Risico’s van internetwerken

Wietse Z. Venema

Wiskunde en Informatica

Technische Universiteit Eindhoven

wietse@wzv.win.tue.nl

titel.fig

Overzicht presentatie

- Gevolgen van aansluiting op Internet.
  Van elektronisch dorp tot metropool.

- Boeven langs de digitale snelweg.
  Risico’s en tegenmaatregelen.

- Conclusies en aanbevelingen.

overzicht.fig

Een kwestie van gezond verstand

- Auto of fiets op slot of in berging.
- Geen snoepjes van vreemden aannemen.
- Handen wassen voor het eten.
- Uitkijken voor het oversteken.
- etcetera...

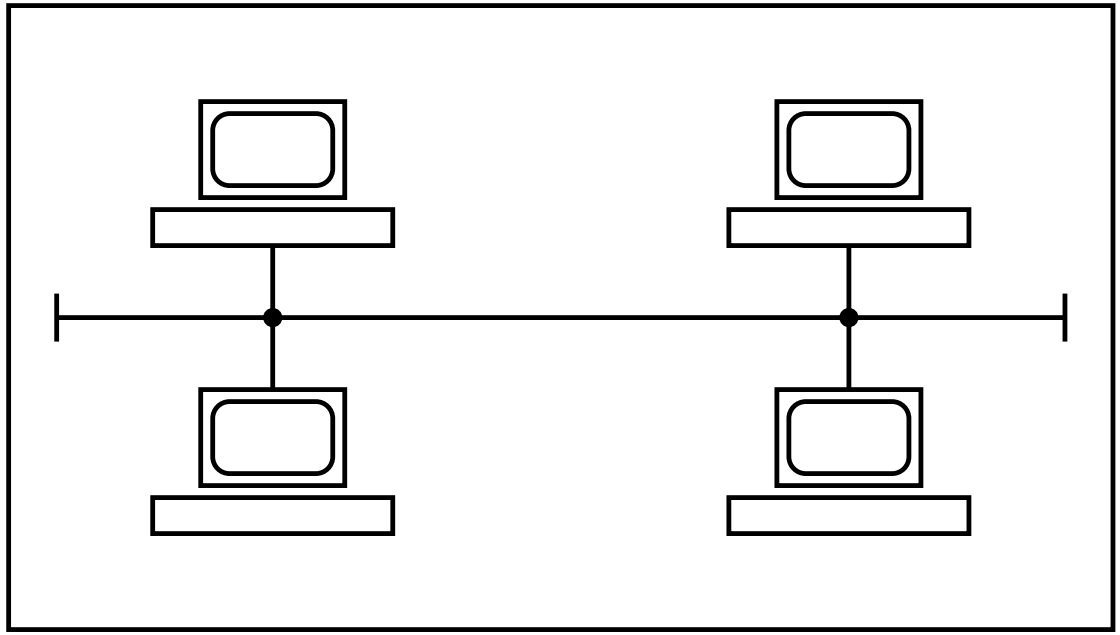
gezond-verstand.fig

Afbakening van het begrip ‘veiligheid’

- Gecontroleerde toegang tot systemen.
- Gecontroleerde toegang tot bestanden.
- Wat is voldoende veilig?

