος (merakos@di.uoa.gr) είναι καθηγητής στο τμήμα Πληροφορικής και Τηλεπικοινωνιών και διευθυντής του Εργαστηρίου Δικτύων Επικοινωνιών στο Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών.

■ Ανάκτηση του κλειδιού Kc

Σε άλλη μία μορφή επίθεσης στο σύστημα GSM, ο επιτιθέμενος εκμεταλλεύεται τις αδυναμίες του αλγορίθμου A5 (και των δύο εκδόσεών του A5/1 και A5/2). Με την επίθεση αυτή ο επιτιθέμενος ανακτά το κλειδί κρυπτογράφησης Kc (64bit) και έτσι έχει τη δυνατότητα να υποκλέψει τα δεδομένα του χρήστη που μεταφέρονται στον αέρα για όσο χρόνο ο κινητός συνδρομητής και το δίκτυο χρησιμοποιούν το ίδιο κλειδί κρυπτογράφησης.

■ Επίθεση στο ασύρματο δίκτυο

Υποκλοπή δεδομένων μπορεί να πραγματοποιηθεί και με μια επίθεση τύπου ενδιαμέσου (man-in-the-middle attack). Ο επιτιθέμενος χρησιμοποιεί ένα δικό του BSS, το οποίο υπερκαλύπτει το σήμα του νόμιμου παροχέα και αναγκάζει το τερματικό του θύματος να συνδεθεί με αυτό. Έπειτα, το παράνομο BSS είτε ζητά από το MS να μεταδίδει τα δεδομένα στον αέρα χωρίς κρυπτογράφηση είτε αλλοιώνει τη διαπραγμάτευση του αλγορίθμου κρυπτογράφησης μεταξύ MS και BTS. Επίσης, ο επιτιθέμενος έχει τη δυνατότητα να παρεμβαίνει στην επικοινωνία του θύματος και του νόμιμου δικτύου. Βέβαια, ο επιτιθέμενος πρέπει να παρέχει στο θύμα τις υπηρεσίες που αυτό ζητά (π.χ. την εγκατάσταση της κλήσης) με τη χρήση μιας άλλης συνδρομής με τον παροχέα, πάνω από την οποία θα πραγματοποιηθεί η ζητούμενη υπηρεσία, που ίσως προδώσει την επίθεση.

■ Υποκλοπή δεδομένων στο σταθερό τμήμα του δικτύου

Εκτός από τις επιθέσεις στο ασύρματο τμήμα του δικτύου, υποκλοπές δεδομένων μπορούν να πραγματοποιηθούν και σε άλλα σημεία του δικτύου GSM. Οι προδιαγραφές του συστήματος ορίζουν ότι χρησιμοποιείται κρυπτογράφηση μόνο στο τμήμα μεταξύ του MS και του BTS. Έτσι, στο υπόλοιπο τμήμα του δικτύου η κρυπτογράφηση των δεδομένων επαφίεται στον παροχέα με ό,τι συνέπειες μπορεί να έχει αυτό για την ασφάλειά τους. Το δίκτυο του παροχέα μπορεί να είναι είτε ενσύρματο είτε ασύρματο, και συχνά η κρυπτογράφηση των δεδομένων στα ενσύρματα τμήματα είναι ανύπαρκτη. Για το λόγο αυτό, τα περισσότερα συστήματα υποκλοπών του GSM χρησιμοποιούν τη συγκεκριμένη αδυναμία.

