Οι ειδικοί συμφωνούν στο γεγονός ότι κανένα «κινητό» δίκτυο δεν μπορεί να είναι απόλυτα ασφαλές

Η ασφάλεια στη δομή και τη λειτουργία των δικτύων κινητής τηλεφωνίας

Των **Χρήστου Ξενάκη** και **Λάζαρου Μεράκου***

Το σύστημα GSM (Global System for Mobile Communications) αποτελεί σήμερα το πιο διαδεδομένο σύστημα κινητής τηλεφωνίας στον κόσμο, με πάνω από 1,5 δισεκατομμύριο συνδρομητές σε περισσότερες από 200 χώρες. Ενα 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.

Η αρχιτεκτονική του δικτύου GSM

Την αρχιτεκτονική του δικτύου GSM 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, η οποία ονομάζεται κάρτα SIM (Subscriber Identity Module). Ο ρόλος του BSS είναι ο έλεγχος της ασύρματης ζεύξης με τους συνδρομητές και η σύνδεσή τους με το σταθερό δίκτυο του παρόχου. Αποτελείται από κάποιους σταθμούς εκπομπής / λήψης (Base Transceiver Stations, BTSs) και τον ελεγκτή του σταθμού (Base Station Controller - BSC). Στο σταθερό τμήμα του δικτύου (NSS) βρίσκεται το Mobile services Switching Center (MSC), το οποίο είναι υπεύθυνο για τις λειτουργίες μεταγωγής στο δίκτυο και για 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. Αλλες οντότητες που απαρτίζουν το NSS και παρέχουν πληροφορίες στο MSC σχετικά με την ταυτότητα των χρηστών και τα κλειδιά που χρησιμοποιούν είναι το Authentication Center (AuC), το Home Location Register (HLR), το Visitor Location Register (VLR) και το Equipment Identity Register (EIR).

Συστήματα ασφάλειας

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

Οι υπηρεσίες ασφάλειας που παρέχει η τεχνολογία GSM είναι: Προστασία της ταυτότητας του συνδρομητή, έλεγχος της αυθεντικότητας της ταυτότητας του συνδρομητή, και προστασία των δεδομένων του χρήστη και της σηματοδοσίας μεταξύ του MS και του BTS.

Η προστασία της ταυτότητας του συνδρομητή διασφαλίζει τη μυστικότητα της ταυτότητας (International Mobile Subscriber Identity - IMSI) και της θέσης του κινητού χρήστη. Βασίζεται στη χρήση μιας προσωρινής ταυτότητας (Temporal Mobile Subscriber Identity - TMSI), η οποία προσδιορίζει έναν κινητό συνδρομητή στο ευαίσθητο τμήμα του ασύρματου δικτύου. Επίσης, περιλαμβάνει μέτρα τα οποία αποκλείουν τη δυνατότητα να αντληθεί η ταυτότητα του χρήστη, έμμεσα, από την υποκλοπή συγκεκριμένων πληροφοριών στο ασύρματο δίκτυο.

Αυθεντικοποίηση

Ένας συνδρομητής GSM πρέπει να αποδείξει την ταυτότητά του (έλεγχος της αυθεντικότητας), προκειμένου να του επιτραπεί η πρόσβαση στο δίκτυο. Το δίκτυο διανέμει πρώτα στο MS έναν τυχαίο αριθμό RAND. Το MS κρυπτογραφεί τον αριθμό χρησιμοποιώντας τον αλγόριθμο A3 και το κλειδί Ki, και στέλνει την υπογεγραμμένη απάντηση πίσω στο δίκτυο. Με βάση αυτή την απάντηση, το δίκτυο ελέγχει εάν 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.

