Deutschlandradio Kultur

Forschung und Gesellschaft am 1. September 2011

Manuskript

Deutschlandradio Kultur

Forschung und Gesellschaft

Reihe : **Forschung und Gesellschaft**

Titel : Hacker im Handynetz
Wie unsicher sind deutsche Mobilfunknetze?

Sprecher/in : Philip Banse

Redakteur/in : Jana Wuttke

Sendung : 01.09.2011 /19.30 Uhr

Regie : Klaus Michael Klingsporn

Besetzung :

Urheberrechtlicher Hinweis:

01 OTON 000113
Ich bereite es jetzt noch vor. Wir haben als Setup das 10-Euro-Telefon mit dem drei-Euro-Kabel an den Computer angeschlossen. Das Telefon ist der Dateneingangskanal in diesen Computer.

02 Sprecher
Karsten Nohl sitzt in seinem Büro in Berlin Mitte. Der Laminat-Boden ist flusenfrei, Besucher sollten ihre Schuhe ausziehen. Auf dem Schreibtisch steht ein ein aktuelles Notebook, angeschlossen ein umprogrammiertes Billig-Handy von Ebay, das alle Telefonate empfängt, die über einen bestimmten Mobilfunkmast, auch Zelle genannt, gehen. Das können an die 100 Gespräche sein. Diese Gespräche sind verschlüsselt, ein zunächst unlesbarer Datenstrom.

03 OTON 000148
Der Rechner kann die Daten jetzt mitschneiden. Er schaut jetzt, wann ein spezielles Telefon, das ich ihm gegeben habe, angerufen wird. Wir könnten das auch auf alle anderen Telefone ausweiten, aber dann wären wir nicht mehr legal.

04 **Sprecher**
Karsten Nohl ist ein bekannter Kryptologe und Sicherheits-Berater. Er zeigt, was in der Szene seit Jahren bekannt ist: Jeder mit etwas technischem Sachverstand kann mit ein paar Euro Handy-Telefonate abhören.

05 **OTON** 000230
Ich starte das mal. So, dann rufe ich mich selber mal an...

06 Sprecher
Karsten Nohl ruft mit seinem Handy ein anderes an, das neben ihm auf dem Schreibtisch liegt. Über Computer-Bildschirm rasen für Laien unverständliche Status-Meldungen.

07 OTON weiter
Du siehst hier da sich schon einiges verändert und es sieht aus als hätte wir das Gespräch schon jetzt geknackt, bevor wir dran gegangen sind. Ich spreche mal hier was rein:

08 **OTON** 001250
Test, 1,2,3. Das hier soll bitte mal geknackt werden.

09 **OTON** 001334
Keine Fehlermeldungen, das ist schon mal gut. Das hier sollte jetzt unsere Sound-Datei sein. (*Aus dem Lautsprecher:*) "Test ein, zwei drei, das soll geknackt werden." Das war jetzt das komplette kurze Gespräch, geknackt und mitgeschnitten.

10 MUSIK
(Rechenzentrum)

11 Sprecher
Das erste Handy-Telefonat führte ein Finne, der damalige finnische Premierminister Harri Holkeri. Ziemlich genau 20 Jahre ist das her. Die Technik von damals ist heute das Rückgrat des mobilen Telefonierens: Wenn wir mit dem Handy telefonieren, telefonieren sehr wahrscheinlich über GSM. Das Global System for Mobile Communications, ist für den weltweiten Mobilfunk, was der Verbrennungsmotor fürs Auto ist: Es gibt bessere Alternativen, aber ohne GSM geht nichts. Nahezu alle Mobilfunknetze der Welt fußen auf GSM - auch alle deutschen.

12 Sprecher
Natürlich können wir über telefonieren und SMS verschicken - aber jeder kann die Gespräche belauschen und die SMS lesen. Denn GSM ist alt und unsicher.

13 **OTON** Welte_000130
Als IT Sicherheitsmensch muss man sagen: Es ist sehr kaputt.

14 Sprecher
Sagt Harald Welte, ein Berliner Hacker, der in Asien Handyhersteller berät und zu den besten GSM-Kennern zählt.

15 **OTON** Nohl_5230
Das kommt aus den 80er Jahren. Da hatte man noch vor den Russen Angst und da wollte man verhindern, dass der Russe an gute Technik kommt. Deshalb hat man in die Telefone, von denen man ja wusste, dass man sie weitläufig verteilen würde, bewusst schlechtere Technik eingebaut als damals schon verfügbar war, um dem Russen das Aufholen so schwer wie möglich zu machen.

16 Sprecher
Natürlich gibt es 20 Jahre Einführung von GSM einen besseren Mobilfunk-Standard: Er heißt UMTS oder auch 3G. Doch diese kostbare neue Technik wollen Telekom, Vodafone und Co. nicht mit Telefonaten verstopfen: Surfen, Video, Spielen - moderne Telefone haben einen enormen Datenhunger entfacht, der nur über UMTS zu befriedigen ist. Telefonate wickeln die Mobilfunkanbieter daher weiterhin lieber über das veraltete GSM ab.

