SIM-Karten
Geschrieben von Marc Ruef <marc.ruef@computec.ch <mailto:marc.ruef@computec.ch?subject=SIM-Karten>> für <http://www.computec.ch/>
Version 1.2b 02. April 2000

1.0 Inhaltsverzeichnis

2.0 Einleitung

Das SIM ist ein fester Bestandteil von GSM (Global System for Mobile Communications), und kann in zwei verschiedenen Kartenformaten vorkommen. Bei Mobiltelefonen, die einen öfteren Wechsel der SIMs vorsehen, wird das Format ID-1 verwendet, wobei bei Mobiltelefonen, bei denen nur selten ein Wechsel der SIM-Karten vorgesehen ist, die Karten mit der kleineren Abmessungen, wessen Format offiziell den Namen ID-000 trägt, zum Einsatz kommen. Diese kleineren Karten werden auch als Plug-In-Elemente bezeichnet. Um eine solche ID-000-Karte in einem Chipkarten-Lesegerät zu nutzen, welches für das Auslesen von ID-1 ausgelegt ist, kann eine sogenannte Mini-SIM Adapterkarte eingesetzt werden. Die Unterschiede dieser beiden Karten liegt weder in ihren technischen Gegebenheiten, noch in ihren logischen oder physikalischen Eigenschaften, sondern nur in ihren Formaten und der Grösse. Das SIM hat im GSM-Netz die Aufgabe, den Zugang zum Netz nur berechtigten Personen zu gewähren und dadurch gleichzeitig eine funktionierende und nicht manipulierbare Abrechnungs-Methode zu realisieren. Um dies zu ermöglichen, muss eine SIM-Karte zwei Funktionen einwandfrei erfüllen: Das Mögliche Speichern von Daten, den Zugang zu diesen Daten zuverlässig schützen und einen kryptografischen Algorithmus unter sicheren Bedingungen ausführen können.
Ursprünglich war geplant, die GSM-Chipkarten alle zwei Jahre auszutauschen, um Ausfällen vorzubeugen, da die Schreib-/Lesezyklen von EEPROMs leider mehr oder minder stark begränzt sind. Da sich in diesem Bereich jedoch verhältnismässig wenige Probleme ergaben, ersetzen die Netzbetreiber aus Kostengründen die SIM-Karten nur bei deren effektiven Ausfällen.

3.0 Die SIM im GSM-Netz

Das GSM-Netz ist die momentan weltweit grösste internationale Chipkarten-Anwendung mit über 6 Millionen eingesetzten Karten weltweit (Stand 1999). Sie ist die erste Realisierung, bei jener die Chipkarten den nationalen und internationalen Ansprüchen der Systembetreiber entspricht. Vor allem jenes ist für die Etablierung von Chipkarten verantwortlich zu machen. In vielen Chipkartenanwendungen wird der DEA (Data Encryption Standart) als kryptografischer Algorithmus verwendet. Da dieses Verschlüsselungsverfahren sehr bekannt, und somit vielen Versuchen einer Attacke ausgesetzt ist, von denen mit ziemlicher Wahrscheinlichkeit bald eine erfolgreich sein wird, benutzt man in der SIM einen eigens entwickelten, von DEA unabhängigen Algorithmus. Jener wurde lange geheim gehalten, und trägt den Namen COMP128.
Im Falle des Versuchs des Nutzens des GSM-Netzes für die Sprachdatenübertragung, ist die SIM-Karte dafür zuständig, dass das Mobile Equipment des Netzbetreibers den Kunden anerkennt, und ihm das Nutzen des Netzes zu erlauben. Der Prozess der Authentisierung ist durch das Hintergrundsystem des SIMs einseitig realisiert. Die Identifizierung der SIM geschieht mit einer im gesamten GSM-System einzigartigen Nummer, die eine maximale Länge von 8 Bytes aufweist, und IMSI (International Mobile Subscriber Identity) genannt wird. Anhand dieser Nummer kann der Teilnehmer vom System weltweit in allen GSM-Netzen identifiziert werden. Um die Identität des Mobil-Kunden so anonym wie möglich zu machen, wird, wann immer die Möglichkeit besteht, statt der IMSI eine TMSI (Temporary Mobile Subscriber Identity) genutzt, die nur innerhalb eines Teils des jeweiligen benutzten GSM-Netzes gültig ist. Aus der IMSI können die kartenindividuellen Schlüssel für die Authentisierungen und Verschlüsselungen der Daten auf der Luftschnittstelle abgeleitet werden. Die Verschlüsselung dieser Daten wird jedoch keinesfalls in der Chipkarte