Κατά τη διαδικασία ελέγχου της αυθεντικότητας της ταυτότητας του χρήστη παράγεται, επίσης, το κλειδί κρυπτογράφησης Kc (64 bits). Η κρυπτογράφηση στο δίκτυο GSM προστατεύει τα δεδομένα του χρήστη και την σηματοδοσία πάνω από το ευαίσθητο τμήμα του ασύρματου δικτύου (μεταξύ του MS και του BTS). Βασίζεται στον αλγόριθμο κρυπτογράφησης A5, οποίος επιλέγεται κάθε φορά από το σύνολο των αλγορίθμων που υποστηρίζει ο κινητός σταθμός.

Οπως αναφέρθηκε προηγουμένως, η ασφάλεια του συστήματος GSM βασίζεται στο κλειδί Ki και στους αλγόριθμους A3, A8 και A5. Για την υλοποίηση των αλγορίθμων A3 και A8 η πλειοψηφία των παρόχων χρησιμοποιεί τον αλγόριθμο COMP 128, ο οποίος κρατήθηκε μυστικός. Παρόμοια, οι υλοποιήσεις του A5 (A5/1 "ισχυρή" έκδοση του αλγόριθμου και A5/2 "ασθενέστερη" έκδοση, η οποία χρησιμοποιείται στις περισσότερες χώρες του κόσμου) δεν δημοσιοποιήθηκαν. Ως συνέπεια, η επιστημονική κοινότητα δεν μελέτησε τους παραπάνω αλγόριθμους, ώστε να αποκαλυφθούν πιθανές ατέλειές τους. Ετσι, 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. Ομως, όπως ήταν αναμενόμενο, οι αλγόριθμοι τελικά διέρρευσαν, ενώ παράλληλα η διαθέσιμη υπολογιστική ισχύ έχει αυξηθεί κατά αρκετές τάξεις μεγέθους.

Αν και οι προδιαγραφές ασφαλείας των συστημάτων κινητής τηλεφωνίας είναι ιδιαίτερα υψηλές, υπάρχουν τρόποι υποκλοπής των «κινητών» δεδομένων, οι οποίοι όμως προϋποθέτουν υψηλή τεχνογνωσία και ιδιαίτερα εξελιγμένο (και ακριβό) εξοπλισμό

Μορφές επίθεσης

Μια από τις επιθέσεις που εκμεταλλεύεται τις αδυναμίες ασφάλειας του GSM έχει σαν στόχο την ανάκτηση του κλειδιού Ki. Στην περίπτωση που κάποιος επιτιθέμενος αποκτήσει αυτό το κλειδί, μπορεί να υποκλέψει παθητικά τα δεδομένα που μεταφέρονται μεταξύ του MS και του BTS ή μπορεί να δημιουργήσει μια κάρτα αντίγραφο της αρχικής ("κλώνο"). Εχοντας μια κάρτα κλώνο, ο επιτιθέμενος μπορεί να συμμετέχει σε συναλλαγές οι οποίες θα χρεώνονται στον νόμιμο συνδρομητή.

Το κλειδί Ki του κάθε συνδρομητή GSM βρίσκεται αποθηκευμένο σε δύο σημεία: στην κάρτα SIM της συσκευής του, και στο HLR του παρόχου, στον οποίο είναι εγγεγραμμένος ο χρήστης. Η κάρτα SIM δεν

παρέχει κάποιο άμεσο τρόπο ανάκτησης του κλειδιού Ki, ακόμα και σε κάποιον που έχει φυσική πρόσβαση σε αυτή. Παρόλα αυτά όμως, ερευνητές ανακάλυψαν μεθόδους με τις οποίες κάποιος κακόβουλος μπορεί να ανακτήσει το κλειδί Ki είτε έχοντας στην κατοχή του μια κάρτα SIM είτε όχι. Αυτές οι μέθοδοι εκμεταλλεύονται κάποιες αδυναμίες του αλγόριθμου COMP 128, ο οποίος χρησιμοποιείται για την υλοποίηση του A3.

Σε άλλη μια μορφή επίθεσης στο σύστημα GSM, ο επιτιθέμενος εκμεταλλεύεται τις αδυναμίες του αλγόριθμου A5 (και των δύο εκδόσεών του A5/1 και A5/2). Με την επίθεση αυτή, ο επιτιθέμενος ανακτά το κλειδί κρυπτογράφησης Kc (64-bit) 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 τον ίδιο κλειδί κρυπτογράφησης.