17 Sprecher
GSM überträgt jedoch längst nicht mehr nur Telefonate. GSM gilt als sicher. In blindem Vertrauen haben wir es fest verbaut ins Fundament unserer Gesellschaft: Die Bundeskanzlerin regiert per SMS; Notrufsäulen verschwinden, weil jeder ein Handy hat. Herzpatienten funken ihren Puls; Techniker regeln den Straßenverkehr; die Bahn steuert ihre Züge, Banken verschicken geheime TAN-Nummern – alles per GSM.

18 Sprecher
Dabei war der Mobilfunk lange eine geschlossene Kiste: Vorne geht Sprache rein, hinten kommt Sprache raus. Wie genau melden sich Handys beim Mast an? Wie genau werden unsere Gespräche verschlüsselt? Alles Betriebsgeheimnisse einer Handvoll Firmen. In jahrelanger Detektivarbeit haben Wissenschaftler und Hacker diese Kiste geöffnet und können jetzt tief in den Maschinenraum des Mobilfunks schauen - und siehe da: eines der wichtigsten technischen Systeme unserer Gesellschaft ist voller Fehler und Sicherheitslücken. Die Mobilfunkkonzerne könnten es weitgehend reparieren, scheuen aber offenbar die Kosten.

19 **OTON** 4540
Jetzt schneiden wir mit..... Das Radio schneidet so viel es kann auf dieser Frequenz mit..... soooo

20 **ATMO** 4230
(Zusammen bauen des Radio, Summen)

21 Sprecher
Fremde SMS zu lesen ist noch einfacher als Handy-Telefonate zu belauschen. Denn während eines Telefonats wird die Funk-Frequenz tausendfach und zufällig gewechselt, diesem Hopping muss der Angreifer folgen, das ist kompliziert. SMS dagegen werden stets auf der gleichen Frequenz übertragen.

22 **ATMO** 3545
Knistern, GSM Static

23 Sprecher
Wieder braucht Karsten Nohl nur ein altes Mobiltelefon und sein Notebook.

24 **OTON** 1720
Schick Du mir doch mal eine SMS unbekannten Inhalts.
(BANSE:) "So ich schicke jetzt eine SMS an das Telefon von Karsten Nohl und der Inhalt soll sein... ich schicke jetzt eine SMS mit geheimem Inhalt. So, fertig, schicke die mal ab."
Ich sehe sie auch, nicht die SMS, nur die verschlüsselten Daten..... so, jetzt lass ich mal das Analyse-Tool drüber laufen.

25 **OTON** 2745

Die interessante Nachricht ist sicher diese hier, die uns zum einen eine Telefonnummer gibt. Die dürftest du wieder erkennen
(BANSE: "Ja, das ist meine.")
Und die uns dann hier unten die SMS gibt: "Wahnsinn, GSM scheint ein Problem zu haben", sagt die SMS. Ja, und das ist auch so. Das hat jetzt hier auf diesem Computer - wenn wir konsequent eins nach dem anderen gemacht hätten - so um eine Minute gedauert.

26 Sprecher
Am meisten Mühe kostet es Nohl, wirklich nur sein eigenes Handy abzuhören. Mit krimineller Energie wäre die Sache einfacher:

27 **OTON** 1700
Dann könnte ich alle anderen SMS in 5 km Umkreis lesen, auch die Gespräche anhören.

28 Sprecher
Das Missbrauchspotential liegt auf der Hand: Von der Parkbank vor dem Bundestag etwa lassen sich viele interessante Telefonate und SMS abfangen. Natürlich höchst illegal, aber gefahrlos, denn der Angreifer hinterlässt keine Spuren. Geheimdienste und Polizei kennen die Schwachstellen von GSM seit Jahren - und nutzen sie, sagt Karsten Nohl.

29 **OTON** Nohl_011250
Die Boxen, die wir jetzt nachgebaut haben, sind schon lange am Markt für mehrere Hunderttausend Euro erhältlich. Hört sich viel an, aber Insiderhandel an der Börse, da kriegt man das schnell wieder rein. Da gibt es einen großen Markt, der genau solche Geräte seit langem handelt. Was natürlich jetzt passieren wird, ist, dass die Preise runter gehen werden. Es werden mehr Anreize geschaffen, auf Datendiebstahl zu gehen.

30 Sprecher
Abhören für Anfänger - die uralten und atemberaubenden Sicherheitslücken unserer mobilen Telefonie liegen jetzt offen zutage. Jeder kann sie nachvollziehen und erforschen. Wer hat das angestoßen, Karsten Nohl?

