softScheck
we identify vulnerabilities others don't

‚IMSI-Catcher‘

Eine technische Bewertung für die Expertenanhörung
des Saarländischen Landtags zur Änderung des Verfassungsschutzgesetzes

Saarbrücken 13. März 2014

Prof. Dr. Hartmut Pohl, geschäftsführender Gesellschafter
Valeri Milke B.Sc., Senior Consultant
Lubomir Stroetmann, Junior Consultant

softScheck GmbH Köln

Inhaltsverzeichnis

1 Management Summary 2
2 Ziele 2
3 Funktion und Zielobjekte 2
4 Technischer Aufbau 3
5 Begriffsverwendung 3
6 Herausforderungen der Geräte und der steuernden Software 3
6.1 Covert Functions, Back Doors 3
6.2 Integrität der Software und Nutzdaten 3
6.3 Authentifizierung der Nutzer, unberechtigte Nutzung und Protokollierung aller Aktivitäten 4
7 Einsatzszenarien für Sicherheitsbehörden 4
7.1 Von der NSA eingesetzte Geräte 4
7.2 Schutzmöglichkeiten 4
7.3 UMTS 4
7.4 Sicheres Protokolldesign 4
8 Security Testing 4
9 Zusammenfassende Forderungen 5
10 Literatur 5

1 Management Summary

Telekommunikationsüberwachung durch Sicherheits- und Strafverfolgungsbehörden ist beim Mobilfunk nur dann möglich, wenn die Mobilgeräte-Nummer bekannt ist; anderenfalls muss die Mobilgeräte-Nummer des Netzteilnehmers mit Hilfe der International Mobile Subscriber Identity (IMSI) oder der Subscriber Identity Module (SIM)-Karte bei der Bundesnetzagentur abgefragt werden.

Wenn die SIM-Karte in einem anderen Land gekauft wurde und die Telefongesellschaft nicht angemessen mit deutschen Behörden kooperiert, kann die Mobilgeräte-Nummer nur aufwändig in Erfahrung gebracht werden.

IMSI-Catcher können den in der Umgebung befindlichen, mit Mobilfunk kommunizierenden Geräten[1] eine sog. stille SMS zusenden mit dem Ziel, die IMSI abzufragen. Darüber hinaus kann der Standort innerhalb der Reichweite des Catchers fortlaufend (Bewegungsprofil) festgestellt werden und es können Gespräche abgehört werden.

IMSI-Catcher wurden 1993 patentiert und werden seit 1998 als Produkt verkauft. IMSI-Catcher werden zunehmend – auch von deutschen Sicherheits- und Strafverfolgungsbehörden auf gesetzlicher Basis - eingesetzt. So wurden 2012 in Deutschland mit IMSI-Catchern über 300.000 „stille SMS" versandt [Heise 2013].

IMSI-Catcher dürfen nur mit behördlicher Genehmigung verwendet werden. Allerdings existieren keine Sicherheitsmechanismen, die eine illegale Nutzung verhindern können. Dementsprechend dürften auch fremde Nachrichtendienste und die Organisierte Kriminalität IMSI-Catchern nutzen.

Abnahme- oder sogar Sicherheitsprüfungen von IMSI-Catchern sind nicht bekannt. Die Einsatzrisiken von IMSI-Catchern werden im Folgenden dargestellt und es werden die notwendigen relevanten und erfolgreichen Security Testing Methoden zugeordnet**.**

2 Ziele

IMSI-Catcher werden in den folgenden Situationen eingesetzt:

1. Bei unbekannter Mobilgeräte-Nummer einer bekannten Person kann mit Hilfe des Catchers die IMSI abgefragt werden. Naturgemäß können dabei weitere Mobilgeräte erfasst werden, so dass die gesuchte Person ausgefiltert werden muss.
2. Sind die Mobilgeräte-Nummer und die zugehörige IMSI bekannt, kann der Standort einer Person festgestellt werden und es kann ein Bewegungsprofil erstellt werden - solange sich das Mobilgerät in der Reichweite des Catchers befindet.
3. Es können alle Mobilgeräte in der Reichweite des Catchers erfasst werden und damit abgeschätzt werden, wie viele Personen sich in der Reichweite des Catchers befinden (z.B. bei einer Demonstration).

Weiterhin können mit den derzeitig angebotenen Catchern auch alle von einem Mobilgerät geführten und ankommenden Gespräche und alle übertragenen Daten[2] abgehört werden.

Während des Catchens können die in Reichweite befindlichen Mobilgeräte gestört und blockiert werden; im letzteren Fall sind keine Notrufe möglich.

