

## FACTSHEET FS 2011-10

**Beveiligingsrisico's van GSM-communicatie****Inleiding**

GSM-telefoons zijn niet meer weg te denken uit onze maatschappij. GSM-telefoons worden gebruikt in een openbaar netwerk dat behalve voor telefonie inmiddels ook gebruikt wordt voor andere toepassingen zoals internetbankieren en authenticatie. Hierbij wordt gebruik gemaakt van de sms-functionaliteit voor het elektronisch bevestigen van transacties en het aantonen van de identiteit van een persoon.

Om af luisteren van GSM-communicatie te voorkomen wordt het draadloze deel van een GSM-verbinding versleuteld. Al meer dan tien jaar geleden zijn de eerste theoretische kwetsbaarheden van deze encryptie gepresenteerd. Later kwamen ook andere theoretische kwetsbaarheden van GSM-encryptie aan het licht. In 2008 zijn zogenaamde 'rainbow-tabellen' berekend waarmee de aanval op de GSM-encryptie aanmerkelijk versneld kan worden. Sinds 2009 heeft de onderzoeker Karsten Nohl diverse aanvallen gepresenteerd waarmee GSM-encryptie gekraakt kan worden, om communicatie daadwerkelijk af te luisteren en zelfs identiteitsfraude op het GSM netwerk mogelijk te maken.

Dit factsheet<sup>1</sup> geeft een overzicht van de belangrijkste kwetsbaarheden van GSM. Het bouwt voort op GOVCERT.NL Factsheet 2009-05 uit december 2009. Vanwege de mate waarin de GSM-risico's zich sindsdien hebben ontwikkeld is besloten de factsheet als een nieuwe publicatie uit te brengen.

UMTS of 3G is niet kwetsbaar voor de hier beschreven kwetsbaarheden. Het factsheet is bedoeld voor organisaties die gebruik maken van GSM en sms-diensten voor vertrouwelijke informatie of authenticatie. Het beschrijft de beveiliging van GSM en sms, de kwetsbaarheden die in de beveiliging zitten, de hierdoor veranderende risico's en hoe je je hiertegen kunt beschermen. Hierbij komen de volgende diensten van een mobiele telefoon aan de orde: mobiele telefonie, sms en mobiel internet.

**De GSM-infrastructuur**

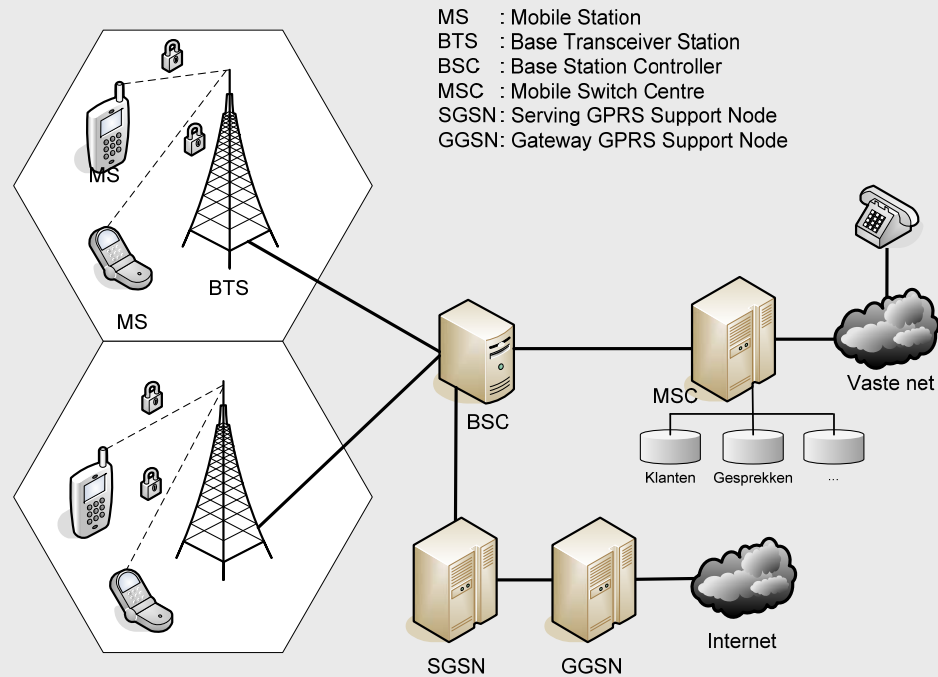
De GSM-infrastructuur bestaat uit verschillende componenten, schematisch weergegeven in figuur 1:

- Een mobiele telefoon (Mobile Station, MS) met Subscriber Identity Module (SIM). Op de SIM is de sleutel opgeslagen die wordt gebruikt voor het authenticeren van de klant op het GSM-netwerk. Deze sleutel wordt ook gebruikt voor het genereren van de sessiesleutels die voor het versleutelen van gesprekken worden gebruikt.
- Base Transceiver Station (BTS), ook wel basisstation genoemd, deze zorgt voor de draadloze communicatie tussen de mobiele netwerk provider en de mobiele telefoon.
- Base Station Controller (BSC), zorgt voor de aansturing van een aantal Base Transceiver Stations waaronder de handover van de mobiele telefoon van de ene BTS naar de andere.
- Mobile Switch Centre (MSC), dit is het hart van de mobiele infrastructuur. Het handelt de gesprekken, sms en andere diensten af. Het MSC zorgt voor het opzetten en verbreken van end-to-end verbindingen, zorgt voor mobiliteit en het monitoren van klanten. Hierin worden onder andere de gegevens over klanten, gesprekken en mobiele apparatuur bijgehouden.

**De belangrijkste feiten op een rij:**

- > Het encryptiealgoritme dat wordt gebruikt voor GSM-communicatie is kwetsbaar.
- > Hierdoor is misbruik door derden via het opvangen van communicatie, ontsleutelen en af luisteren mogelijk.
- > Het is getoond dat gesprekken en sms-berichten gericht zijn af te luisteren.
- > De kwetsbaarheden maken ook belfraude en identiteitsdiefstal mogelijk.
- > Op dit moment zijn de technische middelen die nodig zijn om gesprekken af te luisteren nog niet allemaal publiek beschikbaar. Op basis van wat al publiek is, is het voor iemand met goede kennis van GSM niet moeilijk de ontbrekende stukken in te vullen.
- > UMTS gebruikt encryptiealgoritmen die niet kwetsbaar zijn voor deze aanval.
- > Gebruik voor vertrouwelijke gesprekken mobiele telefoons op basis van UMTS technologie (met UMTS-only mogelijkheid) of overweeg het gebruik van crypto-telefonie.
- > Voer bij gebruik van sms-authenticatie een risicoanalyse uit. Overweeg zonodig de invoering van additionele maatregelen.

<sup>1</sup> Dit document is tot stand gekomen in samenwerking met AIVD/NBV.



**Figuur 1. GSM-infrastructuur**

### GSM-beveiliging

In GSM-communicatie worden verschillende vormen van encryptie gebruikt, die worden aangeduid met de letter A en een cijfer (zie referentie [1]):

1. Authenticatie (A3), waarmee de mobiele telefoon, en daarmee de klant, eenzijdig wordt geauthenticeerd.
2. Sleutelgeneratie (A8), voor het genereren van een sessiesleutel die wordt gebruikt voor de versleuteling van gesprekken.
3. Versleuteling (A5), voor de versleuteling van de gesprekken, sms en data. A5/1 is de sterkere variant van de twee initiële algoritmen voor A5 en wordt voornamelijk gebruikt in West-Europa en Noord-Amerika. Deze versleuteling wordt alleen gedaan tussen het basisstation en de mobiele telefoon.

Wanneer een mobiele telefoon zich aanmeldt bij een basisstation zal authenticatie plaatsvinden. Het mobiele netwerk stuurt via het basisstation een 'challenge' naar de mobiele telefoon. De mobiele telefoon berekent een 'response' hierop die in het mobiele netwerk wordt geverifieerd. De mobiele telefoon verifieert dus niet de authenticiteit van het mobiele netwerk (eenzijdige authenticatie).

