DuD
Datenschutz und Datensicherheit

Sicherheit des GSM-Verschlüsselungsstandards A5

Erik Zenner, Rüdiger Weis, Stefan Lucks

Die Standardisierung von Verschlüsselungsalgorithmen ist eine zentrale Voraussetzung für die Interoperabliltät von Kommunikationssystemen. Häufig geschieht dabei vieles hinter verschlossenen Türen – nicht gerade zum Vorteil für die Sicherheit, wie die folgende Sicherheitsbewertung des GSM-Algorithmus A5/1 zeigt.

Dipl.-Wirtsch.-Inf. Erik Zenner

Promoviert gefördert von der Landesgraduiertenförderung Baden-Würtemberg an der Theoretischen Informatik der Universität Mannheim.
Forschungsschwerpunkte: Kryptographie, Kommunikationssicherheit, Electronic Payments.
E-Mail: zenner@th.informatik.uni-mannheim.de

Dipl.-Math. Rüdiger Weis

Schliesst im Sommer 2000 seine Dissertation an der Universität Mannheim ab und leitet die Cryptolabs der convergence integrated media GmbH, Berlin, San Francisco, Amsterdam.
Forschungsschwerpunkte: Kryptographie, Computersicherheit, Smartcards, Verteilte Multimedia Anwendungen.
E-Maill: ruedi@cryptolabs.org

1 Einleitung

Mobiltelefone haben in den vergangenen Jahren weite Verbreitung gefunden – allein in Deutschland nutzten Ende des Jahres 1999 rund 23,2 Millionen Teilnehmer die neue Technologie. Die Abkürzung „GSM“ steht dabei für „Global System for Mobile Communications“.[1] GSM ist der derzeit am weitesten verbreitete Standard für Mobiltelefonie. Die GSM Association vermeldete gegen Ende des Jahres 1999 über 250 Millionen Endnutzer weltweit, die meisten davon in Europa.

In den letzten Jahren wurden allerdings eine Reihe von Sicherheitsproblemen aufgezeigt. Das gravierendste ist bis heute die Schwäche des Authentifizierungsalgorithmus [SDA98, WeLu98]. Hierdurch kann sogar der geheime Masterschlüssel der Karte ausgelesen werden. Der Chaos Computer Club entwickelte innerhalb weniger Tage die hierzu nötige Software und stellte sie ins Internet [CCC98]. Durch das „Cloning“ der SIM-Karte kann ein Angreifer auf Kosten des Benutzers telefonieren [BoRi98]. Weiterhin können auch Gespräche der erfolgreich angeriffenen Karte problemlos in Echtzeit abgehört werden.

Im folgenden wollen wir uns auf Angriffe gegen die Verschlüsselungsfunktion A5 konzentrieren. Dabei gilt zunächst: Die Mobiltelefonkommunikation ist höchstens so sicher wie die Standards, auf denen sie basiert. Dabei kommt dem GSM-Standard eine besondere Rolle zu – zum einen aufgrund seiner Verbreitung, zum anderen aufgrund einer möglichen Vorbildwirkung für andere Normen. Gerade die GSM Association (bzw. ihre Vorgängerorganisation, die GSM Mobile Unit) hat seit jeher betont, dass ihre Protokolle durch den Einsatz kryptographischer Techniken ein Höchstmaß an Sicherheit böten.

Von unabhängigen Kryptographen wurde jedoch von Anfang an bemängelt, dass die als sicher angepriesenen kryptographischen Verfahren der Öffentlichkeit nicht zugänglich gemacht wurden. Einer solchen Vorgehensweise hängt immer der Ruch an, dass die Algorithmen einer gründlichen Prüfung von unabhängiger Seite nicht standhalten könnten.

Wie sicher ist heute nun aber das Telefonieren mit einem Mobiltelefon? Die folgende Darstellung trägt eine Reihe neuerer Ergebnisse zusammen und versucht, zu einer nüchternen Beurteilung der Sicherheit der GSM-Verschlüsselung zu gelangen.