selber, das heisst im SIM geleistet, da die Berechnungs- und Übertragunskapazität einer Chipkarte heute, und in naher Zukunft, noch nicht für die Echtzeitverschlüsselung von Sprachdaten ausreicht. Die SIM errechnet stattdessen einen temporären und abgeleiteten Schlüssel für die Übertragungsverschlüsselung und gibt ihn an das Mobile Equipment weiter. Jenes ist alsdann für die Verschlüsselungs- und Entschlüsselungsprozeduren zuständig.

3.1 Der Handshake von SIM und GSM-Basisstation

Eine Authentifizierung des Teilnehmers im GSM-Netz basiert auf dem typischen Challenge-Response-Verfahren. Startet ein Mobilfunkteilnehmer ein Gespräch, erstellt die Mobile Station kurz zuvor eine Verbindung zur best empfangenen Basisstation her, und übergibt jener eine Zufallszahl, die IMSI oder TMSI aus der SIM. Der Teilnehmer wird dann anhand einer Datenbankabfrage der Überprüfung unterzogen, ob er beim Netzteilnehmer registriert, sprich Kunde ist. Beim Gutfall erhält der Teilnehmer für die Luftübertragung eine Zufallszahl, welche an die SIM weitergeleitet wird. Diese benutzt nun diese Zufallszahl als Klartextblock für eine Verschlüsselung namens COMP128, deren Schlüssel jeweils karten- und teilnehmerindividuell ausfällt. Das Ergebnis dieser ganzen Prozedur ist ein Schlüsselblock, der via Mobile Equipment und Luftschnittstelle zur Basisstation übertragen wird. Das dort über Standleitungen angeschlossene Hintergrundsystem leitet aus der IMSI den kartenindividuellen Schlüssel ab und führt dann im weiteren die gleiche Berechnung wie die SIM aus. Nachdem der Schlüsselblock nun vom SIM beim Hintergrundsystem angelangt ist, muss jenes nur noch den selbst errechneten Schlüsseltext mit den empfangenenen Daten abgleichen, um über Erfolg oder Verderb der Authentisierung entscheiden zu können. Später wird für das Verschlüsseln der Sprachdaten ein Algorithmus namens A8 verwendet.

SIM (Chipkarte)	**Luftschnittstelle**	**Hintergrundsystem**
	-> IMSI / TMSI ->	Ki = f (IMSI, TMSI)
V	<- Zufallszahl (RND) <-	RNDKi=SR1
RNDKi=SR	-> SR ->	Falls SR=SR1, dann Teilnehmer authorisieren
`ME (Mobile Equipment): SprachdatenKC`	KC=Sprachdaten	enc (KC; Sprachdaten)
...	enc (KC; Sprachdaten)	...