Επίσης, υποκλοπή των δεδομένων μπορεί να πραγματοποιηθεί εφαρμόζοντας μια επίθεση τύπου ενδιαμέσου (man-in-the-middle attack). Ο επιτιθέμενος χρησιμοποιεί ένα δικό του BSS, το οποίο υπερκαλύπτει το σήμα του νόμιμου παρόχου και αναγκάζει το τερματικό του θύματος να συνδεθεί με αυτό. Επειτα, το παράνομο BSS είτε ζητάει από το MS να μεταδίδει τα δεδομένα στον αέρα χωρίς κρυπτογράφηση, είτε αλλοιώνει την διαπραγμάτευση του αλγόριθμου κρυπτογράφησης μεταξύ MS και BTS. Επίσης, ο επιτιθέμενος έχει τη δυνατότητα να παρεμβαίνει στην επικοινωνία του θύματος και του νόμιμου 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 κρυπτογράφηση χρησιμοποιείται, μόνο, στο τμήμα μεταξύ του MS και του BTS. Ετσι, στο υπόλοιπο τμήμα του δικτύου η κρυπτογράφηση των δεδομένων επαφίεται στον πάροχο, με όποιες συνέπειες μπορεί αυτό να έχει για την ασφάλειά τους.

Δυνατότητα εντοπισμού της θέσης του χρήστη

Στο σύστημα GSM, η θέση των συνδρομητών μπορεί να προσδιοριστεί από τους παρόχους με βάση την κυψέλη από την οποία εξυπηρετείται ένας χρήστης και τεχνικών 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 πιθανόν να μην επιθυμεί να γνωστοποιείται σε τρίτους. Ωστόσο, αν κάποιος έχει πρόσβαση στο σύστημα του παρόχου, είτε εκ των έσω, είτε παραβιάζοντας κάποιο λογαριασμό ή υπηρεσία, μπορεί να έχει πρόσβαση σε αυτή την απόρρητη πληροφορία. Μια παρεμφερή πληροφορία που μπορεί ένας τρίτος να εξάγει από ένα σύστημα GSM είναι η παρουσία κάποιου 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. Ετσι, ένας επιτιθέμενος θα μπορούσε, εκμεταλλευόμενος αυτό το χαρακτηριστικό και χρησιμοποιώντας έναν σταθμό βάσης BTS που θα υπερκάλυπτε το σήμα του παρόχου, να ανιχνεύσει την παρουσία κάποιου ατόμου σε κάποια περιοχή, εφόσον το τερματικό του είναι ανοιχτό.

** Ο κ. Χρήστος Ξενάκης είναι διδάκτορας του Πανεπιστημίου Αθηνών και υπεύθυνος της ερευνητικής ομάδας ασφάλειας δικτύων του Εργαστηρίου Δικτύων Επικοινωνιών στο Πανεπιστήμιο Αθηνών*

Ο κ. Λάζαρος Μεράκος είναι καθηγητής στο τμήμα Πληροφορικής και Τηλεπικοινωνιών, και διευθυντής του Εργαστηρίου Δικτύων Επικοινωνιών στο Πανεπιστήμιο Αθηνών

Ημερίδα της VeriSign και της ADACOM

Το σήμερα και το αύριο στις τηλεπικοινωνίες

Με επιτυχία πραγματοποιήθηκε η ημερίδα που διοργανώθηκε πριν λίγες ημέρες από τις εταιρείες VeriSign και ADACOM, υπό τον ευρύτερο τίτλο "Security Beyond Passwords". Οι δύο εταιρείες παρουσίασαν στο ελληνικό επιχειρηματικό κοινό τις πιο εξελιγμένες λύσεις για την επίτευξη της μέγιστης δυνατής προστασίας των συναλλαγών σε δίκτυα φωνής και δεδομένων.