■ Άρνηση εξυπηρέτησης

Ένας άλλος τύπος επίθεσης που μπορεί να πραγματοποιηθεί σε ένα σύστημα GSM αποσκοπεί στην άρνηση παροχής υπηρεσιών (Denial of Service, DoS) σε κάποιο χρήστη. Ο επιτιθέμενος προσπαθεί να διακόψει την επικοινωνία του θύματος με το σύστημα για κάποιο διάστημα. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους. Ο απλούστερος είναι η εκπομπή παρασίτων που θα υπερκαλύψουν το σήμα του παροχέα και θα κάνουν αδύνατη τη χρήση των υπηρεσιών του δικτύου. Τέτοιες συσκευές είναι διαθέσιμες εμπορικά και χρησιμοποιούνται σε δημόσιους χώρους, όπως τα θέατρα, προκειμένου οι συσκευές των θεατών να μην μπορούν να χρησιμοποιηθούν κατά τη διάρκεια της παράστασης. Μια τέτοια επίθεση όμως δύσκολα κατευθύνεται προς συγκεκριμένο χρήστη και γίνεται εύκολα αντιληπτή. Ένας παρόμοιος τρόπος αποκοπής του θύματος από όλες τις υπηρεσίες του δικτύου είναι η χρήση ενός BTS, το οποίο προσποιούμενο το BTS του παροχέα αναγκάζει το θύμα να συνδεθεί σε αυτό, αλλά έπειτα δεν παρέχει καμία υπηρεσία στο θύμα. Ένας ακόμα τρόπος για την επίτευξη του ίδιου στόχου είναι η χρήση ενός MS, το οποίο χρησιμοποιώντας το IMSI του θύματος ζητά από το δίκτυο να διαγραφεί από την κυψέλη στην οποία ανήκει ή ζητά ανανέωση τοποθεσίας σε μια απομακρυσμένη κυψέλη. Και στις δύο περιπτώσεις το MS διαγράφεται από την κυψέλη από την οποία εξυπηρετείται και χάνει πρόσβαση από όλες τις υπηρεσίες.

> **"Ερευνητές έχουν ανακαλύψει μεθόδους με τις οποίες ένας κακόβουλος χρήστης μπορεί να ανακτήσει το κλειδί Ki είτε με είτε χωρίς κάρτα SIM. Πρακτικά, αυτό σημαίνει ότι κάποιος που έχει στην κατοχή του την κάρτα SIM ενός χρήστη για περίπου ένα λεπτό μπορεί να κλέψει το μυστικό κλειδί."**

Ο Χρήστος Ξενάκης (xenakis@di.uoa.gr) είναι διδάκτορας και υπεύθυνος της ερευνητικής ομάδας "Ασφάλεια Δικτύων" του Εργαστηρίου Δικτύων Επικοινωνιών στο Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών.

■ Εντοπισμός θέσης

Στο σύστημα GSM η θέση των συνδρομητών μπορεί να προσδιοριστεί από τους παροχείς με βάση την κυψέλη από την οποία εξυπηρετείται ένας χρήστης και τεχνικές που βασίζονται στην καθυστέρηση διάδοσης του σήματος του τερματικού MS που λαμβάνεται από τους κοντινούς σταθμούς BTS. Ο εντοπισμός της θέσης μπορεί να γίνει με αρκετά μεγάλη ακρίβεια, της τάξης των μερικών δεκάδων μέτρων. Ο εντοπισμός και η παρακολούθηση της θέσης ενός χρήστη είναι προσωπικό δεδομένο, το οποίο ο χρήστης πιθανότατα να μη θέλει να γνωστοποιείται σε τρίτους. Ωστόσο, αν κάποιος έχει πρόσβαση στο σύστημα του παροχέα, είτε εκ των έσω είτε παραβιάζοντας κάποιο λογαριασμό ή υπηρεσία, μπορεί να έχει πρόσβαση σε αυτή την απόρρητη πληροφορία. Μια παρεμφερή πληροφορία, την οποία μπορεί ένας τρίτος να εξάγει από ένα σύστημα GSM, είναι η παρουσία ενός προσώπου σε μια περιοχή, μέσω της ταυτότητας IMSI. Αν και το IMSI στις περισσότερες περιπτώσεις αντικαθίσταται από την προσωρινή ταυτότητα TMSI, το δίκτυο μπορεί να ζητήσει από το τερματικό MS να του αποστείλει το IMSI. Έτσι, ένας επιτιθέμενος, εκμεταλλευόμενος αυτό το χαρακτηριστικό και χρησιμοποιώντας ένα σταθμό βάσης BTS που θα υπερκάλυπτε το σήμα του παροχέα, θα μπορούσε να ανιχνεύσει την παρουσία ενός ατόμου σε κάποια περιοχή, εφόσον το τερματικό του είναι ανοιχτό. CP