3.2 Der Fehler im Algorithmus

Ian Goldberg und Dave Wagner vom ISAAC Forschungszentrum in Berkeley haben eine Schwachstelle in COMP128 entdeckt, die es ermöglicht, den für die Berechnung auf der Chipkarte benötigten, geheimen Schlüssel Ki zu extrahieren. Der Besitz eines Computers, eines Kartenlesegerätes und die Kenntnis des PINs (Personal Intentification Number) der Karte ist für das Wissen um Ki unabdinglich. Diese ganze Attacke, welche differentielle Kryptoanalyse genannt wird, läuft über bestimmte Kombinationen von etwa 150'000 Anfragen, die, wenn sie zu demselben Rechenergebnis kommen, bestimmte Bits des Schlüssels verraten. Gehen wir nun davon aus, dass 6,25 Anfragen von der SIM-Karte pro Sekunde beantwortet werden können, so würde eine Attacke auf eine solche Karte etwa 8 bis 12 Stunden an Zeit kosten. Diese Attacke nutzt einen markanten Fehler der Diffusion: Es wird eine Pipe in COMP128 eingesetzt, welche sich auf die Bytes i, i+8, i+16, i+24 bezieht. Beim zweiten Durchgang werden nocheinmal die selben Byte-Kombinationen eingesetzt. Insgesamt gibt es 5*8 Durchgänge bei COMP128. Die Bytes i, i+8 der Eingabe sind die Bytes i+8, i+16 und i+24 der Ausgabe der differentiellen Kryptoanalyse von COMP128. Jetzt wird durch die Pipe die Bytes i+16 durch i+24 ersetzt. Da die Umläufe non-bijective sind, können wir nun auf einen Zusammenstoss der i, i+8, i+16, i+24 hoffen, was bei der Ausgabe nach zwei Durchläufen der Fall sein sollte. Ironischerweise treten solche Gleichheiten mehr auf, als man dies vermuten könnte, da die Pipe nur mit 4 Bytes arbeitet. Zusammenstösse können daher erkannt werden, da sie einen Zusammenstoss in der Ausgabe von COMP128 verursachen - das heisst, es gleichen sich zwei Authorisierungs-Antworten. Danach kann jeder Zusammenstoss dazu verwendet werden, die Schlüsselbytes i, i+8 in Erfahrung zu bringen, was nach einer Analyse des zweiten Durchganges möglich sein sollte.

Wie angegeben, würde der Term 2^{4*7/2 + 0,5 } = 2^{14.5} ausreichen, um die beiden Schlüssel-Bytes - Jedes der vier Bytes der Ausgabe, nachdem der zweite Umlauf wirklich nur Werte von 7 Bit ausgibt - in Erfahrung zu bringen. Und folglich reicht dann die Anwendung von 8 * 2^{14.5} = 2^{17.5} aus, um den kompletten 128 Bits grossen

Schlüssel Ki herauszufinden. Somit ist also dieses kryptologische Verfahren nicht im Stande, gegen mathematischen Attacken auszuharren. Dieses Problem hätte gar nicht erst so weit um sich greifen können, wenn der Verschlüsselungs-Algorithmus der Öffentlichkeit von Anfang an präsentiert worden wäre. Dann wären Fehler in jenem viel schneller bekannt geworden. In Deutschland setzt nur D2 Privat auf COMP128, wobei jener Algorithmus in Europa jedoch relativ verbreitet ist. Was die Anbieter in der Schweiz einsetzen ist mir nicht bekannt, und offiziell will auch keiner der Anstalten verständlicherweise eine Stellungnahme abgeben.