31 **OTON** Nohl_010236
Frag da mal Harald Welte, er war da eine zentrale Figur. Es ging einfach darum, dass es mal jemand macht. Dass sich mal jemand über viele Monate mit einem ungeheuren Sachverstand hinsetzt und diese akribische Protokolle runter schreib und die Arbeit jedem, der nach ihm kommt, erspart. Harald und Konsorten haben den Damm gebrochen.

*32 **ATMO** Welte - CCC runter / Sachen packen*
(Schritte durch die Wohnung, Papier raschelt)

33 **OTON** Welte - Rundgang Elektroniklab Reverseng (1)
Ich habe hier ein Oszilloskop, ich habe eine Lötstation, ich habe sehr viele Bauteile hier in allen möglichen Bauformen und Größen. Hier zerlege ich Geräte.

34 Sprecher
Harald Welte führt durch seine Werkstatt. Er ist Hacker, Sicherheitsforscher, Autodidakt. Ganz in Schwarz gekleidet bitte er in seiner Erdgeschosswohnung in Berlin Treptow zum Oolong-Tee, den er aus Taiwan mitgebracht hat. Harald Welte ist einer der führenden Mobilfunk-Forscher und berät Mobilfunknetzbetreiber in Europa und Afrika. Schon als Jugendlicher wollte er Technik nicht nur benutzen, sondern verstehen.

35 **OTON** Welte_000700
Ich mag Herausforderungen, wenn Leute das sagen, dass geht nicht, dann will ich zeigen: Geht doch.

36 Sprecher
Eine dieser Herausforderungen war GSM. Ein System, das wir alle jeden Tag nutzen, von dem lange aber nur einige wenige Firmen wussten, wie es wirklich funktioniert. Wie meldet sich ein Handy beim Funkmast an? Wie genau wird eine SMS verschickt? Wie genau läuft die Verschlüsselung ab? All das waren Betriebsgeheimnisse der Mobilfunkindustrie. Die wollte Welte lüften. Denn geheime Systeme haben immer Schwachstellen.

37 **OTON** Welte - Hacker Medienberichterstattung Boten
Ich sehe Leute wie mich, die eben Schwachstellen finden und die öffentlich dokumentieren und bekannt machen, als den Boten. Letztlich sind es nicht wir, die diese mistigen Systeme implementiert haben, sondern wir sind nur diejenigen, die das heraus finden. Oft kommt das in der öffentlichen Berichterstattung nicht heraus. Da sind das immer die bösen Hacker, die versuchen, jemanden übers Ohr zu hauen. Das ist einfach nicht der Punkt. Der Punkt ist, dass die Industrie nicht das nötige Augenmerk auf die Sicherheit legt.

38 Sprecher
Und so lud sich Harald Welte die GSM-Spezifikationen aus dem Netz. Das sind die öffentlich zugänglichen Spielregeln, nach denen GSM funktioniert. Tausende Seiten kryptischer, technischer Anweisungen, voller Querverweise und unbekannter Abkürzungen. Doch wer GSM erforschen will, braucht nicht nur ein Handy und die Basisstation eines Mobilfunkmasts. Ohne die passende Software sind die Geräte nicht mehr als ein Haufen Metall und Plastik. Nur mit der richtigen Software können Telefon und Mobilfunkmast miteinander sprechen, Gespräche abwickeln. Doch die Software ist Betriebsgeheimnis, und die Basisstationen wurden nicht frei verkauft und wenn, kostete alles ein Vermögen. Vor zwei Jahren jedoch tauchte so eine Mobilfunk-Basisstation bei ebay auf. Mehr noch: Es war nicht nur eine Empfangsstation im Angebot, sondern gleich 73. Harald Welte orderte alle und verkaufte sie an Mobilfunkforscher weiter, für 300 Euro das Stück.

39 **OTON** Welte - Hacks GSM
(Gerumpel) ... Das ist ein zehn Jahre altes Gerät von Siemens, deswegen so günstig inzwischen.

40 Sprecher
Harald Welte fing an, die GSM-Spielregeln, die er sich angelesen hatte, in Software zu gießen. Mit einer Handvoll Hacker schrieb er Software für die Basisstation, bastelte sich also seinen eignen Mobilfunkmast; er schrieb auch Software, damit sich Mobilfunkmast und Handy austauschen können. Irgendwann tauchte dann auch noch die Software eines bestimmten Mobiltelefons im Internet auf - damit war das System komplett. Und heute kann jeder ein eigenes GSM-Netz betreiben, sagt Harald Welte - für wenige Hundert Euro und mit einer Versuchslizenz von der Bundesnetzagentur sogar legal.

