Hacking als Open-Source-Projekt
GSM-Verschlüsselung mit Grafikkarten-CPUs geknackt

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Mit Geräten, die in heute in jedem zweiten Kinderzimmer stehen, lässt sich die Verschlüsselung von GSM-Mobiltelefonen brechen. Ein Open-Source-Projekt des Kryptografie-Experte Karsten Nohl beweist: der A5/1-Verschlüsselungscode von GSM ist höchst unsicher. Auf der Sicherheits–konferenz IT-Defense 2010 berichtete Nohl über den aktuellen Stand und ging noch einen Schritt weiter.

Die GSM-Verschlüsselung ist prinzipiell unsicher, das wurde bereits durch mehrere Angriffe auf den A5/1-Algorithmus belegt. Das Abhören von GSM-Gesprächen galt aufgrund technischer Maßnahmen wie dem Frequenzhopping bislang nicht als praktikabel.

Der 28-jährige Mathematiker und Kryptograf Karsten Nohl beweist, dass derartige Argumente hinfällig sind. Er hatte zusammen mit einigen Mitstreitern im August 2009 damit begonnen, die GSM-Verschlüsselung im Rahmen eines Open-Source-Projekts zu hacken. Dazu nutzten sie die Methoden des verteilten Rechnens.

Analog zum SETI@Home-Projekt spenden die Teilnehmer die überschüssige Rechenzeit ihrer Computer, Nohl und seine Krypto-Mannschaft stellen die nötigen Programme und vor allem Treiber zur Verfügung. „Insbesondere moderne Grafikkarten sind besonders gut zum Codebrechen geeignet“, so Nohl auf dem Kongress IT Defense 2010 Anfang Februar in Brühl, „sie bieten bis zu 500 Cores auf kleinem Raum.“

Die Ergebnisse des verteilten Rechnens wandern in eine von Nohl optimierte Code-Tabelle. Mithilfe dieser Tabellen lassen sich die Datenströme dechiffrieren. Nach einigen Minuten kann der Angreifer mithören. Mit etwas höherem finanziellen Aufwand, so Nohl, wäre auch eine Echtzeitdecodierung möglich.

Damit hätten Angreifer erstmals die Möglichkeit, sich aktiv zwischen Gesprächsteilnehmer zu schalten, in dem er eine eigene Basisstation betreibt. Bislang können dies in Deutschland nur Strafverfolgungs–behörden mit Hilfe des so genannten IMSI Catchers.

„Es gibt ein zweites Open-Source-Projekt für die Hardware“, so Karsten Nohl. Zusammenschalten darf er die beiden Projekte nicht, dann würde er sich strafbar machen. Die nötige Funkausstattung gibt es in Onlineshops für rund 1500 Dollar. Sie unterstützt auch Frequenzhopping.

Damit dürfte das letzte Argument der des Brachenverbandes GSMA hinfällig sein, die Nohls Hack als theoretisch möglich aber praktisch nur schwer umsetzbar hinstellten. Nohl Hardware springt genauso, wie eine echte Basisstation von Frequenz zu Frequenz.

Nohl forderte in Brühl die Telefonkonzerne auf, endlich ihre zahllosen Basisstationen auf den neuesten Stand der Verschlüsselungstechnik zu heben: „Eigentlich müssten die Telekommunikationsanbieter nun den A5/1-Verschlüsselungscode durch eine sichere Variante ersetzen, dazu müssten sie nur pro Basisstation einen FPGA umprogrammieren.“ Doch in der Praxis ist die Sache wohl schwieriger. Die meisten Provider haben ihre Serviceverträge gekündigt. Niemand fühlt sich für das dringend nötige Sicherheitsupdate zuständig.

Doch Nohl sieht noch ein weiteres, weit tiefergehendes Sicherheitsproblem. Auch beim Nachfolger UMTS wird den Endgeräten zu

wenig Kompetenz gegeben: sie tun stets, was die Basistation ihnen sagt. So springen auch diese Apparate auf Wunsch in einen unsicheren Verschlüsselungsmodus und geben damit jede Vertraulichkeit auf.

Keine guten Nachrichten für die rund 200 internationalen Sicherheits–experten der IT Defense in Brühl. Nohls GSM Hack hat für die Sicherheitsindustrie weitreichende Folgen. Schließlich laufen nicht nur Alarmmeldungen und Störungsinformationen über GSM, sondern es werden auch Passwörter sowie PINs und TANs per SMS verschickt. Aber auch dieser Dienst, das machte Nohl klar, ist von dem Verschlüsselungs-Hack genauso betroffen. Etliche Sicherheitsszenarien zur Verteilung von Zugangsdaten müssen nun überarbeitet werden.

Nohl plant bereits den nächsten Coup. Das Schnurlostelefonsystem DECT ist technisch jünger als GSM und nutzt stärkerer Verschlüsselung mit einem 80 Bit langen Schlüssel. “Auch der sollte sich mit unseren Tabellen und optimierter Hardware jetzt knacken lassen“, so Nohl.

searchsecurity.de 12.02.10