4.0 Die Verzeichnis-/Dateistruktur der SIM

Das SIM hat ein hierarchisch aufgebautes Dateisystem, welches mit dem MF (Wurzelverzeichnis) und zwei DFs (Unterverzeichnissen), in denen sich die EFs (Dateien) mit den Daten für die Anwendungen befinden, ausgestattet ist. Die möglichen Dateistrukturen für die EFs sind transparent, linear fixed und zyklisch. Die zur Zeit 18 Standart-Befehle sind in der jeweils aktuellen GSM, heute Version 11.11, durch die Klasse A0 definiert. Die GSM 11.11-Spezifikation definiert 30 verschiedene EFs für die Anwendungsdaten, die in zwei DFs zusammengefasst sind. Die File Identifier (FID) der Dateien weisen die Besonderheit auf, dass das erste Byte der DFs immer 7F ist. EFs direkt unter dem MF müssen als erstes Byte des FIDs den Wert 2F haben und EFs unter einem DF den Wert 6F. Zusätzlich zu den spezifizierten Dateien kann der jeweilige Netzbetreiber eigene Dateien für Wartungs- oder Administrationszwecke im SIM speichern. Direkt unter dem MF befindet sich in einem transparenten EF eine im System einzigartige Identifikationsnummer der Chipkarte. Als Verzeichnisse sind ein DF für GSM-relevante Daten und ein DF für Telekommunikationsdaten vorhanden. Im GSM-DF existiert beispielsweise ein EF (EFLP) in welchem die bevorzugte Sprache gespeichert ist, in der dem Benutzer seine Daten am Display des Mobil-Phones angezeigt werden sollen. Sodann existiert auch ein EF (EFIMSI) mit der zugeteilten IMSI. In einer weiteren Datei (EFTMSI) ist die jeweilige TMSI mit einer zusätzlichen Ortsinformation abgelegt. Da diese Datei bei jedem Zellenwechsel im GSM-Netz und jedem Gespräch neu beschrieben werden muss, wird sie vom Betriebssystem der Chipkarte speziell geschützt. Die EEPROM-Seiten, welche oft nur maximale 10'000 Schreib-/Lesezugriffe erlauben, sind in dieser Situation nicht angebracht, da innerhalb der Lebensdauer der SIM diese Informationen viel öfter geschrieben werden würden. Im EFPHASE ist die Information über die Phase der GSM 11.11-Spezifikation gespeichert, die das SIM spezifiziert. Dort steht zur Zeit üblicherweise der Wert 2. Das zweite DF im SIM enthält ein EF namens ADN (EFADN), in welchem die Festrufnummern abgespeichert werden. Nach der Aktivierung eines Mechanismus in der GSM-Anwendung können nur mehr die Festrufnummern angewählt werden, wobei alle anderen Rufnummern blockiert sind. Die nächsten drei EFs (EFSMS, EFSMSS und EFSMSP) enthalten dir Informationen für den Kurzmitteilungs-Service (SMS), sowie diverse dazugehörige Statusinformationen, die über die Luftschnittstelle empfangen und dann zu einem beliebigen Zeitpunkt aus dem SIM ausgelesen werden können. Dies wird zum Beispiel für Broadcast-Messaging, ausgehend vom Netzbetreiber, verwendet, um dem Nutzer den Namen seiner gerade benutzten Mikro-Zelle mitzuteilen. In der letzten EF (EFLND) ist die letzte gewählte Nummer gespeichert.

Bei der Eingabe der 4-stelligen PIN, welche in GSM die Bezeichnung CHV (Chip Holder Virification) trägt, tritt eine kleine Besonderheit auf: Mit einem speziellen Befehl und der richtigen PIN können weitere PIN-Abfragen der Karte vom Benützer der Karte abgeschaltet werden, so dass weitere Eingaben der PIN entfallen und unnötig werden. Der prägnante Nachteil aus dieser Funktion tritt zu Tage, sobald die Karte verloren oder gestolen wurde, da somit dem neuen Besitzer der Karte die Funktionen, wenigstens von der Kartenseite her, unbeschränkt zur Verfügung stehen. Natürlich kann der Benutzer der Karte die PIN-Abfrage auch wieder durch die Inversion der vorher genannten Funktion aktivieren.

Verzeichnisstruktur einer Swissom-Karte

Dateityp FID Struktur
Grösse Read
Update Increment
Invalidate Rehabilidate
Beschreibung

MF 3F00
Wurzelverzeichnis

EFICCID 2FE2
transparent 10 Bytes
Immer Nie Nie Nie
Nie Identifikationsnummer der Chipkarte
DFSWISSCOM **7F10**
DF Swisscom
EFADN 6F3A linear fixed x
Bytes Immer Immer Nie
PIN2 PIN2 Kurzrufnummern (Abbreviated Dialling Numbers)
EFFDN 6F3B linear fixed x
Bytes Immer PIN2 Nie
Nie Nie Festrufnummern (fixed dialling numbers)
EF??? 6F3E ? ? Bytes ?
? ? ? ? Gruppen 1
EF??? 6F3F ? ? Bytes ?
? ? ? ? Gruppen 2
EF??? 6F3D linear fixed 5 x
14 Bytes PIN1 PIN1 Nie
Nie Nie Capability Configuration Pramaters
EFLND 6F44 cyclic x
Bytes PIN1 PIN1 Nie
Nie Nie letzte gewählte Rufnummer
EF??? 6F45 transparent x
Bytes PIN1 PIN1 Nie
Nie Nie Netznachrichten
EFSMSS 6F43 linear
fixed x Bytes PIN1 PIN1
Nie Nie Nie Zustand der gespeicherten Kurzmitteilungen (Short Message Service Status)
EFSMSP 6F42 linear
fixed x Bytes PIN1 PIN1
Nie Nie Nie Einstellungen für die Kurzmitteilungen (Short Message Service Parameters)
EFSMS 6F3C linear fixed 176
Bytes PIN1 PIN1 Nie
Nie Nie Kurzmitteilungen/Kurznachrichten (Short Messages)
EF??? 6F40 linear fixed 30
Bytes PIN1 PIN1 Nie
Nie Nie Eigene Rufnummern
EF??? 6F4A linear fixed 3 x
13 Bytes PIN1 PIN1 Nie
Nie Nie Rufnummernerweiterung 1
EF??? 6F4B linear fixed 3 x
13 Bytes PIN1 PIN2 Nie
Nie Nie Rufnummernerweiterung 2
DFGSM 7F20
DF GSM
EFLP 6F05 transparent x
Bytes Immer PIN1 Nie
Nie Nie Bevorzugte Sprache(n)
EFKC 6F20 transparent 9
Bytes PIN1 PIN1 Nie
Nie Nie Schlüssel Kc (Ciphering Key)
EFSPN 6F46 transparent 17
Bytes PIN1 Gesperrt Nie
Nie Nie Service Provider Name (Netzbetreibername)
EFPUCT 6F41
transparent 5 Bytes PIN1
PIN2 Nie Nie Nie
Preis der Einheit und Währung (Price per Unit and Currency Table)

