Re-encrypting

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

In eerdere Pictogrambijdragen is het PGP/GPG-concept bij herhaling genoemd als een manier om veilig e-mail te versturen.

De afzender kan op deze manier ervoor zorgen dat alleen de geadresseerde inzage heeft in de verstuurde e-mail, terwijl de ontvanger kan controleren of de ontvangen e-mail ook inderdaad afkomstig is van de afzender, in plaats van een grappenmaker die zich voordoet als iemand anders om u op die manier van de meest recente virussen te voorzien.

Met het beschikbaar komen van e-mailprogramma's als Mozilla Thunderbird is het 'dagelijks gebruik' van de bijbehorende encryptietechnieken wel heel eenvoudig geworden: voor encryptie is nog slechts de spreekwoordelijke druk op de knop nodig, voor een elektronische handtekening moet slechts een *pass-phrase* worden ingetypt.

Open en bloot

Binnen de RUG zijn echter ook groepen waarvan de leden onderling graag veilig e-mail willen uitwisselen. Denk aan het RC Security Kernteam of aan het RUG ICT crashteam. Discussies over te nemen beveiligingsmaatregelen en over de manier waarop de beveiliging concreet wordt gerealiseerd sturen we bij voorkeur niet 'open en bloot' over het internet. Zouden we dat wel doen, dan maken we het potentiële hackers wel heel erg eenvoudig, gezien het gemak waarmee e-mail kan worden onderschept.

Wat moet een lid van zo'n groep nou doen om veilig e-mail naar de medegroepsleden te versturen? Laten we de zaak eens op een rijtje zetten:

1. Elk lid moet alle publieke sleutels van alle leden in zijn of haar PGP-*keyring* hebben opgenomen. Dat is eigenlijk geen probleem, want daarvoor kan de PGP-programmatuur zelf zorgdragen.
2. Wanneer een lid e-mail wil sturen naar de overige groepsleden, moet voor elk lid van de groep worden aangegeven dat de versleuteling voor dat groepslid moet plaatsvinden. De PGP-software heeft daar geen problemen mee, maar het is een belasting voor de individuele groepsleden: de groepsleden moeten dan weten wie precies op dat moment lid is van de groep, waarna de e-mail vervolgens expliciet voor elk van de leden moet worden versleuteld, waarna de mail kan worden verstuurd naar de leden van de groep. Dat is complex, lastig, en erg gevoelig voor fouten. Bovendien: waren e-maillijsten niet uitgevonden om de groepsleden dat soort werk uit handen te nemen?

Re-encrypting remailer

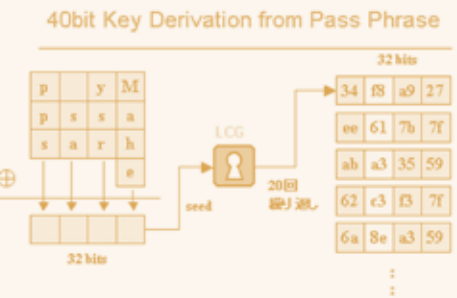
Een e-maillijst heeft een eigen e-mailadres. Het is eenvoudig om mail over de leden van een groep te verspreiden via zo'n lijst: de e-mail hoeft slechts naar de lijst te worden gestuurd en de lijstsoftware zorgt voor verdere ver-

g Remailer

spreiding. Zo'n lijst is echter lastig wanneer e-mail moet worden versleuteld, en dat is nou juist wat de leden van een groep die onderling vertrouwelijke informatie willen uitwisselen graag zouden willen doen.

Leden van een groep kunnen vertrouwelijke informatie op veilige wijze per e-mail uitwisselen wanneer ze gebruikmaken van een zogenaamde *re-encrypting remailer*. Het principe is eenvoudig:

1. De re-encrypting remailer is een programmaatje waar e-mail naar toe kan worden gestuurd. Met andere woorden de re-encrypting remailer heeft zelf een e-mailadres. Laten we het concreet maken: een bestaande groep, bijvoorbeeld het College van Bestuur besluit om in het vervolg vertrouwelijke informatie op veilige wijze onderling te verspreiden.
   Laten we aannemen dat er een mailing list cvb@rug.nl bestaat die tot nu toe altijd voor de verspreiding van e-mail over de CvB-leden is gebruikt. We gaan een re-encrypting remailer introduceren, en koppelen daaraan het adres cvbs@rug.nl, de 's' staat dan voor secure.
   Dus: naast een standaard cvb@rug.nl lijst is er een cvbs@rug.nl voor de uitwisseling van vertrouwelijke informatie.
2. De re-encrypting remailer voor het CvB krijgt nu zelf een PGP-sleutelpaar. Zoals dat hoort blijft de privé-sleutel in het bezit van de remailer, maar wordt de openbare sleutel verspreid over de leden van het CvB. Wordt er een nieuw lid toegevoegd aan het CvB, dan krijgt dat nieuwe lid ook de openbare sleutel (die immers openbaar is). Stapt iemand uit het CvB dan is dat ook geen ramp (voor de remailer).
   Dus: alle leden van de groep krijgen de publieke sleutel van cvbs@rug.nl.
3. Wanneer een lid van het CvB nu vertrouwelijke informatie aan de overige collegeleden wil doen toekomen, wordt deze informatie PGP versleuteld met de openbare sleutel van cvbs@rug.nl en gesigneerd met de privé-sleutel van de afzender: de overige leden van het CvB kunnen zo verifiëren dat de mail inderdaad afkomstig was van hun medecollegelid. Deze versleutelde en gesigneerde mail wordt vervolgens verstuurd naar cvbs@rug.nl, en komt dus terecht bij de re-encrypting remailer.
   Dus: vertrouwelijke informatie wordt versleuteld verstuurd naar cvbs@rug.nl en gesigneerd door de afzender.
4. De remailer controleert de validiteit van de elektronische handtekening. Faalt die controle dan is het spelletje afgelopen en wordt de ontvangen mail genegeerd. Laten we aannemen dat de verificatie lukt. Dan wordt de versleutelde mail ontcijferd met behulp van de privé-sleutel van de remailer en direct daarna weer versleuteld voor alle leden van het CvB. Dat is het re-encrypting gedeelte van de re-encrypting remailer. Het aardige is hierbij dat slechts op één plek hoeft te worden bijgehouden wie momenteel lid zijn van het CvB. De individuele collegeleden hoeven zelf geen mutaties meer in een eigen lijstje bij te houden. Na versleuteling wordt de mail gesigneerd door de remailer en (versleuteld voor de individuele collegeleden) doorgestuurd naar de leden van het CvB (dat is het remail-gedeelte van de re-encrypting remailer).
   Dus: via de remailer wordt de informatie, versleuteld voor de individuele leden van het CvB, doorgestuurd naar die leden.



Downloaden

Zoals gezegd, met het beschikbaar komen van nieuwe e-mailprogramma's zoals Mozilla Thunderbird is het gebruik van (PGP/GPG)-encryptie erg eenvoudig geworden. Wie gebruikmaakt van PGP/GPG-encryptie kan vervolgens gebruikmaken van een re-encrypting remailer om vertrouwelijke informatie over de leden van een groep te verspreiden.

Onlangs hebben mijn collega Hopko Meijering en ikzelf zo'n re-encrypting remailer-programma ontwikkeld. Wie geïnteresseerd is in de remailer: het programma (eigenlijk een Linux shell script) kan worden gedownload van **security.rc.rug.nl/remailer**.

Eventuele vragen over het gebruik ervan kunnen worden gericht aan: Frank B. Brokken, Security Manager: f.b.brokken@rc.rug.nl.