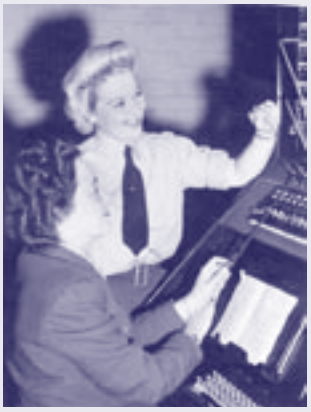
I Spy

Frank Brokken
f.b.brokken@rc.rug.nl

ICT-security

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.



Binnen de wereld van de IT security wordt traditioneel onderscheid gemaakt tussen 'black hat'- en 'white hat'-activiteiten. 'Black hat' heeft betrekking op ongewenste hackers-activiteiten, zoals inbraak en overname van computers door de hacker. Bruce Dorfman (1936) is de schilder die het afgebeelde schilderij *Black Hat* heeft gemaakt.

De black hat-hacker begint vaak met het afluisteren van de informatie die van en naar de computer wordt gestuurd die het volgende slachtoffer zou kunnen zijn. Veel communicatie is van nature persoonlijk of privacy gevoelig, niet alleen bij IT-toepassingen.

Denk maar eens aan de telefoon: een telefoongesprek kon altijd al worden afgeluisterd door het telefoongesprek bij de draad af te tappen. Dat is nog niet zo eenvoudig, tenzij je toegang hebt tot de centrale. Uit allerlei politiefilms en uit wat er zo nu en dan in het nieuws verschijnt, weten we dat het aftappen van een gesprek goed mogelijk is, vooral als je toegang hebt tot de telefooncentrale.

Met de komst van de mobiele telefoons is het aftappen van een telefoongesprek er alleen maar gemakkelijker op geworden. De communicatie wordt immers vrij in de ether rondgestraald door het zendertje dat we 'mobiele telefoon' noemen.
Ik ken niet veel mensen die zich daar zorgen om maken, maar er zijn in mijn omgeving om een of andere redenen wel vrij veel mensen die liever per telefoon, al dan niet draadloos, geen persoonlijke informatie verstrekken, bijvoorbeeld over zakelijke transacties.

Een ontwikkeling zoals we die bij de telefoon hebben gezien, van draadgebonden naar draadloos, zien we momenteel ook optreden bij de communicatie tussen computers. Iedereen kent wel de contactdoosjes waarin de ethernetkabels van onze computers worden geplugd.

Maar draadloze verbindingen zijn sterk in opkomst. Dat is begrijpelijk: wie draadloos kan werken kan (met name bij portable computers) praktisch overal gebruik maken van het internet en is daardoor niet meer afhankelijk van een vaste werkplek. De snelheid van zo'n draadloze verbinding (zo'n 10 Mbit/sec) is voldoende groot om snel te kunnen werken.

Maar hetzelfde type probleem dat we tegenkomen bij telefoonverbindingen, komen we natuurlijk ook tegen bij draadloos verbonden computers. De computers zijn voorzien van een antenne, die voor de communicatie met een ontvangststation, een 'access point' zorgt.

Terwijl het al goed mogelijk is om het verkeer dat via ethernetkabels loopt af te tappen om op die manier te proberen privé-informatie zoals inloggegevens of creditcardnummers af te luisteren, is zoiets bij draadloze verbindingen nog eenvoudiger.
Zowel zender als ontvanger zenden uit in een ongeveer cirkelvormig patroon en de hacker die geïnteresseerd is in afluisteren, hoeft maar ergens binnen die cirkels plaats te nemen met een portable die is voorzien van draadloze zend- en ontvangstmogelijkheden om de communicatie tussen access points en andere portables te kunnen afluisteren: een voor normaal gebruik uiteraard onwenselijke situatie.

De oplossing blijkt opnieuw versleuteling (encryptie) te zijn. Maar de praktijk blijkt iets minder eenvoudig te zijn dan het toepassen van 'zomaar encryptie'. Veel draadloze interface-kaartjes zijn voorzien van de mogelijkheid om encryptie en decryptie op respectievelijk verstuurde en ontvangen informatie toe te passen. Die versleuteling heet 'Wired Equivalent Privacy'.
Maar, zoals Bruce Potter en Bob Fleck (2002) in hun boek '802.11 Security' al schrijven (O'Reilly, 0-596-00290-4): "*There are many problems with WEP that greatly reduce its advertised security*".
Wie de details wil weten, leze Potter en Fleck's boek (en zie ook S. Fluhrer, I. Mantin en A. Shamir: '*Weaknesses in the Key Scheduling Algorithm of RC4*', op de securitypagina **security.rc.rug.nl/documenten/**).

In plaats van de eenvoudige WEP-encryptie werd bij eerdere gelegenheden gesteld dat hardware-encryptie, zoals die door bijvoorbeeld bepaalde CISCO draadloze LAN-interface-kaartjes werd aangeboden, diende te worden gebruikt. Die situatie is inmiddels door de tijd achterhaald.
Over het algemeen zullen de Nederlandse universiteiten nu overgaan op het gebruik van de 802.1X-standaard, een standaard voor authenticatie. Het is geen standaard die op zich iets met de toepassing van encryptie op de verstuurde informatie te maken heeft, maar de 802.1X-standaard kan goed worden toegepast bij zogenaamde EAP-TTLS-verbindingen. Hierbij is continu sprake van encryptie, ook na de authenticatie.

Het grote voordeel van EAP-TTLS is, naar mijn mening, dat we er op een aantal punten flink op vooruitgaan: de dure CISCO-kaart is niet meer nodig; er is sprake van continue encryptie bij een inherent onveilig medium (namelijk de draadloze verbinding tussen stations); en in principe kan iedereen gebruik maken van deze aanpak zonder verdere kosten. De EAP-TTLS-encryptie, tenslotte, kan worden afgedwongen door het access point waar de toegang tot het netwerk wordt geregeld. Dat lijkt me een positieve ontwikkeling.

Links

- Meer over het schilderij Black Hat van Bruce Dorfman is te vinden op **www.artoftheprint.com/artistpages/dorfman_bruce_blackhat.htm**
- S. Fluhrer, I. Mantin en A. Shamir: 'Weaknesses in the Key Scheduling Algorithm of RC4': **security.rc.rug.nl/documenten/**
- Een beschrijving van EAP-TTLS is verkrijgbaar via **www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-02.txt**
  Informatie over authenicatie en authorisatie voor WLAN m.b.v. 802.1X: **www.surfnet.nl/innovatie/wlan/**