Dr. Stefan Lucks

Arbeitet gefördert von der DFG Grant KR 1521/3-1 als wissenschaftlicher Mitarbeiter der Theoretischen Informatik an der Universität Mannheim.
Forschungsschwerpunkte: Kryptographie, Computersicherheit, Komplexitätstheorie.
E-Mail: lucks@th.informatik.uni-mannheim.de

2 Der A5/1 Algorithmus

Der Algorithmus, mit dessen Hilfe im GSM-Standard digitalisierte Sprachdaten auf der Luftschnittstelle ver- bzw. entschlüsselt werden, wird in den Entwurfsunterlagen mit dem Kürzel A5 bezeichnet. Es gibt wenigstens zwei Versionen dieses Algorithmus. Die kryptographisch stärkere Version wird mit A5/1 bezeichnet und ist für den Einsatz in Europa bestimmt. Der Algorithmus A5/2 dagegen gilt als „schwaches“ Verschlüsselungsverfahren und ist für den Export in Länder konzipiert, in denen der Einsatz von Kryptographie nur unter Auflagen zulässig ist. Wir beschränken uns im folgenden auf die Betrachtung des A5/1.

Über die Funktionsweise des Algorithmus war zunächst wenig bekannt, da die

[1] Siehe auch Pütz, Gateway, DuD 6/1997.

Entwurfsunterlagen geheimgehalten wurden. Erste Untersuchungen des Algorithmus stützten sich auf Teile dieser Unterlagen, die Anfang der 90er Jahre auf anonymem Weg (in einem Briefumschlag ohne Absender) an die Bradford University gelangt waren. Zwar war das Material unvollständig, doch bekamen die beteiligten Wissenschaftler eine erste Vorstellung davon, wie der Algorithmus arbeitete.

Der englische Kryptograph Shepherd war der erste, der sich im Jahre 1994 im Rahmen einer wissenschaftlichen Veröffentlichung ernsthaft mit der Sicherheit des A5/1 Algorithmus auseinandersetzte. Seine Ergebnisse beunruhigten jedoch den britischen Informationsgeheimdienst GCHQ so sehr, dass dieser die Veröffentlichung untersagte. Dieses Verbot bestärkte natürlich diejenigen Kritiker, die seit jeher vermutet hatten, dass Geheimdienste bei der Entwicklung des A5/1 mitgewirkt und dafür gesorgt hatten, dass der Algorithmus nicht „zu sicher“ für einen nachrichtendienstlichen Zugriff würde. Bis heute ist nicht bekannt, zu welchem Ergebnis Shepherd bei seinen Untersuchungen gekommen ist.

Eine Veröffentlichung von Jovan Golic aus dem Jahre 1997 beschrieb zwei mögliche Angriffe auf den A5/1 [Golic97]:

2.1 Direkter Angriff

Der *„direkte“ Angriff* benötigt als Eingabe neben dem verschlüsselten Signal („Chiffretext“) auch einen Sekundenbruchteil des unverschlüsselten Datenstroms („Klartext“). Diese Annahme ist nicht unrealistisch, da es sich dabei auch um eine winzige Gesprächspause o. ä. handeln kann. Der Angriff muss laut Golic im Mittel etwa 2^{40} Knoten eines Suchbaumes durchlaufen.

Allerdings konnte Zenner in [Zen99] zeigen, dass der tatsächliche Aufwand im Mittel eher bei 2^{42} Schritten liegt. Überdies ist jeder dieser Rechenschritte vergleichsweise aufwendig. Es ist daher zwar möglich, dass ein Unbefugter auf die von Golic beschriebene Art und Weise ein Telefonat entschlüsseln kann. Allerdings muss er dabei Verzögerungen in Kauf nehmen, die bei „normaler“ Hardwareausstattung (sprich: schneller PC) im Bereich von Monaten liegen dürften.

2.2 Time-Memory-Tradeoff

Bei einem *Time-Memory-Tradeoff* benötigt ein Angriff umso weniger Zeit für die eigentliche Entschlüsselung, je mehr Speicherplatz zur Verfügung steht. Der von Golic beschriebene Angriff ist jedoch für das gezielte Abhören eines vorher festgelegten Telefonates nicht geeignet, da er einer Vielzahl von Beschränkungen unterworfen ist. Ein Beispiel: Ein Angreifer, der über 862 Gigabyte an Speicherplatz verfügt, muss immerhin 130 Minuten an Klartext mit dem zugehörigem Chiffretext kennen und benötigt, wie Biryukov und Shamir in [BiSh99] vorrechnen, über 3 Wochen Rechenzeit allein für Festplattenzugriffe. Sinnvoll ist ein solches Vorgehen nur für einen Angreifer, der über immens leistungsfähige Hardware verfügt und dem es ausreicht, wenn er nur einen Bruchteil der mitgeschnittenen Telefonate tatsächlich entschlüsseln kann.