Πιο αναλυτικά, οι ομιλητές της διοργάνωσης επικεντρώθηκαν στην ανάγκη "προστασίας της ταυτότητας" (Identity Protection), επισημαίνοντας τη διαρκή αύξηση των κινδύνων που υπάρχουν στο σύγχρονο επιχειρηματικό περιβάλλον, καθώς και την εμφάνιση νέων απειλών, όπως credit card theft, identity theft και Phishing, σε συνδυασμό και με τους τρόπους με τους οποίους οι υπηρεσίες των Adacom - VeriSign συμβάλλουν στην αντιμετώπισή τους.

Μετά τον εναρκτήριο χαιρετισμό του διευθύνοντα συμβούλου της ADACOM, κ. David Samuel, ο γενικός διευθυντής της ADACOM, κ. Πάνος Βασιλειάδης αναφέρθηκε στην ομιλία του στη χρήση της προηγμένης ηλεκτρονικής υπογραφής μέσα από το θεσμοθετημένο πλαίσιο της χώρας μας, επισημαίνοντας, μεταξύ άλλων, ότι "σημαντικό ρόλο αναμένεται να έχει η χρήση της προηγμένης ηλεκτρονικής υπογραφής στην ελληνική ηλεκτρονική διακυβέρνηση μέσω του υποέργου 9 του ΣΥΖΕΥΞΙΣ".

Οι ομιλίες των προσκεκλημένων της VeriSign κάλυψαν τους τομείς της περαιτέρω επέκτασης του μοντέλου της "Ενοποιημένης Αυθεντικοποίησης", ανεξάρτητα από τον τύπο συσκευής ή δικτύου, καθώς και τις πρωτοποριακές μεθόδους που σήμερα διατίθενται για την ασφάλεια στα δίκτυα φωνής και την προστασία των φορητών συσκευών.

Παρουσίαση εφαρμογών στην πράξη

Το ενδιαφέρον των παρευρισκομένων συγκέντρωσε η παρουσίαση της μελέτης - περίπτωσης της εφαρμογής της υπηρεσίας "μοναδικών κωδικών" των ADACOM - VeriSign στην τράπεζα της Alpha Bank. Οι δύο ομιλητές της τράπεζας, κ. Γεράσιμος Μοσχονάς, Group Information Security Officer, Compliance Division, και κ. Θεόπεμπτος Βήχος, Assistant Manager, Alternative Channels Division, επεσήμαναν "την ευκολία υλοποίησης και τον εντυπωσιακό ρυθμό αποδοχής της υπηρεσίας μοναδικών κωδικών από τους χρήστες του Alpha Web Banking", ενώ αναφέρθηκαν και στα μελλοντικά σχέδια της τράπεζας, αφενός να "καταστήσει υποχρεωτική τη χρήση της συσκευής μοναδικών κωδικών για όλους τους χρήστες - πελάτες της τράπεζας που προβαίνουν σε "επικίνδυνες" συναλλαγές", αφετέρου να "εισαγάγει την υπηρεσία υποδομής δημοσίου κλειδιού (PKI)".

Εθνικό Κέντρο Τεκμηρίωσης

Τρίτη πρόσκληση για τη Δράση της ευρωπαϊκής έρευνας στην ασφάλεια

Η τρίτη πρόσκληση υποβολής προτάσεων για την Προπαρασκευαστική Δράση του προγράμματος Ευρωπαϊκή έρευνα στον τομέα της ασφάλειας" θα παρουσιαστεί σε ημερίδα που διοργανώνει το Εθνικό Κέντρο Τεκμηρίωσης (ΕΚΤ), σε συνεργασία με τη Γενική Γραμματεία Ερευνας και Τεχνολογίας (ΓΓΕΤ) και με την υποστήριξη της Ευρωπαϊκής Επιτροπής, στις 31 Μαρτίου 2006, στην Αθήνα (Εθνικό Ιδρυμα Ερευνών, Βασ. Κωνσταντίνου 48).

