



Alle Artikel und Hintergründe

02.08.2010

[Drucken](#) | [Senden](#) | [Feedback](#) | [Merken](#)

## HINTERGRÜNDE, ARTIKEL, FAKTEN

finden Sie auf den Themenseiten zu...

[Mobilkommunikation](#)

[Datenschutz](#)

[Hacker](#)

[ALLE THEMENSEITEN >>](#)

## MEHR AUF SPIEGEL ONLINE

**Hackerkongresse:** Die Verteidiger der digitalen Welt (01.08.2010)

**CCC-Congress:** Sicherheitsforscher hacken Mobilfunk-Verschlüsselung (29.12.2009)

**Hackerkongresse:** Abhörprogramm für Handys

## MEHR IM INTERNET

[Ettus Research LLC](#)

[OpenBTS](#)

## Billig-Abhörtechnik für Handys

# Lauschangriff für jedermann

Von Uli Ries



Fotostrecke: 4 Bilder

Uli Ries

**Nur wer Technik für 100.000 Euro kauft, kann fremde Handys abhören und mitschneiden - glaubten Experten bisher. Doch jetzt kommt die Lauschoffensive zum Schleuderpreis: Ein Hacker führt vor, dass es auch 1000 Euro und ein bisschen Gratis-Software tun.**

## DEF CON

**Wikipedia:** IMSI-Catcher

**WHISPER SYSTEMS:** RedPhone 0.1

SPIEGEL ONLINE ist nicht verantwortlich für die Inhalte externer Internetseiten.

ANZEIGE



The advertisement for neu.de features a smiling woman on the left. The main text reads "Singles in Ihrer Nähe!" (Singles near you!). Below this is a search bar labeled "Postleitzahl eingeben:" (Enter zip code:). A green button with a right-pointing arrow says "finden & flirten" (find & flirt). In the bottom left corner, there is a badge that says "DEUTSCHES INSTITUT FÜR SERVICE-QUALITÄT" (German Institute for Service Quality), "1. PLATZ Beste Singlebörse" (1st Place Best Single Marketplace), and "TEST 02/2010" (Test 02/2010).

Las Vegas/Hamburg - Diese Demonstration gehörte zu den brisantesten Events der [weltweit beachteten Hacker-Konferenz Defcon](#): Das Abfangen und Mithören von Mobiltelefonaten mit Hilfe einfachen, preiswerten Equipments. Das ist so illegal, dass der britische Hacker Chris Paget darauf verzichtete, sein Können quasi am lebenden Objekt vorzuführen. In Deutschland beispielsweise würden ihm dafür im schlimmsten Fall drei Jahre Knast drohen. Auch in Vegas verzichtete Paget darum darauf, seinen Mix aus einer [frei verfügbaren, etwas über 1000 Euro teuren Hardware](#) und einer speziell zu diesem Zweck [angepassten Linux-Variante](#) in einem echten Mobilfunknetz zu demonstrieren.

Stattdessen wählte er für seine Demonstration während der in Las Vegas stattfindenden Hackerkonferenz Funkfrequenzen, die in den USA nicht von Netzbetreibern genutzt werden. Handelsübliche Mobiltelefone verbinden sich dennoch mit dem Aufbau - zwei Minuten nach Start der Demonstration waren es bereits über 30 Stück.

"Insbesondere eure iPhones scheinen mein Funknetz zu lieben", ruft der Hacker dem Publikum zu. Sämtliche Kommunikation der gekaperten Smartphones wandert von nun an durch die Ausrüstung des [Hackers](#). Prinzipiell ließen sich die Telefonate vor der Weiterleitung fein säuberlich mitschneiden. Weder das belauschte Opfer, noch der Partner am anderen Ende würden etwas vom Mitschnitt bemerken.

Dass Pagets Aufbau praxistauglich ist, bestätigt ausgerechnet die für die weltweit verwendeten Mobilfunk-Standards verantwortliche GSM Association (GSMA). Gegenüber SPIEGEL ONLINE erklärt eine Sprecherin: "Der Einsatz einer gefälschten Basisstation ist ein möglicher Weg, um Telefonate zu belauschen."