41 **OTON** Welte_002200
Die erste Folge ist eine Nachvollziehbarkeit der Schwachstellen. Forscher sagen seit langem, dass es Schwachstellen gibt. Aber auf die hat man nicht gehört, man hat immer gesagt: Zeigen sie das doch mal. Das Problem ist aber, bekannte Schwachstellen werden immer - durch wen auch immer - ausgenutzt werden: Geheimdienste oder organisierte Kriminalität. Einfach zu sagen, ach, das macht schon niemand, führt nicht weiter. Man muss es beheben und die Demokratisierung der Technik ist vielleicht der einzige Weg, den Druck aufzubauen, das zu beheben.

42 Sprecher
Es gibt aber auch Angriff auf das Mobilfunknetz, gegen die kein Kraut gewachsen ist.

43 ATMO
Chaos Communication Camp

Sprecher
Der ehemalige sowjetische Militärflughafen Finowfurt, 50 km nördlich von Berlin. Zwischen alten Kampfjets und Gras überwachsenen Hangars haben sich 3000 Hacker und Computer interessierte eingefunden zum Chaos Communication Camp, dem Hackertreffen des Chaos Computer Clubs.

ATMO hoch

44 Sprecher
Fünf Tage kampieren die Hacker in Zelten und Wohnmobilen, basteln, diskutieren und probieren neue Techniken aus.

45 **OTON** Stuge_000020
Wir haben unser eigenes GSM Netz aufgebaut.

46 Sprecher

Peter Stuge ist Schwede und arbeitet in Berlin an einem vom Bundesforschungsministerium bezahlten Projekt zu GSM-Sicherheit. Durch eine rostige Metalltür geht er leicht nach vorn gebeugt ins Innere eines der Hangars. Ein fensterloser Raum mit rohen Betonwänden, voller Kabel, Kisten und blinkender Rechner.

47 **OTON** Stuge_000320
Hier haben wir unsere erste Basisstation, diese Kiste eine Nokia Metroside BTS. Wir betreiben die mit 3 Radiomodulen, die sind auf dem Dach. ....

48 Sprecher
Ein eigenes Mobilfunknetz - das ist nur möglich, weil die Hacker um Harald Welte die Software geschrieben und ins Internet gestellt haben. An die 1000 Menschen haben über dieses Handynetz des Camps telefoniert, natürlich gratis.

49 **OTON** Stuge_001235
Wir machen das um die GSM zu verstehen, die Technik zu verstehen. Es ist interessant zu sehen, wie das alles funktioniert.

50 Sprecher
Denn wenn jeder sein eigenes Mobilfunknetz aufbauen kann, öffnen sich weitere Sicherheitslöcher. Denn die heutige Mobilfunktechnik wurde vor 20 Jahren entwickelt. Damals konnte sich keiner vorstellen, dass jeder Interessierte sein eigenes Mobilfunknetz einrichten kann. Und so galt beim Design der Technik die Annahme: Mobilfunknetze sind vertrauenswürdig. Eine Annahme, die sich heute als fatal erweist, sagt Peter Stuge:

51 **OTON** Stuge_001131
Das Telefon kontrolliert nie, dass es das richtige Netz ist. Wenn ich sage, das ist das richtig Netz, dann wird das nie überprüft. Ich muss nur sagen laut genug, ich bin O2, das reicht.

52 Sprecher
Die Mobilfunkprovider könnten einschalten, dass sich ihre Mobilfunknetze gegenüber den Telefonen ausweisen, Handys sich also nur mit legitimen Netzen verbinden. Aber das ist bisher nicht geschehen.

53 **OTON** Weinmann
IMSI 262420221539103 - ok to attack? *(Lachen, Applaus)*

54 Sprecher
Welche Gefahren für Handy-Nutzer entstehen, wenn jeder ein illegales Mobilfunknetz installieren kann, dass sich als legitimes Telekom-, Vodafone, 02 oder Eplus-Netz ausgibt, zeigte Jan Philipp-Weinmann von der Universitäten Luxemburg vor einem halben Jahr beim Kongress des Chaos Computer Clubs in Berlin. Demnach melden sich Handys einfach bei diesem falschen Netz an, erklärt Weinmann. Und wer immer

dieses falshe Netz betreibt, kann er Sicherheitslücken des Funkchips ausnützen, Software auf die Telefone spielen und sie komplett kapern, sie also zu Abhörwanzen machen, Telefonate mitschneiden oder sogar die eingebaute Handy-Kamera aktivieren.

55 OTON Weinmann **(Englisch)**
Übersetzer
Was ist das schlimmste Szenario, das man sich vorstellen kann? So eine kleine Mobilfunkstation ist so groß wie ein Ziegelstein, sie können das in ihrem Rücksack tragen. Sie können diese Station in sensiblen Gebieten aufstellen: am Flughafen, an der Europäischen Kommission, in Finanz- oder Botschaftsvierteln. Und dann nehmen sie Gespräche und übertragen sie zu sich. Bei einigen Handys lässt sich auch die Kamera aktivieren. Es gibt auch andere Szenarien, die mich wirklich schockiert haben. So sind einige BMW- und Porsche-Modelle mit Mobilfunk-Chips ausgestattet. Diese sind direkt mit dem Bord-Computer verbunden, der das Auto steuert. Die Hersteller wollen ihren Kunden so aus der Ferne bei Pannen helfen. Durch die Sicherheitslücken können sich diese Modelle aber in große ferngesteuerte Autos verwandeln.

