GSM-Unsicherheit

Vortrag: *Andreas Bohk, Lucky Green, Janus* <ich@andreas.org>

Bericht: *Dirk Steinhauer* <moose.uni.de>

Welche Sicherheitsmerkmale sind im GSM Netz implementiert? Wenigstens kann man dort nicht wie im alten analogen C-Netz einfach mit einem Scanner mithören, denn zwischen Basisstation und Telefon werden die Daten verschlüsselt. Auch sind die Telefonnummern an sich nicht auf der SIM-Karte gespeichert, sondern nur in einer zentralen Datenbank des Netzbetreibers, wo zu jeder SIM-Nummer die Telefonnummern zugeordnet wird.

Wenn sich das Telefon authentifizieren will, bekommt es vom Authentification Center (AC) eine RAND Challenge, die in der SIM-Karte mit dem Geheimschlüssel und dem A3-Algorithmus zum SRES verarbeitet wird. Diese SRES geht zurück an den AC, der sie mit einer von ihm berechneten SRES vergleicht. Sind beide identisch, gibt das AC grünes Licht. Der A3 Algorithmus ist nicht in jedem Netz gleich, aber es gibt einen Referenzstandard dafür (COMP128), der bis vor kurzem nicht bekannt war (Security by obscurity). Bis auf die sicherheitsrelevanten Themen ist aber der GSM-Standard unter [1]http://www.etsi.fr/ zu finden.

Zur Verschlüsselung werden 128 Bit RAND und 128 Bit KI 40 mal durchrotiert, allerdings sind das 1. und 8., das 2. und 9. Byte (usw...) miteinander verbunden. Nach 6-18 Stunden und in der Regel 150.000 Durchläufen kann man sich den Geheimschlüssel durch diesen Bug generieren und auf einem Simulator eine echte Karte emulieren. Der A5-Algorithmus ist ein 64 Bit langer Key, von dem allerdings die letzten 10 Bit Nullen sind. Ein weiterer Key (A8) dient der Schlüsselgenerierung.

Lucky Green erzählte von den Begebenheiten, die dazu geführt haben, daß er den COMP128 gefunden hat: Er stolperte bei einer Übersetzung eines GSM Manuals über den Befehl "Run GSM Algorithm" und versuchte, im Netz etwas über COMP128 herauszufinden. Er fand nur eine in Teilen falsche Version und suchte drei Monate, um den richtigen Algorithmus zu finden. Den gab er zwei Freunden, die sich an der UC Berkley auf Kryptografie spezialisiert haben, und innerhalb vor zwei Stunden war er geknackt.

Drei Tage vor der Veröffentlichung fand er einen Hersteller, der Chipkarten mit COMP128 und veränderbarer Schlüssel herstellt, und natürlich bestellte er alle 8 in Nordamerika verfügbaren Exemplare. Mittlerweile wird in etwa 100 Millionen Mobiltelefonen COMP128 eingesetzt, und die Austauschkosten werden sich auf etwa 1,6 Millionen Dollar belaufen. Auch die 12 Provider weltweit, die nicht COMP128 benutzen, setzen aus irgendeinem unerfindlichen Grund die letzten 10 Bits des A5 auf Null. Natürlich war es nicht Sinn des Experiments, GSM zu zerstören, sondern nur darauf hinzuweisen, daß es immer ein Problem ist, wenn Kryptoschlüssel nicht öffentlich gemacht werden.

Übrigens es ist auch kein Problem, eine unechte Basisstation zu bauen, die nur Challenges aussendet um so an die Schlüssel mehrerer Mobiltelefonen zu kommen. Bei Motorola-Telefonen kann man sogar recht einfach die Software ändern und so aus einem handelsüblichen Telefon und mit ein wenig krimineller Energie eine unechte Basisstation bauen. Dies ist möglich, da sich die Basisstation nicht authentifizieren muß, sondern nur das Telefon. Andreas ist davon überzeugt, daß die GSM Standards absichtlich so niedrig gehalten wurden. So werden beispielsweise nur die Daten zwischen Handy und Basisstation mit A5 verschlüsselt, aber nicht zwischen der Basisstation und dem Netz an sich, wo Funkstrecken benutzt werden. (Richtfunkstrecken). Wenn man sich in einem anderen Netz befindet (Ausland), dann werden vom Heimnetz an das Roamingnetz fünf Tripplets aus RAND, SRES und KI geschickt aber nur eins davon benutzt. Die restlichen könnte theoretisch ein anderer benutzen, um so ohne eigene Selbstkosten zu telefonieren.

Die von den Netzbetreibern verbreitete Legende, daß man sich mit der selben SIM mehrmals in ein Netz einloggen kann, ist nicht wahr. Um Gespräche abzuhören genügt übrigens A8, A3 und COMP128. A5 muß man nicht unbedingt kennen. Aber nicht nur das GSM-Netz an sich, sondern auch viele Telefone haben Schwachstellen oder ausgeschaltete Features, die man in einem Servicemode aktivieren kann. Durch diesen Servicemode kann man aus seinem Billighandy manchmal ein "Top the line" Gerät machen.

Weitere Informationen zum Thema sind das im Hansa-Verlag erschienene "Handbuch der Chipkartentechnik" von Ranke und Effing ISBN 3-496-18893-2 ISO 7816 für Chipkarten an sich der GSM Standard 11.11 [2]http://www.efri.fr/ und das Programm Serprog von Tron, das (wie auch Wafercards) im Archiv zu finden ist.

References

1. http://www.etsi.fr/
2. http://www.efri.fr/