veiligheid.fig

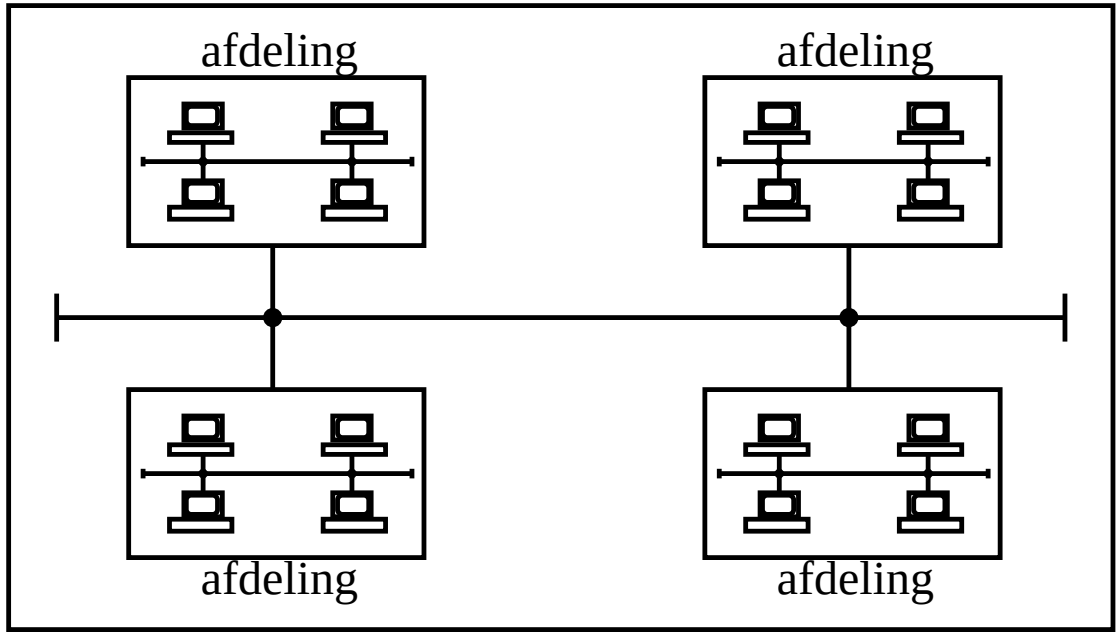
Een lokaal geisoleerd netwerk



- Afdeling met orde 10 - 100 systemen.
- Relatief beschermde omgeving.

lan-eiland.fig

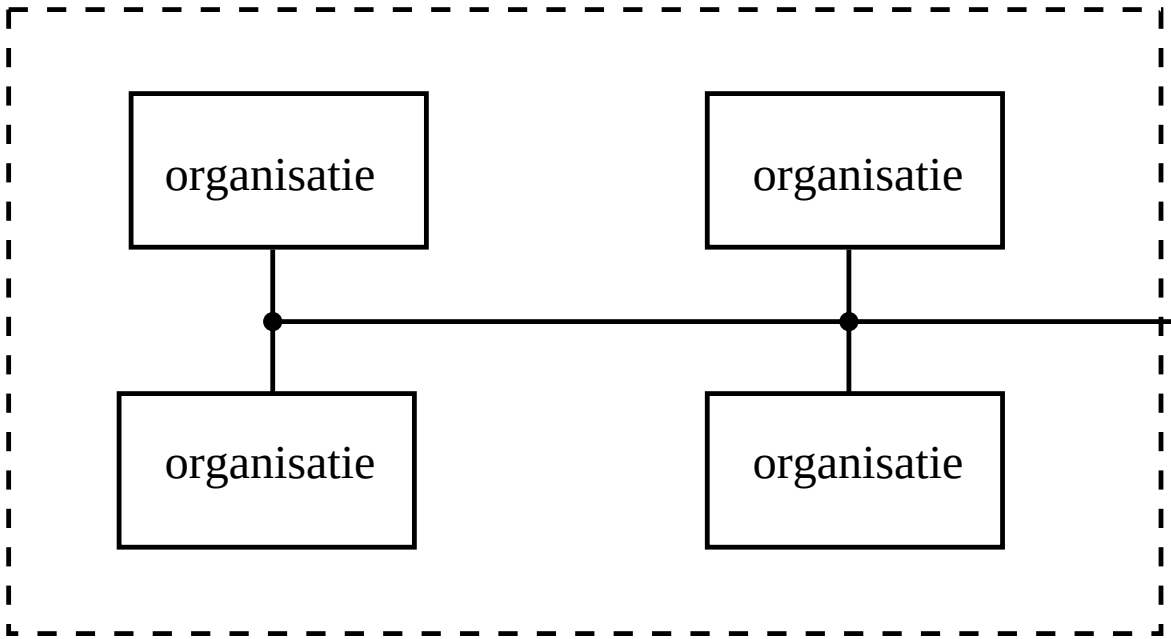
Koppeling binnen de organisatie



- Organisatie met 10^3 - 10^4 aansluitingen.
- Minder beschermd, heterogene gebruikersgroep.

lan-koppeling.fig

De elektronische metropool



- SURFnet met ordegrootte 10^5 aansluitingen.
- Relatief onbeschermde omgeving.