56 **OTON** Welte_5945
Die Frage etwa, ob man so etwas wie einen Computervirus in ein GSM Netz injizieren könnte. Auch das sind hoch komplexe Rechnersysteme, die ein bisschen wie die Windows-Rechner in den 90er Jahren nicht auf Hacker-Einbrüche vorbereitet sind. Zum Beispiel das Szenario, dass ganze Städte mit umprogrammierten Telefonen vom GSM Netz getrennt werden könnten, ist denkbar.

57 Sprecher
Forscher wie Harald Welte und Jan-Philipp Weinmann stehen immer wieder vor der Frage, was sie machen sollen, wenn sie solche Sicherheitslücken entdecken.

58 **OTON** Weinmann
Übersetzer
Ich will, dass diese Lücken gefixt werden. Telefone werden für unser Leben wichtiger sein als Schreibtisch-Computer. Wir müssen die Hersteller drängen, Telefone sicherer zu machen. Ich habe diese Sicherheitslücken Herstellern der Funkchips in Mobiltelefonen gezeigt. Meines Wissens hat wenigsten einer von ihnen eigene Tests gemacht - und sieben Mal mehr Sicherheitslücken gefunden als ich.

59 **ATMO** Spaar_013200
(Gang auf Wiese, mit Unterhaltung)

60 Sprecher
Eine Schwäche der GSM-Technik, die selbst verantwortungsvolle Mobilfunkkonzerne und Chiphersteller nicht stopfen können, bekommen Interessierte in Spitzmäusing präsentiert, auf einem 100 Jahre alten Bauernhof abseits der Straße, 150 Autokilometer östlich von München.

61 **OTON** Spaar_013220

Wir gehen jetzt in den Ziegenstall. Die wissen, dass wenn sie von draußen von der Wiese rein kommen, dass sie ihr Futter erwarten können, deswegen wird jetzt erstmal das Futter in den Stall gebracht. Dann holen wir die Ziegen rein. (BANSE: „Wie viele sind das?“) Das sind sieben.

62 **ATMO** Spaar_013200
(Gang auf Wiese, mit Unterhaltung)

63 Sprecher
Dieter Spaar ist der Einsiedler unter den deutschen Mobilfunkforschern. Mit seinen sieben Thüringer Waldziegen lebt er auf einem alten Alleinlage-Hof mitten im Wald. In harten Wintern muss er einen Kilometer Schnee räumen, damit seinen Geländewagen zur Straße kommt. Der nächste Nachbar wohnt 500 Meter entfernt. Dieter Spaar hat einen für Großstädter unerträglich langsamen Internetzugang und auch mit dem kommerziellen Mobilfunk ist es nicht weit her in Spitzmäusing.

64 **OTON** Spaar_000140
Hier ist die Abdeckung ziemlich schlecht. Der Hof liegt in einer Senke, hier ist der Empfang - mittelprächtig, würde ich mal sagen.

65 Sprecher
Dieter Spaar ist Diplomingenieur der Elektrotechnik, selbstständig, er programmiert Software für Firmen.

66 **ATMO** Spaar_013630
Ziegen rennen vorbei

67 **OTON** Spaar_013650
Nur vor dem Rechner zu sitzen, kann´s hier auch nicht sein. Da ist das mit den Tieren ein schöner Ausgleich.

68 **OTON** Spaar_013730
Jetzt sind sie alle im Stall.

69 **ATMO** Spaar_013740 ATMO
(Ziegen fressen)

70 Sprecher
Auch für Dieter Spaar war GSM lange einfach zum Telefonieren da. Ein geschlossenes System, in das man rein spricht, damit auf der anderen Seite wieder Sprache raus kommt. Dann aber kaufte Harald Welte, der Berliner Mobilfunk-Hacker, diese Basisstation bei Ebay. Dieter Spaar bekam das mit und wollte ebenfalls mal sehen, ob er diese Geheimtechnik nicht zum Laufen bekommt.

71 **OTON** Spaar_002912

Das ist das Büro in dem die ich arbeite, in dem die Hobbyaktivitäten im Rahmen von GSM stattfinden.

72 Sprecher
Auf dem Schreibtisch - ein alter Windows-Rechner, Platinen und einige Bergkristalle. Hier wird Dieter Spaar jenen Angriff vorführen, der lange nur in der Theorie existierte.

73 **OTON** Spaar_003100
Das ist ein Denial of Service Angriff auf das GSM Netz. Da kann ein Telefon eine Zelle, nicht das ganze Netz, aber eine Zelle lahm legen. Der Angriff ist zwar nicht von mir entdeckt worden, theoretisch ist das schon lange bekannt. Aber ich wollte das mal ausprobieren ob das in der Praxis auch funktioniert.