2.3 Schlüsselverkürzung

Im April 1998 fanden die Amerikaner Briceno, Goldberg und Wagner bei Untersuchungen von Handys verschiedener Provider heraus, dass A5/1 zwar wie schon vermutet einen Schlüssel der Länge 64 bit verwendet, dass jedoch alle von ihnen untersuchten Implementierungen des Algorithmus 10 dieser Bits auf ‘0’ setzten [SDA98]. Die effektive Schlüssellänge betrug somit nur noch 54 bit, was eine massive und vor allem vorsätzliche Schwächung des Algorithmus darstellte und Zweifel an der Ernsthaftigkeit des Sicherheitsversprechens der GSM aufkommen liess.

2.4 Reverse Engeneering

Wie bereits geschildert, basierten die Sicherheitsanalysen zunächst auf unvollständigen Entwurfsunterlagen. Mitte des Jahres 1999 veröffentlichten Briceno, Goldberg und Wagner einen Algorithmus in C, den sie durch Reverse Engineering herausgefunden hatten [BGW99]. Obwohl eine offizielle Bestätigung von Seiten der GSM nicht erfolgte (und auch kaum zu erwarten war), kann davon ausgegangen werden, dass es sich dabei um den korrekten Code des Verschlüsselungsalgorithmus A5/1 handelt.

2.5 Biryukov/Shamir-Angriff

Ende des Jahres 1999 veröffentlichten die am Weizmann-Institut in Israel tätigen Kryptographen Biryukov und Shamir eine Vorabversion eines Fachartikels mit dem klangvollen Namen „Real Time Cryptanalysis of the Alleged A5/1 on a PC“ [BiSh99]. Die Ankündigung, dass der vorgestellte Angriff den A5/1 selbst auf einem einfachen PC in Echtzeit entschlüsseln könnte, war natürlich sensationell. Konkret schlagen Biryukov und Shamir einen PC mit 128 MB RAM und zwei Festplatten zu je 73 Gigabyte vor – eine Ausrüstung, die zwar nicht in jedem Büro steht, die aber ohne große Schwierigkeiten für etwa 10.000 DM zu beschaffen ist.

Der Angriff selbst ist eine Weiterentwicklung des von Golic beschriebenen Time-Memory-Tradeoffs, der so modifiziert wurde, dass er den Schlüssel, mit dem ein Telefonat codiert wurde, innerhalb von weniger als einer Sekunde errechnen kann. Die wichtigste algorithmische Neuerung gegenüber Golics Entwurf ist die Verwendung einer „biased birthday attack“, bei der gezielt Datensätze mit bestimmten Eigenschaften (sog. „samples“) im Vorhinein berechnet und auf der Festplatte gespeichert werden. Voraussetzung hierfür ist die von Biryukov und Shamir nachgewiesene niedrige „sampling resistance“ des Algorithmus, die ein gezieltes Erzeugen solcher erwünschter Datensätze ermöglicht.

Von entscheidender Bedeutung für die praktische Umsetzbarkeit ist zudem die von Biryukov und Shamir vorgeschlagene Methodik, mit der der (eigentlich für hohe Geschwindigkeit in Hardware entworfene) A5/1 mittels Table-Lookups extrem effizient in Software implementiert werden kann. Nichtsdestotrotz erfordern die Vorberechnungen, die vor dem eigentlichen Angriff geleistet werden müssen, einen erheblichen Aufwand. Im vorliegenden Fall sind sie so umfangreich, dass die Autoren sie nicht selbst durchführen konnten, obwohl ihnen zweifellos die Rechnerausstattung des Weizmann-Institutes zur Verfügung stand. Dennoch sind diese Berechnungen möglich und für einen mit ausreichend finanziellen Mitteln ausgestatteten Angreifer auch kein ernsthaftes Hindernis.