Voor het versleutelen van de draadloze communicatie wordt eerst volgens het A8-algoritme voor sleutelgeneratie een 64-bits sessiesleutel aangemaakt, die enkele dagen geldig kan blijven. Het A8-algoritme is geïmplementeerd in de SIM. De gegenereerde sessiesleutel wordt door het A5-algoritme gebruikt om daadwerkelijk de spraak en data te versleutelen. Het A5-algoritme is geïmplementeerd in de telefoon. In de implementatie van A3 en A8 met het cryptografisch algoritme COMP-128 is in de loop der jaren een aantal kwetsbaarheden blootgelegd [2]. Omdat de meeste operators een eigen implementatie of nieuwere versie voor A3/A8 hebben gekozen, is de kans op aanvallen via COMP-128 kleiner geworden en niet het doelwit van deze aanval.

#### *Het sms-encryptie-algoritme*

Sms is ooit ontwikkeld voor het versturen van niet-gevoelige informatie over een GSM-netwerk. Daarom zijn basale beveiligingsmaatregelen als wederzijdse authenticatie, end-to-end versleuteling van tekstberichten en onweerlegbaarheid van het versturen of ontvangen van sms-berichten geen onderdeel geweest van het ontwerp van de gsm/sms architectuur. Voor de versleuteling wordt van hetzelfde algoritme A5/1 gebruik gemaakt als voor de versleuteling van gesprekken.

#### *Het GPRS encryptie-algoritme*

Datacommunicatie via GSM (GPRS) wordt met een ander algoritme versleuteld (GEA3-algoritme) dan spraak. In het verleden zijn ook in het GEA3-algoritme enkele zwakheden ontdekt.

## De aanval op het GSM encryptie-algoritme

Het A5/1-algoritme dat voor versleuteling van de gesprekken zelf wordt gebruikt, ligt zwaar onder vuur. Er zijn diverse onderzoeken gepubliceerd die kwetsbaarheden in dit algoritme blootleggen (o.a. [3]). In december 2009 heeft Nohl de vorderingen op dit gebied laten zien, waaronder de berekening en publicatie van de rainbowtabellen [4]. In juli 2010 heeft Nohl laten zien dat hij in staat is een versleutelde telefoonconversatie in verschillende losse stappen te ontsleutelen en af te spelen [5]. Het opvangen van de versleutelde telefoonconversatie was geen onderdeel van deze demonstratie. Een complicerende factor is dat gesprekken heel vaak van frequentie veranderen (frequency hopping) waardoor het opvangen van een gesprek moeilijk is. Een paar maanden later is gedemonstreerd dat onderzoekers in staat zijn sms-berichten gericht op te vangen en te ontsleutelen. In december 2010 hebben Sylvain Munaut en Karsten Nohl live tijdens de 27C3 laten zien dat ze daadwerkelijk een versleuteld gesprek kunnen opvangen, ontsleutelen en afspelen [6]. In december 2011 heeft Nohl tijdens het 28C3 congres de mogelijkheden van identiteits- en belfraude gedemonstreerd [7].

### Risico's aan het gebruik van gsm

Gebruik makend van de bekende zwakheden in de GSM-algoritmes, samen met de kraak van het GSM-encryptie-algoritme, zijn de volgende risico's ontstaan bij het gebruik van gsm:

- Het afluisteren van gesprekken

Met de kraak van het A5/1-algoritme is het mogelijk dat iemand die in de buurt staat van de beller, met de juiste ontvangstapparatuur straks dit gesprek 'draadloos' kan afluisteren. Dit is met name een risico voor gesprekken met een vertrouwelijk karakter. De kosten van de apparatuur die nodig is voor het afluisteren waren tot voor kort rond de € 1500. Onderzoekers hebben de kosten voor het opvangen van een GSM-signaal drastisch verlaagd naar enkele tientallen euro's. Hierdoor wordt het voor een groter publiek mogelijk om GSM-communicatie op te vangen en er mee te experimenteren.

Een andere aanvalsvorm, die misbruik maakt van de eenzijdige authenticatie, is zich met de juiste apparatuur voor te doen als een GSM-netwerk (false base station attack). Als de mobiele telefoon zich op een nep-netwerk aanmeldt, kan het gesprek vervolgens afgeluisterd worden. Deze aanval wordt ook wel IMSI-catching genoemd. Op sommige telefoons kan dit zichtbaar zijn met een open slotje op het scherm omdat er geen encryptie wordt gebruikt. Overigens kunnen gesprekken natuurlijk in het netwerk achter de BTS afgeluisterd worden, maar dan is er toegang nodig via de netwerkoperator.