EF??? 6F39 cyclic x
Bytes PIN1 PIN2 PIN1
Nie Nie Gebührenzähler
EFSST 6F38 transparent 4
Bytes PIN1 Gesperrt Nie
Nie Nie SIM Service Table
EF??? 6F37 transparent 3
Bytes PIN1 PIN2 Nie
Nie Nie Gebührengrenze
EF??? 6F30 transparent ??
Bytes PIN1 PIN1 Nie
Nie Nie Bevorzugte Netze
EF??? 6F31 transparent 1
Byte PIN1 Gesperrt Nie
Nie Nie Suchperiode für die bevorzugten Netze
EF??? 6F7B transparent 12
Bytes PIN1 PIN1 Nie
Nie Nie Verbotene Netze
EFIMSI 6F07 transparent 9
Bytes PIN1 Gesperrt Nie
Nie PIN1 IMSI
EF??? 6F78 transparent 2
Bytes PIN1 Gesperrt Nie
Nie Nie Access Control Class
EF??? 6F74 transparent 10
Bytes PIN1 PIN1 Nie
Nie Nie Broadcast Control Channels
EFLOCI 6F7E transparent 11
Bytes PIN1 PIN1 Nie
Nie PIN1 TMSI + Ortsinformationen
EFPHASE 6FAE
transparent 1 Byte
Immer Nie Nie Nie
Nie Phaseninformationen über GSM bzw. dessen Phasenidentifikation
EF??? 6FAD transparent 3
Bytes Immer Gesperrt Nie
Nie Nie Administrative Data

5.0 Das Übertragungsprotokoll

Die Kommunikation zwischen Mobile Equipment und SIM läuft mit dem Übertragungsprotokoll T=0 in den Standartparametern ab. Allerdings kann die Convention der Datenübertragung von der Karte mit Hilfe des ATR frei gewählt werden. Ein PTS ist vorgesehen, wird jedoch zur aktuellen Stunde noch nicht benutzt, da einige Vorschreibungen von T=0 dies (noch) nicht erlauben.

6.0 SIM-Karten selber bauen und simulieren

Zur erfolgreichen Simulation einer SIM-Karte wird die Ki und die IMSI benötigt. Die IMSI der Karte kann man, wenn man das Wissen um die PIN der Karte besitzt, direkt auslesen. Sie steht im elementary file 6F07.

Mit diesen Kentnissen kann man nun mit der Hilfe eines Computers diese SIM-Karte simulieren. Weiterhin benötigt man für den Klon noch ein Stück Hardware, Season-Interface oder Inverse-Reader genannt. Auch wird gemunkelt, dass mittels eines IMSI-Catchers on-the-fly eine SIM-Karte mit einem schnellen Computer real-time emulierbar ist.

Marc Ruef <marc.ruef@computec.ch <mailto:marc.ruef@computec.ch?subject=SIM-Karten>>
<http://www.computec.ch/>