Κύριος ομιλητής είναι ο κ. Pieter De Smet, εκπρόσωπος της Γενικής Διεύθυνσης Επιχειρήσεων της Ευρωπαϊκής Επιτροπής, ο οποίος θα παρουσιάσει τόσο την τρέχουσα πρόσκληση υποβολής προτάσεων, με προϋπολογισμό 15 εκατ. ευρώ και καταληκτική ημερομηνία τη 10η Μαΐου 2006, όσο και τις προοπτικές του προγράμματος για την ασφάλεια στο 7ο πρόγραμμα Πλαίσιο για την έρευνα.

Ο εθνικός εκπρόσωπος του προγράμματος καθ. Γ. Πάγκαλος θα παρουσιάσει την εθνική συμμετοχή στην προπαρασκευαστική Δράση, ενώ εκπρόσωπος του ΕΚΤ θα παρουσιάσει τις υπηρεσίες που προσφέρει το ΕΚΤ ως Εθνικό Σημείο Επαφής στους οργανισμούς που ενδιαφέρονται να συμμετάσχουν στα προγράμματα Πλαίσιο.

Οι στόχοι της Δράσης

Στόχος της προπαρασκευαστικής Δράσης είναι η προετοιμασία ενός ολοκληρωμένου ευρωπαϊκού προγράμματος για την ενίσχυση της ασφάλειας των ευρωπαίων πολιτών μέσω της έρευνας και της τεχνολογίας, το οποίο θα περιλαμβάνεται στο 7ο πρόγραμμα Πλαίσιο για την έρευνα (2007-2013). Απευθύνεται δε, σε δημόσιες αρχές, δημόσιες και ιδιωτικές επιχειρήσεις, πανεπιστήμια και ερευνητικούς οργανισμούς της ΕΕ.

Τομείς κάλυψης

Η νέα πρόσκληση είναι η τελευταία για την προπαρασκευαστική Δράση και καλύπτει τους παρακάτω τομείς:

- Βελτιστοποίηση της ασφάλειας και της προστασίας δικτυωμένων συστημάτων.
- Προστασία από την τρομοκρατία (συμπεριλαμβάνονται η βιοτρομοκρατία και συμβάντα που ενέχουν χρήση βιολογικών, χημικών και άλλων ουσιών).
- Βελτίωση της διαχείρισης κρίσεων (συμπεριλαμβάνονται οι επιχειρήσεις εκκένωσης, αναζήτησης και διάσωσης, ελέγχου των ενεργών παραγόντων και αποκατάστασης) .
- Εξασφάλιση διαλειτουργικών και ολοκληρωμένων συστημάτων πληροφοριών και επικοινωνίας
- Βελτίωση της ικανότητας αντίληψης των καταστάσεων (π.χ. διαχείριση κρίσεων, αντιτρομοκρατικές ενέργειες, έλεγχος συνόρων).

Συνολικά προβλέπεται η χρηματοδότηση 6-8 έργων, που θα απορροφήσουν 12,5 εκατ. ευρώ, ενώ 2,5 εκατ. ευρώ θα διατεθούν σε υποστηρικτικές δράσεις, οι οποίες θα συμβάλλουν στην προετοιμασία του μελλοντικού ευρωπαϊκού προγράμματος για την έρευνα στον τομέα της ασφάλειας ή θα αφορούν θέματα ανθρώπινων παραγόντων σε σχέση με την ασφάλεια.

Στην εκδήλωση οι συμμετέχοντες θα έχουν την ευκαιρία για περαιτέρω συζητήσεις για την από κοινού συμμετοχή σε κοινοπραξίες για την υποβολή προτάσεων.

Το πρόγραμμα και το δελτίο συμμετοχής για την ημερίδα είναι διαθέσιμα στο δικτυακό τόπο του ΕΚΤ (http://www.ekt.gr). Η είσοδος στην εκδήλωση είναι ελεύθερη.