Bei geeigneter Programmierung des Catchers können auch Gespräche (Anrufer und Angerufener) simuliert werden. Es können Daten gefälscht und simuliert werden.

3 Funktion und Zielobjekte

IMSI-Catcher simulieren gegenüber einem im Mobilfunk kommunizierenden Endgerät eine Basisstation (Base Transceiver Station, BTS); gegenüber einer regulären Basisstation simuliert der Catcher ein Endgerät.

Zum Abhören kann die Verschlüsselung abgeschaltet werden. Nur die (simulierte) Basisstation kann vorgeben, ob verschlüsselt kommuniziert wird oder nicht. Damit ist es dem IMSI-Catcher möglich die Kommunikation in Klartext mitzuschneiden – ggf. auch zu modifizieren. Weiterhin werden mit Hilfe der Anfrage „Location Area Update" Standortinformationen der im Mobilfunk kommunizierenden Endgeräte ermittelt.

Endgeräte innerhalb der Reichweite eines IMSI-Catchers buchen sich bei ihm ein, wenn das Signal des IMSI-Catchers stärker ist als das Signal der regulären BTS. Dies ist möglich, wenn eine Authentifizierung zwischen Mobiltelefon und BTS nur einseitig durchgeführt wird (GSM). Lediglich das Endgerät au-

[1] Handys, Smart Phones, Tablets, Notebooks etc. – aber auch stationäre Geräte.
[2] Gespräche, SMS, MMS, YouTube, WhatsApp, Flickr, Twitter, Facebook, E-Mails, Surfen (Google, …) etc.

thentifiziert sich - nicht das BTS. Der IMSI-Catcher veranlasst das Endgerät per ‚stiller SMS' – einer auf dem Endgerät für den Nutzer nicht sichtbaren SMS, die Location-Update Prozedur einzuleiten. Der IMSI-Catcher führt mit dem Mobilgerät ein Handshake durch mit Identity Request und Identity Response - diese enthält die IMSI.

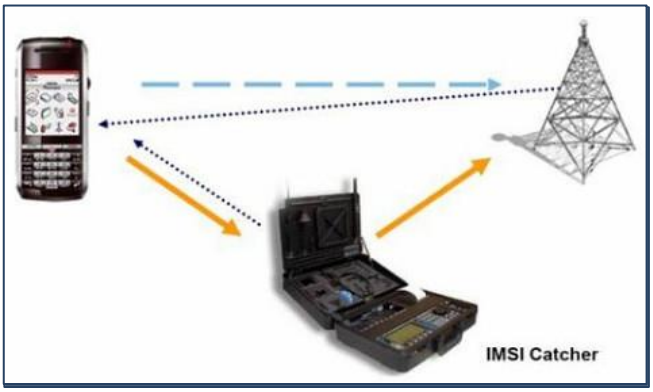

Abb.: Simulation einer Basisstation durch einen IMSI-Catcher [Zeus News 2011]

Zur Weiterleitung von Gesprächen benötigt die Basisstation eine eigene SIM-Karte.

Auch ist es möglich Kommunikation lokal zu verhindern, indem die ausgehende Kommunikation vom IMSI-Catcher verworfen und nicht an die reguläre BTS weitergeleitet werden (Denial of Service - Angriff).

Es werden mobile und stationäre IMSI-Catcher angeboten.

IMSI-Catcher können auch mit marktüblichen Komponenten selbst gebaut werden, der Aufwand liegt bei 1500 € [Heise 2010]; dazu kann die Open-Source-Software „OpenBTS" zum Simulieren einer Funkzelle des GSM-Netzes eingesetzt werden [OpenBTS 2014].

4 Technischer Aufbau

IMSI-Catcher und vergleichbare Geräte bestehen aus einem speicherprogrammierbaren Computer (mit Prozessor Hauptspeicher und peripheren Speichern) und grafischem Ausgabegerät (Bildschirm) sowie Sender(n) und Empfänger(n) für Mobilfunk. Über den Mobilfunk sind IMSI-Catcher an das Internet angeschlossen.

5 Begriffsverwendung

Die Funktionen von IMSI-Catchern gehen mit den Abhör- und Manipulationsmöglichkeiten - wie oben dargestellt - weit über ein Catchen von IMSIs hinaus. IMSI catchen ist also nur eine Funktion unter vielen. Solche Geräte sollten daher korrekt als „**Computer-gesteuerte Abhöreinrichtungen für den Mobilfunk**" bezeichnet werden.

Durch die Computersteuerung und damit mit beliebig auswechselbaren und erweiterbaren Programmen ist grundsätzlich eine uneingeschränkte Nutzung bis hin zum Missbrauch möglich.