Das Auftauchen des [Discount-IMSI-Catchers](#) ist ein Alptraum für die Netzbetreiber. Denn bislang vermochten lediglich Strafverfolger und finanziell potente Industriespione sich die mindestens 100.000 Euro und mehr kostenden Gerätschaften zu beschaffen. Die einen legal, die anderen auf dem Schwarzmarkt.

### **Auch verschlüsseltes GSM hält Angreifer nicht mehr ab**

Jetzt kann jeder technisch halbwegs versierte Kleinkriminelle auf die Pirsch nach spannenden Handytelefonaten gehen. Zwar verweist die GSMA auf eine ganze Reihe von technischen Vorkehrungen, die einen solchen Angriff eigentlich unmöglich machen sollen. Diese Mechanismen greifen jedoch nur, wenn sich Mobiltelefon und Funknetz mit Hilfe des modernen 3G-Standards, hierzulande besser bekannt als UMTS, verständigen.

Wie Paget im Gespräch mit SPIEGEL ONLINE erläutert, hebt er den 3G-Schutz jedoch spielend leicht aus: Seine Basisstation gaukelt dem Mobiltelefon lediglich die Fähigkeit zu unverschlüsselten GSM-Verbindungen vor. GSM ist der kleinste gemeinsame Nenner aller Mobiltelefone und heutiger Funknetze und lässt sich auch

standardkonform ohne Codierung betreiben. Aber auch herkömmliches, verschlüsseltes GSM hält Angreifer inzwischen nicht mehr ab: Der deutsche [Mobilfunk-Experte Karsten Nohl kann auch Mitschnitte von verschlüsselten Gesprächen knacken](#). Laut GSMA können Mobiltelefone prinzipiell durch eine Warnung im Display auf die fehlende Codierung hinweisen.

Keiner der von SPIEGEL ONLINE hierzu befragten Handyhersteller konnte oder wollte die Existenz einer solchen Warnfunktion jedoch bestätigen. Weder Platzhirsch Nokia noch Mitbewerber Motorola oder Research in Motion, Hersteller des bei Geschäftskunden beliebten Blackberrys, förderten Brauchbares zu Tage. Geschlossen ratlos zeigte man sich auch auf Seiten der Netzbetreiber. T-Mobile hüllt sich trotz diverser Anfragen in Schweigen, O2 und Vodafone verwiesen immerhin noch auf die GSMA. Chris Paget vermutet, dass den in jedem Telefon steckenden SIM-Karten die Fähigkeit zur Anzeige der Meldung genommen wurde - damit es in Ländern wie Indien, in denen die Codierung untersagt ist, nicht zu ständig neuen Warnmeldungen kommt.

### Gezielte Attacken sind nur schwer möglich

Pagets Attacke ist zum Glück für Netzbetreiber und deren Kunden nicht allein der rechtlichen Konsequenzen wegen in der Praxis nur eingeschränkt umsetzbar: Der Lauscher muss sein Equipment unbedingt in die unmittelbare Nähe seiner Opfer bringen. Halbwegs unauffällige Antennen lassen die Basisstation des Lauschers einen Kreis mit einem Radius von 20 Metern so mit Funksignalen ausleuchten, dass sich alle in der Nähe befindlichen Handys automatisch mit ihr verbinden. Denn die Telefone bauen stets Kontakt zur Basis mit dem stärksten Signal auf und nicht mit der, die die höchste Übertragungsrate verspricht. Letztere wäre in jedem Fall die von den gekaperten Handys verschmähte UMTS-Station des Netzbetreibers.

Außerdem kann die Hacker-Hardware jeweils nur maximal sieben Telefonate gleichzeitig abfangen und weiterleiten. Für sieben weitere wäre ein zweiter Aufbau notwendig. Außerdem bleibt es dem Zufall überlassen, welches Opfer dem Lauscher ins Netz geht. Gezielte Attacken sind somit also nur schwer möglich. Leer geht ein Angreifer auch aus, wenn sich sein Opfer bewegt und so in den Bereich einer anderen, legitimen Station kommt.