Schwieriger ist da schon die Beschaffung der unverschlüsselten digitalen Daten, die auch für diesen Angriff notwendig sind. Die Berechnungen von Biryukov und Shamir stützen sich auf die Annahme, dass dem

Angreifer zwei Minuten an korrespondierenden Klartext-/Chiffretextblöcken zur Verfügung stehen. Die Antwort auf die Frage, woher er diese bekommen sollte, bleiben die Autoren schuldig. Das Problem liegt also ähnlich wie schon beim Golic-Angriff: Es ist zwar möglich, mit Hilfe des Time-Memory-Tradeoffs aus einer großen Anzahl von Telefonaten einzelne Gespräche zu entschlüsseln, der Angreifer kann dabei aber vorher keine Aussage darüber treffen, *welches* der mitgeschnittenen Gespräch er nun tatsächlich knacken kann.

3 Sicherheitsbewertung

Alle oben beschriebenen Entschlüsselungsmethoden stehen nur solchen Angreifern zur Verfügung, die über hervorragende Sachkenntnis und Hardware sowie ausreichend finanzielle Ressourcen verfügen und die das Abhören von Telefonaten mit einer gewissen Regelmäßigkeit betreiben.

Das von einigen Mahnern heraufbeschworene Schreckensbild vom Heimanwender, der mit seinem PC und einer selbstgebastelten Abhöranlage Handytelefonate abhört, ist vorläufig noch übertrieben. Gebrochen werden kann der A5/1 aber mit einiger Sicherheit von Großunternehmen und vor allem von internationalen Nachrichtendiensten.

Es gibt ausreichend Hinweise darauf, dass gerade letztere bereits Ende der 80er Jahre maßgeblichen Einfluss auf die Entwickung des A5/1 genommen haben, vermutlich mit dem Ergebnis, dass der Algorithmus von Anfang an für sie zu brechen war. Dieses „von Anfang an“ liegt nun überdies mehr als zehn Jahre zurück, und was damals bereits möglich war, ist mit moderner Hardware natürlich um so leichter.

Die Warnung ist daher nicht neu, aber aktueller denn je: Sensible Daten sollten niemals ohne zusätzliche starke Verschlüsselung über Telefon- und schon gar nicht über Mobiltelefonverbindungen übertragen werden.

Literatur

[Ande94] Ross Anderson, „A5 (Was HACKING DIGITAL PHONES)“, sci.crypt, 17. Juni 1994.

[BiSh99] Biryukov, A., Shamir, A., „Real Time Cryptanalysis of the Alleged A5/1 on a PC (preliminary draft)“. URL: http://cryptome.org/a51-bs.htm

[BSW00] Biryukov, A., Shamir, A., Wagner, D., „Real Time Cryptanalysis of A5/1 on a PC“, CRYPTO 2000, Springer, LNCS, 2000.

[BoRi98] Bogk, A., Rieger, F., „Security by obscurity“, Die Datenschleuder #63, 1998.

[BGW99] Briceno, M., Goldberg, I., Wagner, D., „A pedagogical implementation of A5/1“. URL: http://www.scard.org/gsm/a51.html

[CCC98] Chaos Computer Club, ftp://ftp.ccc.de/pub/gsm

[Golic97] Jovan Dj. Golic, „Cryptoanalysis of Alleged A5 Stream Cipher“, Eurocrypt ’97, Springer LNCS 1233, 1997.

[SDA98] The Smartcard Developer Association., „Smartcard Developer Association Clones Digital GSM Cellphones“. http://www.scard.org/press/19980413-01/

[WeKu98] Weis, R., Kuntze, R., „GSM-Algorithmen entschlüsselt“, Funkschau 11/98, Weka Verlag, 1998.

[WeLu98] Weis, R., Lucks, S., „Sicherheitsprobleme bei Authentifizierung und Verschlüsselung in GSM-Netzen“, in DuD 09/1998, Vieweg Verlag, 1998.

[Weis00] Weis, R., GSM Security Page, http://www.cryptolabs.org/gsm/

[Zen99] Zenner, E., „Kryptographische Protokolle im GSM-Standard: Beschreibung und Kryptanalyse“, Diplomarbeit, Universität Mannheim, 1999.