GSM providers kunnen het afluisteren van gesprekken bemoeilijken door aanpassingen door te voeren in de manier waarop de communicatie versleuteld wordt (bijvoorbeeld door 'random padding').

- Het afluisteren van sms-berichten voor authenticatie

Op dezelfde manier waarop een gesprek afgeluisterd kan worden, kan dit ook voor sms-verkeer. Als de sms-berichten gebruikt worden voor authenticatie van gebruikers of om bij elektronisch bankieren transacties goed te keuren, kan dit mogelijk gebruikt worden bij fraude. Voor het inschalen van de risico's hiervan moet ook rekening worden gehouden met het volgende:

- Alleen een sms-bericht is meestal niet genoeg voor het uitvoeren van een transactie. Sms-berichten zijn vaak gekoppeld aan een gebruikersnaam en eventueel ook een wachtwoord, die dan allemaal nodig zijn voor een transactie.
- Sms-berichten worden alleen verstuurd als de mobiele telefoon aan staat. Deze worden in een beperkt gebied, de cel waar de telefoon op aangemeld is, uitgezonden. Ter indicatie: in een stad gaat het dan om een gebied van enkele honderden meters. Wanneer een aanvalleur een transactie wil uitvoeren ontvangt niet alleen hij maar ook het slachtoffer het sms-bericht. Omdat het slachtoffer deze sms niet verwacht, kan hij achterdochtig worden en hierop actie ondernemen.
- Als de mobiele telefoon van het slachtoffer wordt nagebootst, bijvoorbeeld door het klonen van de SIM of het uitvoeren van een spoofing aanval, kun je het bericht ook ontvangen als de telefoon van het slachtoffer uitstaat, en zonder dat het slachtoffer het bericht zelf ontvangt. Het klonen van een SIM is een moeilijke opgave, zeker zonder de SIM in bezit te hebben.
- Als de mobiele telefoon ook voor mobiel internet wordt gebruikt, en de mobiele telefoon is besmet met malware dan zouden de sms-berichten hiermee ook opgevangen kunnen worden en voor een aanval misbruikt kunnen worden.

Hierdoor is het moeilijk een grootschalige aanval op te zetten op diensten die van sms-berichten gebruik maken. Het uitvoeren van een gerichte aanval zal door het kraken van het A5/1-algoritme wel makkelijker worden.

GSM providers kunnen het afluisteren van SMS-berichten bemoeilijken door aanpassingen door te voeren in de manier waarop de communicatie versleuteld wordt (bijvoorbeeld door 'random padding').

- **Belfraude en identiteitsdiefstal (spoofing)**

De sleutel om berichten en gesprekken af te luisteren kan ook worden gebruikt om iemands identiteit op het GSM-netwerk tijdelijk over te nemen. Naast de sessiesleutel zijn dan een beperkt aantal gegevens nodig die afgeluisterd kunnen worden tussen mobiele telefoon en zendmast.

Deze kwetsbaarheid kan ernstige consequenties hebben, omdat er op het tegoed of abonnement van een ander gebeld kan worden. Ook kunnen betaalnummers gebeld worden met de opgevangen gegevens. En ten slotte kan iemands identiteit overgenomen worden voor zowel het voeren als beantwoorden van gesprekken, als het ontvangen en versturen van sms-berichten.

Aan deze aanval zijn echter een tweetal beperkingen. Ten eerste dient de telefoon van de aanvaller in hetzelfde gebied (location area) te zijn als het slachtoffer om de opgevangen gegevens te misbruiken. Als een aanvaller het gesprek van een slachtoffer wil beantwoorden of een sms-bericht wil ontvangen, moet de mobiele telefoon van het slachtoffer uit staan.

GSM-providers kunnen hun netwerk beschermen tegen deze aanval door een sessiesleutel niet voor meer dan één gesprek of sms te gebruiken.