74 Sprecher
Dank der Freizeitforschungen der letzten Jahre, konnte sich auch Dieter Spaar ein eigenes kleines Mobilfunknetz aufbauen. Die Basisstation, sein Funkmast, ist so groß wie eine Brotdose und steht neben dem Telefon. In seinen Händen hält Dieter Spaar zwei alte Mobiltelefone.

75 **OTON** Spaar_003745
Jetzt habe ich hier ein spezielles Telefon, in dem ist die Software im Telefon so modifiziert, dass es, wenn ich eine spezielle Nummer wähle, diesen Denial of Service Angriff auf das Netz startet.

76 Sprecher
Dazu muss man wissen: Jeder Mobilfunkmast bietet eine bestimmte Anzahl von Funk-Kanälen: 40 Kanäle bedeuten, dass 40 gleichzeitige Telefonate möglich sind. Wenn eine Handy eine Nummer wählt, bittet es den nächsten Mobilfunkmast um einen Kanal. Ist ein Kanal frei, reserviert der Mast ihn für einige Sekunden, damit sich das Handy verbinden kann. Falls keine Verbindung zustande kommt, wird der Kanal nach zwei Sekunden wieder frei gegeben. Normale Handys fragen möglichst selten nach einem Kanal, um nicht zu viele Reservierungen auszulösen und so den Mast zu blockieren. So sehen es die GSM-Spielregeln vor. Doch Dieter Spaars umprogrammiertes Telefon hält sich nicht an diese Spielregeln:

77 **OTON** Spaar_004109
Der Angriff funktioniert jetzt so, dass dieses Telefon dauernd sagt: Ich möchte einen Kanal. Dauernd heisst in dem Fall: Es sind im Schnitt 100 bis 200 Anforderungen pro Sekunde, die dieses Telefon stellt. Wenn man sich vorstellt: Ich habe nur 40 Kanäle, dann sind die nach einer knappen halben Sekunde alle belegt. Zwei Sekunden dauert es bis eine frei gegeben wird. Dann ist aber schon wieder die nächste Anforderung von diesem Angriffstelefon da, das heisst ich habe keinen freien Kanäle mehr. In der Praxis heisst das, jemand der jetzt ein Gespräch führen will oder angerufen wird, der kriegt kein Netz mehr.

78 Sprecher

Dieter Spaar hält die beiden Telefone an einen Verstärker.

79 **OTON** Spaar_004410
Das ist das Dauerfeuer *(lautes Knattern)* dieses Dauerfeuer setzt das Telefon ab, was dauernd Kanäle anfordert. So hört sich das an, wenn ein Telefon ganz normal das Netz anfordert.... *(GSM Knistern)* Wesentlich langsamer, ganz anderes Takten.

80 **OTON** Spaar_004240 Jetzt starten wir auf dem Telefon den den Angriff. Da wird eine spezielle Nummer gewählt *(BANSE: „####43")* Wenn ich das starte, man sieht´s auch auf dem Bildschirm, dann geht´s richtig los. Wenn ich jetzt einen Anruf zu machen, 2222, versuche zu telefonieren, aber es passiert nichts. Meine Software auf dem Bildschirm sagt nur, dass alle Kanäle belegt sind.

81 **OTON** Spaar_004822
Bei Ebay bekomme ich diese Telefon für 15 Euro, wenn jemand Schaden machen will, kauft er 100 solcher Telefone und legt die in einen Abfallkorb.

82 ATMO
Spaar Werkstatt

83 Sprecher
Die Telefone sind kaum zu orten und blockieren den Funkmast, solange ihr Akku hält. Damit lassen sich Notrufsysteme lahmlegen oder Mobilfunkprovider erpressen.

84 **OTON** Spaar_004615
Es ist nicht bekannt, dass das schon mal gemacht wurde. Ein Script-Kiddie hat davon nichts, man sieht ja nicht, was passiert, der Reiz ist nicht gross.

85 **OTON** Spaar_005140
Gegen diesen Angriff kann man nichts machen. ich könnte was neues machen, aber dann funktionieren Milliarden Telefone nicht.

86 **OTON** Spaar_005029
Als die Spezifikation geschrieben wurde, hat sich niemand vorstellen können, dass jemand außerhalb der Industrie so ein Telefon modifizieren kann, damit es Dinge macht, für die es nicht vorgesehen ist.

87 **OTON** Spaar_005651
Den Netzbetreibern ist es bekannt. Man wartet hier auch einfach ab, wir können eh nichts dagegen tun, warten wir mal ab. Was will er tun? Er kann nichts dagegen tun. Ich denke er muss abwarten und damit leben, wenn so was passiert.

