MOBIEL GEH@CKT

Het lijkt een ware nachtmerrie: heb je net een romantisch smsje verstuurd aan je nieuwe vlam, kan je zus thuis op de computer precies lezen wat jij hebt geschreven. Is dit de realiteit? 'Nog niet', zegt de Nijmeegse informaticus Fabian van den Broek. 'Maar het is slechts een kwestie van tijd. Over een of twee jaar kan het al zover zijn.'

Tekst: Fabian van den Broek en Lieke Steijvers, Fotografie: Dick van Aalst, Illustratie: Ton Meijer

Eind 2009 stonden de kranten er vol van: hackers zijn erin geslaagd om de gsm-beveiliging te kraken! Binnenkort zijn alle mobiele telefoongesprekken afluisterbaar! De aanleiding was een publicatie van twee Duitse onderzoekers. Zij presenteerden op internet een enorme tabel met versleutelingscodes. Met die codes én de juiste apparatuur zou het mogelijk zijn gsm-signalen op te vangen en te vertalen naar een leesbaar sms of telefoongesprek.

Criminelen

Fabian van den Broek studeerde informatica in Nijmegen en schreef zijn scriptie over gsm-versleuteling. "Iedereen kan met de juiste apparatuur onbeveiligde gesprekken en sms'jes opvangen", zegt hij. "Er zijn tot nu toe nog geen criminelen gevonden met de juiste instrumenten om dit ook daadwerkelijk te doen, maar je kunt je voorstellen dat dit een enorm bedreigend scenario is."

Gsm is op dit moment het meest gebruikte mobiele netwerk. De communicatie tussen twee mobiele telefoons gaat altijd via een gsm-mast. Het is onmogelijk gesprekken zomaar uit de lucht op te vangen, tenzij je zélf die zendmast bent en beschikt over de versleutelingscode. Maar hoe krijg je die code in handen?

Een mobieltje stuurt tijdens een telefoongesprek of sms versleutelde pakketjes informatie naar de mast. Iemand die de pakketjes opvangt, kan deze dus niet lezen zonder de sleutel. Sommige van deze pakketjes zijn echter standaardpakketjes. Daarvan is de inhoud, vóór versleuteling, dus al bekend. Stel nou dat je alle mogelijke sleutels zou opschrijven in een grote tabel en daar de bijbehorende versleuteling van die pakketjes achter zet. Als je dan een van deze versleutelde pakketjes ontvangt, kun je simpelweg de bijbehorende gebruikte sleutel opzoeken. Daarmee kan je vervolgens ook de pakketjes waarvan de inhoud nog niet bekend is ontsleutelen. Als je tenminste het geduld hebt ze allemaal uit te proberen!

Schimmig

Ook als onderzoeker begeef je je soms op glad ijs, zegt Fabian. "Voordat de Duitse onderzoekers de versleutelingstabel op internet plaatsten, zijn twee Amerikanen zeven maanden bezig geweest aan een tabel. Maar ze hielden er ineens mee op. Zijn ze bedreigd? Is het ze verboden door de Amerikaanse staat? We weten niet precies waarom ze gestopt zijn, maar feit is dat de mobiele industrie een schimmige wereld kan zijn."

De gsm-versleuteling is al vijftien jaar in handen van één organisatie en is in die tijd nooit veranderd. Halverwege de jaren negentig zijn er zwakheden in de versleuteling gevonden maar providers gaven geen krimp. Zo zou een mobieltje je eigenlijk moeten waarschuwen tegen ongeautoriseerde zendmasten via een symbooltje van een open slotje in het beeldscherm. Maar veel providers zetten deze waarschuwing uit. "Het is een industrie waarin veel geld omgaat en veranderingen zijn duur. Nu komt het onderzoek gelukkig op gang en zal ook de mobiele industrie aan de bak moeten om de veiligheid te waarborgen", zegt Fabian.

Frequenties

De publicatie van de tabel betekent niet dat vanaf nu iedereen telefoongesprekken kan gaan afluisteren. Volgens Fabian hebben veel media die conclusie veel te voorbarig getrokken. De makers van de tabel zijn er zelf nog niet eens in geslaagd de versleuteling te doorbreken.

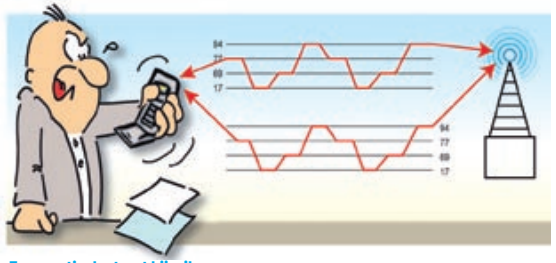
Om te beginnen is de hardware waarmee je zelf voor zendmast kunt spelen ontzettend duur. Maar belangrijker nog dan de kosten is de wisseling tussen frequenties. Tijdens een telefoongesprek verspringt de verbinding tussen de mobiele telefoon en de zendmast voortdurend heen en weer tussen de beschikbare frequenties (zie illustratie). Dit maakt het erg lastig om een gesprek goed op te vangen. Een methode om het gesprek toch te achterhalen is om verschillende gesprekken tegelijkertijd op te vangen en daar later het goede gesprek uit te filteren. Maar door de grote hoeveelheid data die je daarvoor vanuit je ontvanger naar je computer moet sturen, is dit voorlopig nog moeilijk.

Afluisteren

Los van deze praktische bezwaren is het afluisteren van mobiele gesprekken nog slechts een kwestie van tijd, zegt Fabian. "Ik verwacht dat de versleuteling binnen een of twee jaar wordt doorbroken en dat er ook een oplossing komt voor het frequentieprobleem. En dan is het hek van de dam natuurlijk. Om niet afluisterbaar te zijn, moeten providers overstappen naar nieuwe versleutelingen, maar dit is zeer kostbaar. En ook een nieuwe versleuteling kan weer worden doorbroken. Als je er echt zeker van wilt zijn dat je telefoongesprekken niet afluisterbaar zijn, dan moet je telefoons gebruiken die met software de gesprekken tussen de ene en de andere mobiel versleutelen, door sleutels uit te wisselen."

Ook kraker worden?

Wil je meewerken aan het betrouwbaar maken van mobiele telefoons? Ga dan informatica studeren. In Nijmegen ligt de focus op betrouwbaarheid van software in praktische toepassingen zoals de ov-chipkaart, stemcomputers en software in vliegtuigen.



Frequentie doet wat hij wil

Tijdens een telefoongesprek verspringt de verbinding tussen de mobiele telefoon en de zendmast voortdurend heen en weer tussen de beschikbare frequenties. Dit maakt het erg lastig om een gesprek goed op te vangen.