### **Mogelijke maatregel: UMTS**

Als opvolger van GSM is UMTS ondertussen in gebruik. UMTS levert mobiele telefoondiensten en snelle datacommunicatie. De beveiliging van UMTS verschilt met die van GSM op twee belangrijke punten:

- **Encryptie:**

Bij UMTS wordt gebruik gemaakt van de UEA1-encryptie met een sleutellengte van 128 bits voor de versleuteling tussen mobiele telefoon en basisstation. De UEA1-encryptie van UMTS is beter dan A5/1 van GSM omdat de sleutellengte twee keer zo lang is. Verder is het UEA1-algoritme al lange tijd geleden gepubliceerd, in tegenstelling tot de GSM-encryptie, en is onderzocht door wetenschappelijke instellingen. Daarbij zijn er nog geen significante zwakheden gevonden.

- **Tweezijdige authenticatie**

UMTS heeft tweezijdige authenticatie: niet alleen is de handset door het netwerk geauthenticeerd, ook is de mogelijkheid ingebouwd dat de handset het netwerk authenticeert. Dit levert meer bescherming tegen een *false basestation attack*.

Daarnaast wordt in UMTS de integriteit van het signaleringsverkeer beveiligd met een aparte sleutel.

### **Aanbevelingen**

- Voor vertrouwelijke gesprekken is het verstandig rekening te houden met de risico's van GSM en gebruik te maken van het UMTS-netwerk. UMTS heeft een beter encryptie-algoritme en biedt daarmee een hoger niveau van vertrouwelijkheid. Daarnaast beschermt het gebruik van UMTS tegen aanvallen die gebruik maken van GSM-spoofing, gericht op belfraude en identiteitsdiefstal.
- Kies bij de aanschaf van nieuwe mobiele apparatuur voor toestellen met een UMTS-only functie. Dat voorkomt dat de telefoon (ongemerkt) overschakelt op GSM voor betere ontvangst. Overweeg aparte cryptotelefonietoepassingen voor zeer gevoelige of als Staatsgeheim gerubriceerde informatie. Door beperkte dekking is het echter niet altijd mogelijk van UMTS gebruik te maken.
- Aanbieders van sms-authenticatiediensten moeten bepalen hoe zij met de veranderende risico's van sms-berichten omgaan. Voer bijvoorbeeld een risicoanalyse uit en overweeg de implementatie van aanvullende preventieve, detectieve of correctieve maatregelen. Denk hierbij ook aan mogelijkheden die aanvallers hebben om gericht iemand af te luisteren. Ontwikkel geen nieuwe sms-authenticatietoepassingen die afhankelijk zijn van versleuteling tussen BTS en mobiele telefoon. Houd er rekening mee dat klanten niet massaal overschakelen op UMTS.

### **Tot slot**

Het af luisteren van mobiele GSM kan het vertrouwen van gebruikers ernstig schaden, ondanks dat bijvoorbeeld het ontvangen sms-bericht alleen niet voldoende is om een transactie uit te voeren. Aanbieders van sms-authenticatiediensten moeten voorbereid zijn op vragen van klanten.

### **Referenties**

- [1] Een overzicht van GSM-standaarden is te vinden op de website van ETSI: [http://webapp.etsi.org/key/key.asp?full\\_list=y](http://webapp.etsi.org/key/key.asp?full_list=y)
- [2] Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer and Stephane Tinguely, *Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards*, mei 2002: <http://www.research.ibm.com/intsec/gsm.html>
- [3] Alex Biryukov, Adi Shamir, David Wagner, *Real Time Cryptanalysis of A5/1 on a PC*: <http://cryptome.org/a51-bsw.htm>
- [4] A5/1 cracking project: <http://reflexor.com/trac/a51>
- [5] Presentatie Karsten Nohl Blackhat 2010: [http://srlabs.de/research/decrypting\\_gsm/](http://srlabs.de/research/decrypting_gsm/)
- [6] 27C3 Berlijn, <http://events.ccc.de/congress/2010/wiki/Documentation>
- [7] 28C3 Berlijn, <http://events.ccc.de/congress/2011/wiki/Documentation>
- [8] Een goed overzicht van A5/1 (in het Engels) is te vinden op Wikipedia: <http://en.wikipedia.org/wiki/A5/1>