Wachtwoorden

Frank Brokken
f.b.brokken@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.

Wachtwoorden, in goed Nederlands ook wel *passwords* genoemd, worden in praktisch alle gevallen gebruikt om de identiteit van gebruikers van computersystemen te verifiëren. De gedachte is simpel: vraag de gebruiker iets wat alleen hij/zij kan weten, en je weet dat je het met deze bepaalde gebruiker te doen hebt. Een soort elektronisch identiteitsbewijs, dus.

Good guys, bad guys

Aan het gebruik van passwords kleven natuurlijk ook bezwaren. De computer kan niet zien wie zich feitelijk identificeert (zoals een douanebeambte de foto in het paspoort kan vergelijken met het gezicht van degene die het paspoort presenteert), waardoor anderen kunnen proberen iemands wachtwoord te raden, om zich zo illegaal toegang tot een computer te verschaffen.

Dat is een bekend probleem met wachtwoorden: ze kunnen worden geraden. Dat is vooral een probleem omdat blijkt dat vrijwel iedereen gebruik maakt van triviale wachtwoorden: de naam van vriend/vriendin/echtgenoot/echtgenote, de naam van een huisdier, het automerk, de geboortedatum, de straatnaam, noem maar op. Wachtwoorden zijn vaak zo eenvoudig te raden, dat er computerprogramma's zijn geschreven die op die manier proberen wachtwoorden te raden, om zo ofwel (de *good guys*) mensen te informeren over het feit dat ze een zwak wachtwoord hanteren, zodat ze hun wachtwoord kunnen wijzigen, ofwel om (de *bad guys*) zich op die manier illegaal toegang tot computers te kunnen verschaffen (zie bijvoorbeeld **www.openwall.com/john**).

Uiteindelijk is, met voldoende tijd en geduld, elk wachtwoord te kraken. Niet dat dat altijd even eenvoudig is: het computersysteem dat ik gebruik, hanteert bij een foutief ingevoerd wachtwoord een oplopende wachttijd voordat ik het opnieuw mag proberen. Dat maakt het lastig om binnen een acceptabele hoeveelheid tijd een wachtwoord te achterhalen door steeds maar weer proberen te raden.

Briefje onder toetsenbord

Maar de universitaire 'Acceptable Use Policy' (AUP, **www.rug.nl/rc/security/aup**) geeft nog een paar extra adviezen: maak ook eens gebruik van hoofdletters (anders dan aan het begin), van cijfers en van leestekens. Maar bij dat soort wachtwoorden ontstaat een ander beveiligingsrisico: het wachtwoord wordt moeilijk te onthouden, en dus wordt het op een briefje geschreven dat onder het toetsenbord wordt geplakt. Zo is het middel natuurlijk erger dan de kwaal.

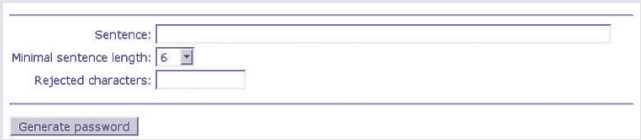
Om een wachtwoord dat niet uit een bekend woord bestaat toch te kunnen onthouden, kan de gebruiker gebruikmaken van een zin, waaruit het wachtwoord is afgeleid. De AUP geeft een paar voorbeelden: 'b1VidH' als wachtwoord, met als bijbehorend eenvoudig te onthouden zinnetje 'Beter één vogel in de hand...'. Mooi, zo'n regel. Je moet alleen oppassen dat je de zin waar je wachtwoord van is afgeleid niet meeprevelt wanneer je verbinding maakt met je computer....

De meeste leden van onze universitaire gemeenschap zijn wel in staat om zinnetjes te bedenken. Tenslotte kan elke zin daarvoor worden gebruikt: de titel van een favoriet boek, spreekwoorden, uitspraken, teksten uit liedjes, noem maar op. Maar hoe maak je daar nou een mooi wachtwoord uit? Dat is natuurlijk een deel van het creatieve proces, en daarom bij uitstek geschikt om door de computer zelf uitgevoerd te worden.

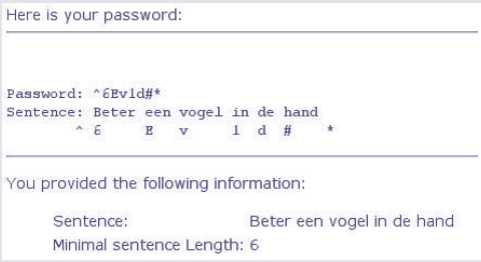
Wachtwoordgenerator

Onlangs werd ik benaderd door mijn collega Jaap Haaijer die in de context van zijn werkzaamheden een hele serie wachtwoorden moest genereren voor een aantal gasten van het RC. Na wat onderling overleg heeft dat geresulteerd in een aardig stukje gereedschap dat we voor iedereen ter beschikking hebben gesteld: een wachtwoordgenerator.