Einen wirksamen, weitreichenden

ANZEIGE



**Für Singles mit Niveau**  
Jetzt ElitePartner.de  
kostenlos kennenlernen und  
den richtigen Partner finden.



**4 % p.a. aufs Tagesgeld**  
Bei vollständigem  
Depotwechsel. Kostenloser  
Umzugsservice.



**Alte Schulfreunde finden!**  
Erfahren Sie kostenlos, was  
aus Ihren ehemaligen  
Schulfreunden geworden ist.

adcloud

Schutz gegen die Attacke gibt es  
bislang jedoch nicht - und  
relevant ist sie allemal:

Naheliegende Beispiele für Anwendungen wären das Belauschen von Hotelzimmern aus Nachbarräumen heraus, kostengünstige Industriespionage aus geparkten Fahrzeugen bis hin zu einer alptraumhaften Verschärfung des Stalking-Problems. Von Sittentätern über Kleinkriminelle bis zu leicht außerhalb der Legalität operierenden Privatdetektiven könnten sich etliche Zielgruppen für die Technik interessieren. Ein radikaler Wechsel zu UMTS/3G, der das GSM-Problem per Abschaltung lösen würde, kommt für die Netzbetreiber nicht in Frage. Zu groß ist ihre Furcht, dass über Nacht Millionen von Handy-Kunden ohne Empfang dastehen.

Abhilfe versprechen einzig Handys mit eingebauten Verschlüsselungsmechanismen. Solche bei hochrangigen Politikern und Wirtschaftsbossen beliebten "Merkel-Phones" sind jedoch teuer und sichern zudem nur, wenn beide Kommunikationspartner in ein Krypto-Handy sprechen. Das Gleiche gilt für Nachrüstsätze, wie sie für manche Nokia- und Blackberry-Modelle angeboten werden. Besitzer eines Android-Smartphones können sich kostenlos behelfen: Die Gratis-Software [RedPhone](#) verschlüsselt Telefonate unknackbar, wenn auch sie von beiden Gesprächspartner verwendet wird. Genau wie die GSM-Lausch- und Knackattacken entstammt auch RedPhone der Hackergemeinde - der offensichtlich daran gelegen ist, dass [Mobiltelefonieren](#) endlich sicher wird.

---

**DIESEN ARTIKEL...**

[Drucken](#) | [Senden](#) | [Feedback](#) | [Merken](#)

---

#### SOCIAL NETWORKS



---

#### FORUM



#### Diskutieren Sie über diesen Artikel

Die neuesten Beiträge:

insgesamt 1 Beitrag [zum Forum...](#)

---

heute, 13:06 Uhr von **Faust007**: **Man-in-the-middle-Angriff**

Ohne Verschlüsselung werden immer MITM-Angriffe erfolgreich sein. DECT geführte Gespräche werden mit wenig Aufwand [Com-On-Air-Karte und Linux Kenntnisse] abgehört. WLAN Netze auch WPA2 gesichert sind jetzt schon [...] [mehr...](#)

---

**Und Ihre Meinung? Diskutieren Sie mit! [zum Forum...](#)**

ANZEIGE



#### Private Krankenkasse 59€

TOP - Testsieger Private Krankenkasse ab nur 59,- Euro! Für Selbständige und Freiberufler

[Mehr Informationen](#)



#### TNT Express

Finden Sie in nur 3 Schritten die passende Versandlösung für Ihren Bedarf. Mit TNT Express!

[Mehr Informationen](#)



#### Traumpartner gesucht?

Finden Sie mit freenetSingles, der beliebtesten Partnerbörse Deutschlands, Ihren Traumpartner.

