Overpeinzingen aan het van het jaar...

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.

Onlangs, begin november, is de Annual Security Award voor de tweede keer uitgereikt. Deze keer niet aan leden van de universitaire gemeenschap zoals vorig jaar, die zich beroepshalve al met ICT-security bezighouden, maar aan Bas Keur en Marije de Vink, studenten aan de Faculteit der Rechten.

Juridische aspecten

Een goede ontwikkeling omdat het laat zien dat de Annual Security Award voor iedereen binnen de RUG bereikbaar is. Min of meer bij toeval sluit hun bijdrage goed aan bij het vorige onderwerp uit deze column (dat, om met collega Mark Godlieb te spreken, betrekking had op het onderwerp 'Hoe zet ik mijn computer bij het grofvuil').

De onderzoeksstage van Marije en Bas richtte zich op het gebruik van de digitale handtekening en encryptie. Dat is dan ook de titel van hun rapport: 'Digitale Handtekening en Encryptie'. Een boeiend onderwerp, zowel vanuit juridisch als technisch oogpunt. Voor wat betreft de juridische aspecten verwijs ik graag naar het onderzoeksverslag van Marije en Bas. Voor wat betreft de technische aspecten: het gebruik van digitale handtekening en encryptie is doorgaans gebaseerd op het gebruik van geavanceerde encryptietechnieken, die tot nog niet zo lang geleden slechts moeilijk konden worden gebruikt in combinatie met bestaande software (zie ook Pictogram van juni 2002).

Om nog even een korte samenvatting te geven: digitale handtekeningen en encryptie zijn gebaseerd op het volgende eenvoudige principe: er zijn twee kleine bestanden die respectievelijk de 'privé-sleutel' en de 'publieke sleutel' worden genoemd. De bijbehorende software maakt het mogelijk om een van beide bestanden te gebruiken om documenten en dergelijke te versleutelen, om vervolgens het andere bestand te gebruiken om het versleutelde bestand te decoderen.

Faken

Een prachtig systeem: wie iets zodanig wil beveiliging dat alleen de bedoelde lezer de informatie nog maar kan lezen, gebruikt de (algemeen beschikbare) publieke sleutel van de bedoelde lezer. Handig voor een document waarin privégegevens zoals passwords en pincodes worden bewaard.

Aan de andere kant: omdat ik als enige toegang heb tot mijn eigen privé-sleutel kan ik die gebruiken om een document te voorzien van een 'elektronische handtekening'. Iedereen kan nu, gebruik makend van mijn publieke sleutel (die immers publiek toegankelijk is), nagaan dat het document inderdaad door mij is getekend. Het krachtige van dit systeem is dat het niet is te faken en dat informatie

einde

die eenmaal is voorzien van een elektronische handtekening niet meer kan worden gewijzigd: elke wijziging maakt de handtekening ongeldig. Bij ongeschonden informatie rapporteert de software bijvoorbeeld:

```
gpg: Signature made Mon Nov
 29 21:06:06 2004 CET using
 DSA key ID 38C66170

gpg: Good signature
 from "Frank B. Brokken
 <f.b.brokken@rc.rug.nl>"
```

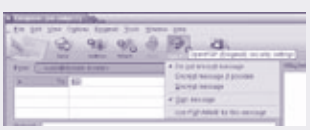
terwijl een (willekeurige) wijziging van het document wordt gestraft met:

```
gpg: Signature made Mon Nov
 29 21:06:06 2004 CET using
 DSA key ID 38C66170
gpg: BAD signature
 from "Frank B. Brokken
 <f.b.brokken@rc.rug.nl>"
```

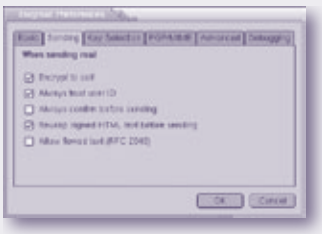
Authenticiteit

Digitale handtekeningen zijn met name handig voor wie wel eens e-mail verstuurt en de geadresseerde in de gelegenheid wil stellen om eenvoudig de authenticiteit van de afzender te verifiëren. Omdat de handtekening ook niet door met virussen geïnfecteerde computers kan worden gebruikt of geïmiteerd weet je als ontvanger ook, bij een intacte handtekening, dat eventuele attachments zoals door de afzender bedoeld zijn meegestuurd. In een wereld waarin digitale handtekeningen gemeengoed zijn wordt het voor een virus wel erg moeilijk om zich nog (automatisch) te vermenigvuldigen. Iets om over na te denken, zo aan het einde van het jaar....

Tot voor kort kon de software die beschikbaar was voor het gebruik van encryptie en digitale handtekeningen slechts met moeite worden gebruikt. Vaak werd van de gebruiker verwacht dat hij/zij overweg kon met slecht functionerende software die de gebruiker telkens weer met lastig op te lossen problemen confronteerde. Tegenwoordig kunnen echter ook standaard RUG e-mailprogramma's (zoals Mozilla Thunderbird) worden voorzien van goede plug-ins die het gebruik van encryptie en digitale handtekening eenvoudiger maken dan het schrijven van de documenten zelf: de simpele 'druk op de knop' is vaak het enige dat van de gebruiker wordt gevraagd. Die er een boel zekerheid en veiligheid voor terug krijgt.



In tegenstelling tot een paar jaar geleden is er nu eigenlijk geen reden meer om het gebruik van encryptiemogelijkheden en digitale handtekeningen nog langer uit de weg te gaan. Kortom, plaats de passende PGP/GPG plugin in uw e-mailprogramma (of laat 'm plaatsen door ICT-beheer) en neem eens de moeite om die nieuwe mogelijkheden te leren gebruiken. Uiteindelijk kan de universitaire ICT-security niet zonder uw medewerking. Met andere woorden: Don't be part of the problem, be part of the solution!



Alvast plezierige feestdagen en een veilige jaarwisseling toegewenst van

Frank B. Brokken
Security Manager
(Part of the Solution)

Links

- Annual Security Award:
  www.rug.nl/rc/security/award
- Mozilla Thunderbird:
  www.mozilla.org/projects/thunderbird/
- Mozilla Thunderbird GPG plugin:
  enigmail.mozdev.org/
- Surfnet Public PGP key server:
  http://pgp.surfnet.nl:11371/
- GNU Privacy Handbook:
  www.gnupg.org/gph/en/manual.html
- International PGP Home Page:
  www.pgpi.org
- The Protection of Your Secret Key:
  senderek.de/security/secret-key.protection.html