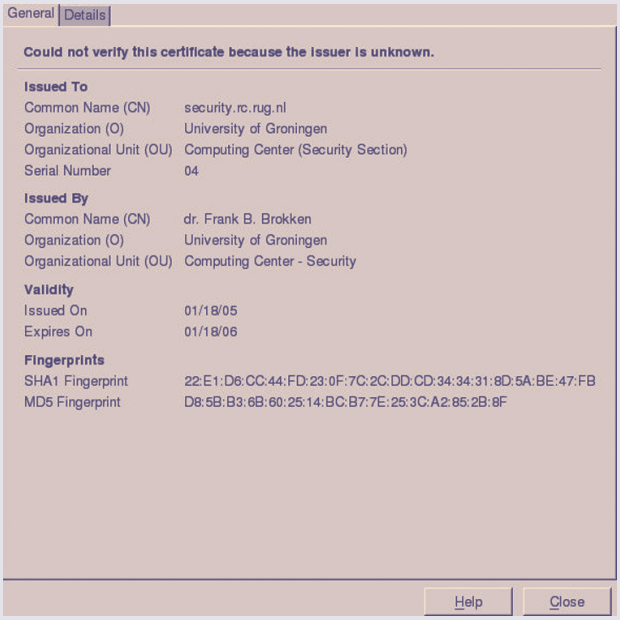
De gedachte is eenvoudig: vul een tekst in, waarvan het programma dan een wachtwoord afleidt. Bied dezelfde tekst nogmaals aan, en er wordt (zeer waarschijnlijk) een ander wachtwoord gegenereerd, dat opnieuw een nauw verband heeft met de ingevoerde tekst. Het programma is op zich niet bijzonder, en voert een aantal eenvoudige, intuïtief aansprekende transformaties uit op de ingevoerde tekst: soms worden kleine letters in hoofdletters getransformeerd, soms worden eenvoudige woorden vervangen door leestekens (bijvoorbeeld 'is' wordt '='), soms worden cijfers voor letters gesubstitueerd ('s' wordt '5', 'g'



figuur 1



figuur 2



figuur 3

wordt '9', etc.). De transformaties worden niet altijd uitgevoerd, dus niet elke 'g' zal als '9' in een wachtwoord terugkomen. Door dit toevalsgedrag kan het programma uit dezelfde zin hele series verschillende wachtwoorden genereren.

Op de webpagina **www.rug.nl/rc/security/adviezen/passwords** staat een hyperlink naar **https://security.rc.rug.nl/password**. Deze pagina toont een invulschermpje en een (instelbare) minimale zinslengte. Sommige computersystemen accepteren niet alle reguliere tekens (*characters*) in wachtwoorden. Dergelijke tekens kunnen eveneens worden gespecificeerd (zie figuur 1) voor een illustratie van de aangeboden invoervelden).

^6Ev1d#*

Laten we 'Beter één vogel in de hand' eens invullen. Na op 'generate password' te hebben geklikt, krijg ik ^6Ev1d#* (*zie figuur 2*).

Het dakje aan het begin en de asterisk aan het einde zijn leestekens die door het programma op toevallige wijze worden gekozen. Dat is dus telkens weer iets anders. Verder zien we de volgende substituties:

B(eter) → b → 6
e(en) → E
i(n) → 1
h(and) → H → #

Bieden we dezelfde zin nog een keer aan, dan krijgen we een ander wachtwoord. Bijvoorbeeld:

-61vIdh%

Maar telkens is er een duidelijke relatie tussen de ingevoerde zin en het gegenereerde wachtwoord. De ervaring leert dat na een paar keer intypen het wachtwoord, in combinatie met de gebruikte zin, erg goed kan worden onthouden. De voordelen zijn duidelijk: het wachtwoord wordt niet meer door standaard wachtwoordkraakprogramma's gevonden; het wachtwoord is goed te onthouden dankzij de zin waarvan het wachtwoord werd afgeleid, waardoor briefjes onder het toetsenbord overbodig worden; en het aantal zinnen waaruit wachtwoorden kunnen worden gegenereerd is onbeperkt.

Afluisteren

Tenslotte: **https://security.rc.rug.nl/password** is een https-verbinding. Dat betekent dat de verbinding tussen uw computer en 'security.rc.rug.nl' versleuteld is, en dus niet kan worden afgeluisterd. De *bad guys* zijn we op die manier kwijt, maar hoe weten we nou of de *bad guys* zich niet voordoen als security.rc.rug.nl? Op het moment dat uw browser voor de eerste keer verbinding maakt met security.rc.rug.nl wordt een certificaat getoond. Dat certificaat is hier gegeven in figuur 3.

De feitelijke verschijningsvorm van het certificaat kan per type browser enigszins verschillen, maar essentieel zijn de vermelde *fingerprints*. Als een *SHA1 fingerprint* wordt getoond, dan moet die gelijk zijn aan:
22:E1:D6:CC:44:FD:23:0F:7C:2C:DD:CD:34:34:31:8D:5A:BE:47:FB

Als een *MD5 fingerprint* wordt getoond, dan moet die gelijk zijn aan:
D8:5B:B3:6B:60:25:14:BC:B7:7E:25:3C:A2:85:2B:8F

Als dat niet het geval is, maak dan geen gebruik van de wachtwoordgenerator. Zijn de *fingerprints* wel gelijk aan de hier vermelde, dan kan er veilig gebruik worden gemaakt van de wachtwoordgenerator. Het gegenereerde wachtwoord wordt dan alleen aan uzelf beschikbaar gesteld.

Veel plezier met het genereren van veilige wachtwoorden

Frank B. Brokken
Security Manager.