88 Sprecher
Diese Strategie scheinen die Mobilfunkbetreiber auch an einer anderen heiklen Stelle ihrer Handynetze zu verfolgen: Dem Mikrowellen-Uplink.

89 **ATMO** Spaar_012100
Das ist das Lager, Messgeräte...

90 Sprecher
Ein Mobiltelefonat wandert vom Handy zum Mobilfunkmast. Von dort muss es ins Telefonnetz. In Großstädten sind die Mobilfunkmasten meist per Kabel ans Telefonnetz angeschlossen. Auf dem Land aber ist das mitunter zu teuer und so werden die gesamten Telefonate dieses Mobilfunkmasts per Funk übertragen. Dies geschieht mit Mikrowellen, Funkwellen, mit denen sich viele Daten gleichzeitig übertragen lassen. Die Funk-Strecke zwischen Mobilfunkmast und dem Telefonnetz nennen Experten Mikrowellen-Link.

91 **OTON** Spaar_005830
Man weiss, das bei GSM die Verschlüsselung geknackt ist, aber nach unseren Informationen ist auf diesen Mikrowellen-Links gar keine Verschlüsselung aktiv.

92 Sprecher
Das würde bedeuten, dass jeder eine passende Antenne in den Funkstrahl halten könnte und so nicht nur ein Telefonat belauschen könnte, sondern alle Telefonate, die über einen Funkmast abgewickelt werden, das können an die 100 Gespräche sein.

93 **OTON** Spaar_010430
Manchmal kommt man an die Antenne sehr leicht ran. Studenten haben die auf dem Dach, da sind die Mikrowellenantennen. Wenn ich aber den Mast habe, gibt es Bereiche, wo Nebenkeulen ankommen und ich guten Empfang habe. Oder hinter Antenne geht der Strahl ja weiter.

94 Sprecher
Bisher ist nicht bekannt, dass jemand auf diese Weise Gespräche im Zehnerpack abhört hat. Das liegt wieder mal den lange horrenden Preisen der Geräte. Die nötige Mikrowellen-Ausrüstung wurde ebenfalls nicht frei verkauft und kostete Zehntausende Euro. Jetzt werden diese Mikrowellen-Links langsam abgebaut - und landen bei ebay. Für unter 1000 Euro.

95 **OTON** Spaar_010220
Habe so eine Komponente... (*Gang in einen anderen Raum*) Das ist so eine Einheit... Wie so eine Tortenplatte, dahinter sitzt die Hardware, Ericsson Minilink, 26 GHz....

96 Sprecher
Dieter Spaar geht in einen Nebenraum und kramt zwischen Pappkartons eine Mikrowellen-Antenne hervor. Ein grauer Trichter, vorne verschlossen, groß wie eine Tortenplatte. Damit dürfte sich der eine oder andere Mikrowellen-Link abhören lassen.

97 **OTON** Spaar_010140
Müsste grundsätzlich grundsätzlich gehen, aber bisher nicht ausprobiert.

98 Sprecher
Auch hier liesse sich die Privatsphäre der Handykunden recht einfach schützen, sagt Dieter Spaar:

99 **OTON** Spaar_01650
Den Mikrowellen-Link zu verschlüsseln, ist kein Problem mehr. Es ist halt eine Investition. Der Operator müsste in Hardware investieren.

100 Sprecher
Jeder mit etwas technischem Sachverstand und krimineller Energie kann Handytelefonate abhören, SMS lesen und Handynetze teilweise lahmlegen. Es darüber hinaus möglich, Telefone komplett zu übernehmen und ihn Abhörwanzen zu verwandeln. Doch Mobilfunk muss nicht abhörbar sein; die Hürde für Angriffe ließe sich mit überschaubarem Aufwand entscheidend nach oben setzen. Die deutschen Mobilfunkbetreiber Telekom, Vodafone, O2 und E-Plus könnten viele dieser lange bekannten Sicherheitslücken schließen, sagt der Berliner Verschlüsselungs-Forscher Karsten Nohl. Beispiel SMS.

101 **OTON** 2810
Da gibt es eine Technik die ist genial einfach und bombastisch effektiv.

102 Sprecher
Wenn eine SMS übertragen wird, wandert nicht nur die reine SMS-Nachricht durch die Luft. Übertragen werden auch für Nutzer unsichtbare Informationen - manchmal meldet die Funkzelle dem Telefon auch nur: Ich habe Dir gerade nichts zu sagen.

103 **OTON** 2810
Allerdings ist in GSM jede Nachricht gleich lang, das heißt auch eine "Ich habe Dir nichts zu sagen"-Mitteilung wird auf die Maximalgröße aufgebläht. Und zwar erweitertet immer durch die gleiche Zeichenfolge. Hier siehst Du das Muster 2b2b2b und so weiter. Die einfache, aber sehr effektive Idee ist es, statt dieser vorhersagbaren Zeichenfolge einfach Zufallszahlen hier einzufüllen. Das ist alles. Setze überall Zufallszahlen ein - das macht es für uns, wenn das konsequent über alle Nachrichten gemacht wird, zur Zeit unmöglich, Nachrichten zu entschlüsseln.