6 Herausforderungen der Geräte und der steuernden Software

Da der IMSI-Catcher aus einem speicher-programmierbaren Computer besteht, können eine Reihe von IT-spezifischen Herausforderungen auftreten wie unberechtigtes Eindringen in diesen Computer (fremde Nachrichtendienste, Organisierte Kriminalität) zum Mithören und Verfälschen von Ergebnissen. Neben funktionalen Tests sind daher insbesondere Security Tests unverzichtbar.

6.1 Covert Functions, Back Doors

Die zur Steuerung des IMSI-Catchers eingesetzte Software sollte exakt dem Design entsprechen – also nicht weniger Funktionen enthalten, als im Design vorgegeben. Dies kann mit funktionalen Tests geprüft werden.

Die Software sollte auch nicht mehr Funktionen enthalten als die in der Dokumentation aufgeführten – also keine nicht-dokumentierten Funktionen (Covert Functions) und auch keine Möglichkeiten enthalten, auf Software und Daten unberechtigt über nicht-dokumentierte APIs (Back Doors) zuzugreifen. Dies lässt sich (nur) mit Security Tests überprüfen.

6.2 Integrität der Software und Nutzdaten

Aufgezeichnete Kommunikation kann verändert werden. Die Integrität der Kommunikation lässt sich

überprüfen, wenn eine Prüfsumme, besser eine kryptografische Prüfsumme eingesetzt wird.

Darüber hinaus ist es unverzichtbar, alle Ergebnisse mit einem überprüfbaren Datum und einer überprüfbaren Uhrzeit (Zeitstempel) zu versehen.

6.3 Authentifizierung der Nutzer, unberechtigte Nutzung und Protokollierung aller Aktivitäten

Es dürfen ausschließlich Berechtigte den IMSI-Catcher nutzen können; dazu müssen die Benutzer identifiziert und authentifiziert werden (z.B. mit einem Password, Token etc.).

Jegliche Nutzung muss mit Datum, Uhrzeit, Nutzer und durchgeführten Aktivitäten vom IMSI-Catcher gerichtsfest (mit einer digitalen Signatur ‚versiegelt') programmgesteuert protokolliert werden – die Protokolle müssen zeitnah ausgewertet werden.

7 Einsatzszenarien für Sicherheitsbehörden

7.1 Von der NSA eingesetzte Geräte

Von der NSA sind die folgenden Geräte zum Abhören von Mobiltelefonen bekannt:

- **CANDYGRAM** ist ein GSM-Basisstations-Simulator (für die Frequenzbereiche 900/1800/1900 MHz), der die Standortdaten der Handys von Zielpersonen über das Senden von nicht angezeigten SMS überprüft.
- **CYCLONE HX9** ist ein GSM-Funkzellensimulator für Angriffe auf GSM-900-Mobilfunkgeräte. Solche Basisstationen werden benutzt, um Handys abzuhören und Daten von ihnen abzufangen. Es besteht der Verdacht, dass die NSA damit etwa das Mobiltelefon von Bundeskanzlerin Angela Merkel abgehört hat.
- **NEBULA** ist ein GSM-Zellensimulator für 2G-Netze (900 MHz) und 3G-Netze (2100 MHz).
- **TYPHON HX**: Ein GSM-Zellensimulator für alle weltweit gängigen GSM-Frequenzen (850/900/1800/1900 MHz).

7.2 Schutzmöglichkeiten

Ein Schutz gegen IMSI-Catcher ist nur möglich, indem der Einsatz eines IMSI-Catchers durch Irregularitäten im Netzwerk erkannt werden kann und darauf hin die GSM-Verbindung unterbrochen wird. Eine Implementierung eines solchen IMSI-Catcher Detektors existiert bereits in dem Open-Source Projekt „CatcherCatcher" von SRLabs, welche auf der OsmocomBB-Platform unter Einsatz eines alten Motorola-Handys basiert.

7.3 UMTS

Im Gegensatz zu GSM schreibt UMTS eine gegenseitige Authentifizierung vor. So muss sich die Basisstation gegenüber Endgeräten authentifizieren, wodurch eine simulierte Basisstation auffallen würde. Da sich Handys derzeit aber automatisch mit GSM Stationen verbinden, wenn keine UMTS Station verfügbar ist, reicht es für einen Angreifer aus, die UMTS-Frequenzen mittels eines Störsenders zu blockieren. Dadurch weichen die Handys auf GSM aus und können mit dem IMSI-Catcher abgefangen werden. IMSI-Catcher einiger Hersteller haben eine solche Funktionalität bereits eingebaut.