[Mehr Informationen](#)



## NEWS VERFOLGEN

Lassen Sie sich mit kostenlosen Diensten auf dem Laufenden halten:

[Hilfe](#)

alles aus der Rubrik [Netzwelt](#)

[Twitter](#) | [RSS](#)

alles aus der Rubrik [Netzpolitik](#)

[RSS](#)

alles zum Thema [Mobilfunk](#)

[RSS](#)

© SPIEGEL ONLINE 2010

Alle Rechte vorbehalten

Vervielfältigung nur mit Genehmigung der SPIEGELnet GmbH

## MEHR AUS DEM RESSORT NETZWELT

[BEST OF WEB](#)

[SILBERSCHEIBEN](#)

[BILDERWELTEN](#)

[ANGEFASST](#)

[ANGESPIELT](#)



**Netz-Fundstücke:** Was Sie im Internet unbedingt sehen müssen



**Das lohnt sich:** Die besten CD- und DVD-Schnäppchen



**Bessere Fotos:** So holen Sie ganz einfach mehr aus Ihren Bildern raus



**Gadget-Check:** Handys und anderes Spielzeug in Matthias Kremers Praxistest



**Game-Tipps:** Spiele für Computer und Konsole im SPIEGEL-ONLINE-Test

## ÜBERSICHT NETZWELT ▶▶

▲ TOP

### DER SPIEGEL



Inhalt  
Abo-Angebote  
Heft kaufen

### Dein SPIEGEL



Inhalt  
Abo-Angebote  
Heft kaufen

### SPIEGEL GESCHICHTE



Inhalt  
Abo-Angebote  
Heft kaufen

### SPIEGEL WISSEN



Inhalt  
Abo-Angebote  
Heft kaufen

### KulturSPIEGEL



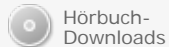
Inhalt

### Service von SPIEGEL-ONLINE-Partnern

#### AUTO UND FREIZEIT



Routenplaner



Hörbuch-Downloads

#### ENERGIE



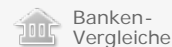
Gasanbieter-Vergleich

#### JOB

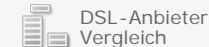


Gehaltscheck


#### FINANZEN UND RECHT




Banken-Vergleiche




DSL-Anbieter Vergleich


 Benzinpreis-  
vergleich


 Kfz-  
Versicherung


 Bußgeld-  
rechner


 Kliniksuche

 Bücher  
bestellen


 Arztsuche

 buch aktuell


 Partnersuche


 Das  
Telefonbuch


 Hotels


 Stromanbieter-  
Vergleich

 Energiespar-  
Ratgeber


 Energie-  
vergleiche

 Brutto-Netto-  
Rechner

 Uni-Tools


 2650  
Headhunter


 Ferientermine


 Kredite  
vergleichen

 Kranken-  
versicherung

 Währungs-  
rechner

 Versicherungs-  
vergleiche

 Handytarife

 Immobilien-  
Börse

 Prozesskosten-  
Rechner

 Rechts-  
beratung

[Home](#) [Politik](#) [Wirtschaft](#) [Panorama](#) [Sport](#) [Kultur](#) [Netzwelt](#) [Wissenschaft](#) [UniSPIEGEL](#) [SchulSPIEGEL](#) [Reise](#) [Auto](#) [Wetter](#)

#### DIENTSE

[Schlagzeilen](#)  
[RSS](#)  
[Newsletter](#)  
[Mobil](#)

#### VIDEO

[Nachrichten Videos](#)  
[SPIEGEL TV Magazin](#)  
[SPIEGEL TV Programm](#)

#### MEDIA

[SPIEGEL QC](#)  
[Mediadaten](#)  
[Selbstbuchungstool](#)  
[buchreport](#)  
[weitere Zeitschriften](#)

#### MAGAZINE

[DER SPIEGEL](#)  
[Dein SPIEGEL](#)  
[SPIEGEL GESCHICHTE](#)  
[SPIEGEL WISSEN](#)  
[KulturSPIEGEL](#)  
[UniSPIEGEL](#)

#### SPIEGEL GRUPPE

[Abo](#)  
[Shop](#)  
[SPIEGEL TV](#)  
[manager magazin](#)  
[Harvard Business Man.](#)  
[SPIEGEL-Gruppe](#)

#### WEITERE

[Hilfe](#)  
[Kontakt](#)  
[Nachdrucke](#)  
[Datenschutz](#)  
[Impressum](#)

 [TOP](#)