104 Sprecher
Mehr Aufwand ist nötig, um auch die Telefonate sicher zu verschlüsseln. Die deutschen Mobilfunkunternehmen nutzen einen veralteten Verschlüsselungsstandard, mit dem Kürzel A5/1. Der Nachfolger A5/3 ist wesentlich besser, alle neuen Telefone beherrschen ihn - die Software der Mobilfunkmasten müsste allerdings aufgefrischt werden. Das kostet zwar Geld, aber dafür Mobil-Telefonate besser geschützt.

105 **OTON** 5411
Es würde jetzt darum gehen, die zur Zeit des kalten Krieges bewusst schlecht ausgewählte Kryptografie durch was Modernes zu ersetzen und an dieser offensichtlichen Aufgabe scheitern die Netzbetreiber zur Zeit.

106 Sprecher
Sagt Karsten Nohl.

107 **OTON** 2945
Wenn man so eine einfache Maßnahme seit drei Jahren nicht macht, dann läuft irgendwo was falsch. Dann geht es bei den drei Netzbetreibern, die es noch nicht gemacht haben, nicht um Kosten oder Aufwand, sondern darum, dass man sich des Problems noch nicht bewusst ist.

108 **OTON** Welte_000912
… Sicherheit im GSM-Kontext ist die Sicherheit der Netzbetreiber vor Betrug durch den Anwender. Aber die Sicherheit des Anwenders vor staatlicher Überwachung oder Organisierter Kriminalität, die interessiert niemanden.

109 **ATMO** 000045
Welte holt Mate und trinkt.

110 Sprecher
Dabei reagieren die Sicherheitsexperten deutscher Mobilfunkprovider durchaus erfreut auf seine Arbeit, sagt der Berliner Hacker Harald Welte.

111 **OTON** Welte_001040
Die Sicherheitsleute bei den Netzbetreibern sind immer begeistert, weil die oft wissen, dass da Probleme sind, aber keine Gehör finden beim Management, die sagen, wir verkaufen deswegen keine Telefon zusätzlich, warum sollen wir da was tun? Aber jetzt, da es teilweise in die allgemeine Öffentlichkeit dringt, steigt das Gehör auf die interne Sicherheitsabteilung der Netzbetreiber. Das ist schon mal ein guter Schritt in die richtige Richtung. Ob man dann das nötige Geld in die Hand nimmt, ist noch mal eine andere Frage. Aber es ist wichtig dieses Bewusstsein zu schaffen. Und es ist schon ein ernsthaftes Interesse da.

112 Sprecher
Warum installieren die deutschen Mobilfunkbetreiber keine aktuellen Verschlüsselungstechniken und lassen zu, dass Telefonate problemlos abgehört und SMS gelesen werden können? Wir hätten den Unternehmen gern die Möglichkeit gegeben, ihr Handeln zu erklären. Doch keiner der vier deutschen Mobilfunkbetreiber war zu einem Interview über die Sicherheit der GSM-Netze bereit.
Ï
113 Sprecher
Natürlich gibt es 20 Jahre nach der Einführung von GSM einen neuen, besseren Mobilfunkstandard: UMTS hat aus vielen Konstruktionsfehlern seines Vorgängers gelernt.

114 **OTON** 3200
UMTS ist nach heutigem Kenntnisstand sicher.

115 Sprecher
Sagt Kryptograf Karsten Nohl. Die Verschlüsselung der UMTS-Gespräche sei um Größenordnungen besser als bei GSM und heute nicht zu knacken.

116 Sprecher
Nur wenige Telefone lassen sich umständlich dazu zwingen, Telefonate über UMTS zu transportieren. Doch auch wenn die Verschlüsselung von UMTS heute nicht zu knacken ist - natürlich lassen sich auch UMTS-Gespräche abhören, sagt Hacker Harald Welte.

117 **OTON** Welte_001935
Es gibt auch bei UMTS Angriffe. Der einfachste ist: Aktuelle Telefone können ja GSM und UMTS. Und über den UMTS-Kanal kann man dem Telefon sagen: Schalte doch mal auf GSM zurück. Und damit kann man dann wieder die ganzen GSM Angriffe verwenden.

Verwendete Musik:

Sonho a Vida;
K & I: NeLaS;
Lizenz: http://creativecommons.org/licenses/by/3.0/
Info zur Gruppe & Download: http://www.jamendo.com/de/album/3649

Mijingiri Onion Killers;
K & I: exes alt;
Lizenz: http://creativecommons.org/licenses/by/3.0/
Info zur Gruppe & Download: http://www.jamendo.com/de/album/62022