7.4 Sicheres Protokolldesign

Sicherheit gegen eine simulierte Basisstation kann nur durch eine beidseitige Authentifizierung erreicht werden – nicht nur das Handy muss sich gegenüber der Basisstation, sondern auch die Basisstation muss sich gegenüber dem Handy authentifizieren. Ob ein Netzwerkprotokoll solche Sicherheitsvoraussetzungen erfüllt kann durch Threat Modeling der Protokollspezifikation überprüft werden.

8 Security Testing

Angriffe auf Computer und insbesondere Software sind nur dann erfolgreich, wenn Sicherheitslücken ausgenutzt werden. Ziel muss es daher sein, möglichst alle Sicherheitslücken zu identifizieren und zu korrigieren (patchen).

Dazu werden die folgenden Tool-gestützten Methoden eingesetzt:

- Threat Modeling: Untersuchung des Design der Software zur Identifizierung bislang nicht-erkannter Sicherheitslücken
- Static Source Code Analysis: Überprüfung des Quellcodes zur Identifizierung bislang nicht-erkannter Sicherheitslücken

- Penetration Testing: Identifizierung bereits bekannter Sicherheitslücken
- Dynamic Analysis – Fuzzing: Identifizierung bislang nicht-erkannter Sicherheitslücken im Maschinencode

Erfahrungsgemäß können erst durch den Einsatz dieser 4 Methoden alle Sicherheitslücken identifiziert werden.

9 Zusammenfassende Forderungen

1. Der **Begriff** ‚IMSI Catcher' kennzeichnet nur einen (kleinen) Teil der installierten Funktionen. Damit ist der Begriff irreführend – er sollte durch den Begriff ‚Computergesteuerte Abhöreinrichtung für den Mobilfunk' ersetzt werden.
2. Der Computer muss – wie andere Computer auch - unverzichtbar mit **Sicherheitsmaßnahmen** gegen jegliche unberechtigte Nutzung abgesichert werden. Berechtigte Nutzung muss gerichtsfest und damit nachvollziehbar vollständig **protokolliert** werden.
3. Bei der Abnahme muss das Gesamtsystem ‚Computer-gesteuerte Abhöreinrichtung für den Mobilfunk' mit allen Funktionen – insbesondere den Sicherheitsfunktionen - **einer Funktionsprüfung** unterzogen werden.
4. Die eingesetzten Programme müssen im Hinblick auf Korrektheit und Manipulierbarkeit **Security Tests** unterzogen werden.
5. Es muss sichergestellt werden, dass eine **Mitbenutzung** durch andere Behörden nicht erfolgen kann, weil ein Löschen der Ergebnisse und Zwischenergebnisse nicht vollständig erreichbar ist.

10 Literatur

Appelbaum, J.:	NSA ANT Mobilfunk o.O. o.J. http://cryptome.org/2013/12/nsa-ant-mobilfunk.pdf
Book, C.:	Networking & IT Security Blog. 2012 http://rfc791.de/2012/04/18/gsm-angriff-mittels-imsi-catcher
Fox, D.:	Der IMSI-Catcher. DuD - Datenschutz und Datensicherung 26, 2002, 4
Freist, R.:	Von Handys aufspüren und abhören. PCWelt ???: http://www.pcwelt.de/ratgeber/Silent-SMS-und-IMSI-Catcher-Handys-aufspueren-und-abhoeren-6144406.html
Heise (Ed.):	IMSI-Catcher für 1.500.- Euro im Eigenbau. 2010 http://www.heise.de/security/meldung/IMSI-Catcher-fuer-1500-Euro-im-Eigenbau-1048919.html
Heise (Ed.):	Handy-Überwachung: Bundesbehörden verschickten 2012 über 300.000 „stille SMS". 2013 http://www.heise.de/newsticker/meldung/Handy-Ueberwachung-Bundesbehoerden-verschickten-2012-ueber-300-000-stille-SMS-1951371.html
OpenBTS (Ed.)	Software Radio. 2014 http://openbts.org/
Schiffhauer, N.:	Lauschangriff auf Handys. FAZ-Net 9. August 2007 http://www.faz.net/aktuell/technik-motor/computer-internet/spionagetechnik-lauschangriff-auf-handys-1463546.html Nil07
SRLabs (Ed.)	CatcherCatcher. 2014 https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/CatcherCatcher

softScheck
we identify vulnerabilities others don't

Prof. Dr. Hartmut Pohl
Geschäftsführender Gesellschafter
softScheck GmbH Köln www.softScheck.com

Büro: Bonner Str. 108. 53757 Sankt Augustin

Tel.: +49 (2241) 255 43 - 12
Mobil: +49 (172) 9437 - 329
Fax: +49 (2241) 255 43 - 29

Hartmut.Pohl@softScheck.com