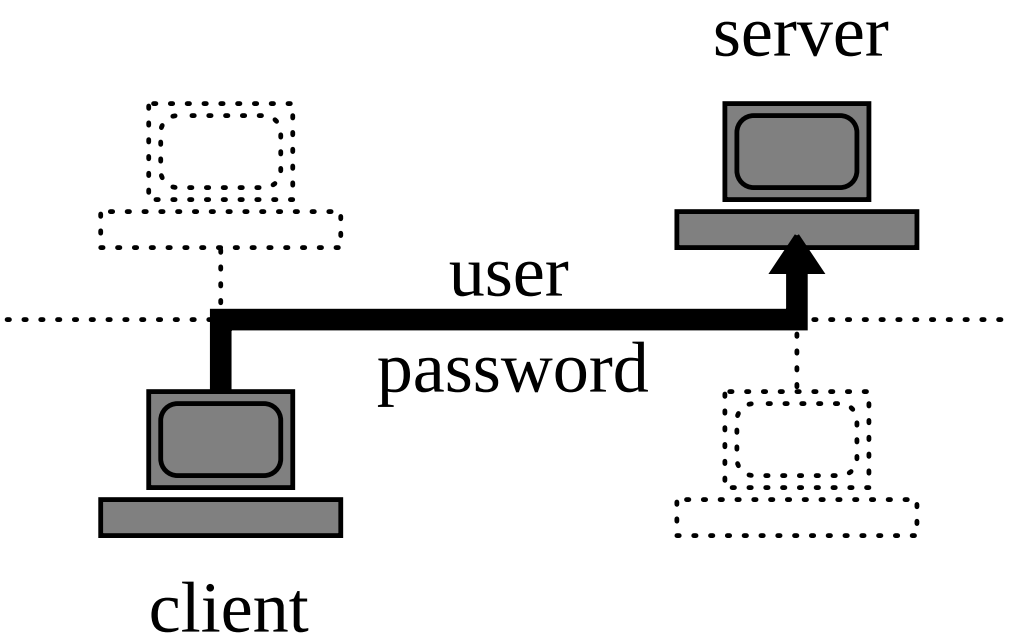
lan-extern.fig

Boeven op de digitale snelweg

- Bescherming tegen ongewenste toegang:
  - niet afluisterbare wachtwoorden
- Bescherming van gegevenstransport:
  - privacy, herkomst, integriteit
- Afbakening van grens van het lokale net:
  - firewalls.

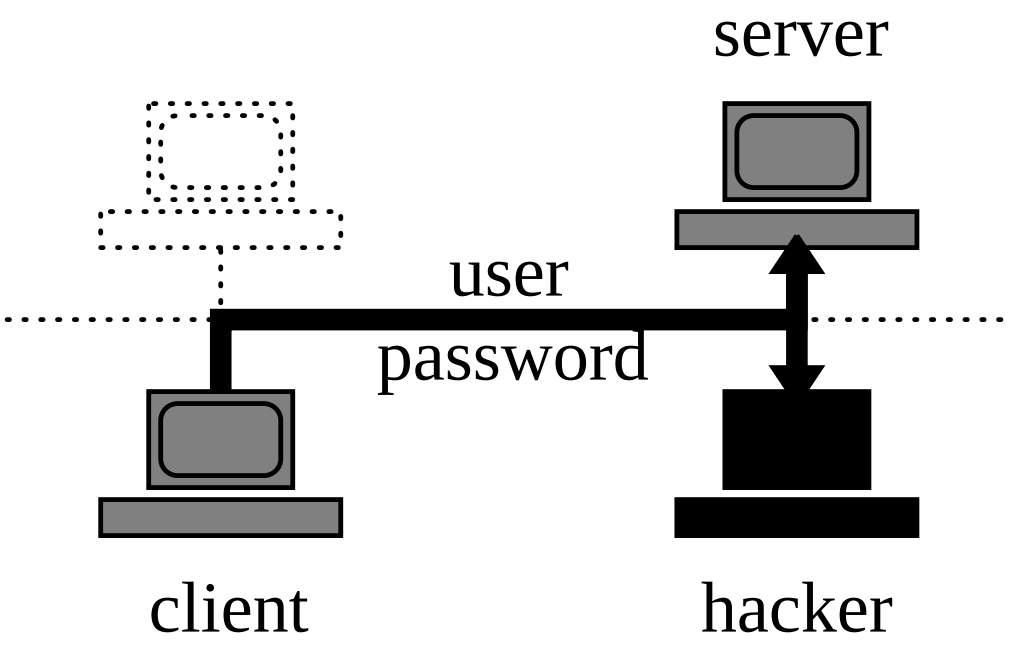
boeven.fig

Lokale netwerk login



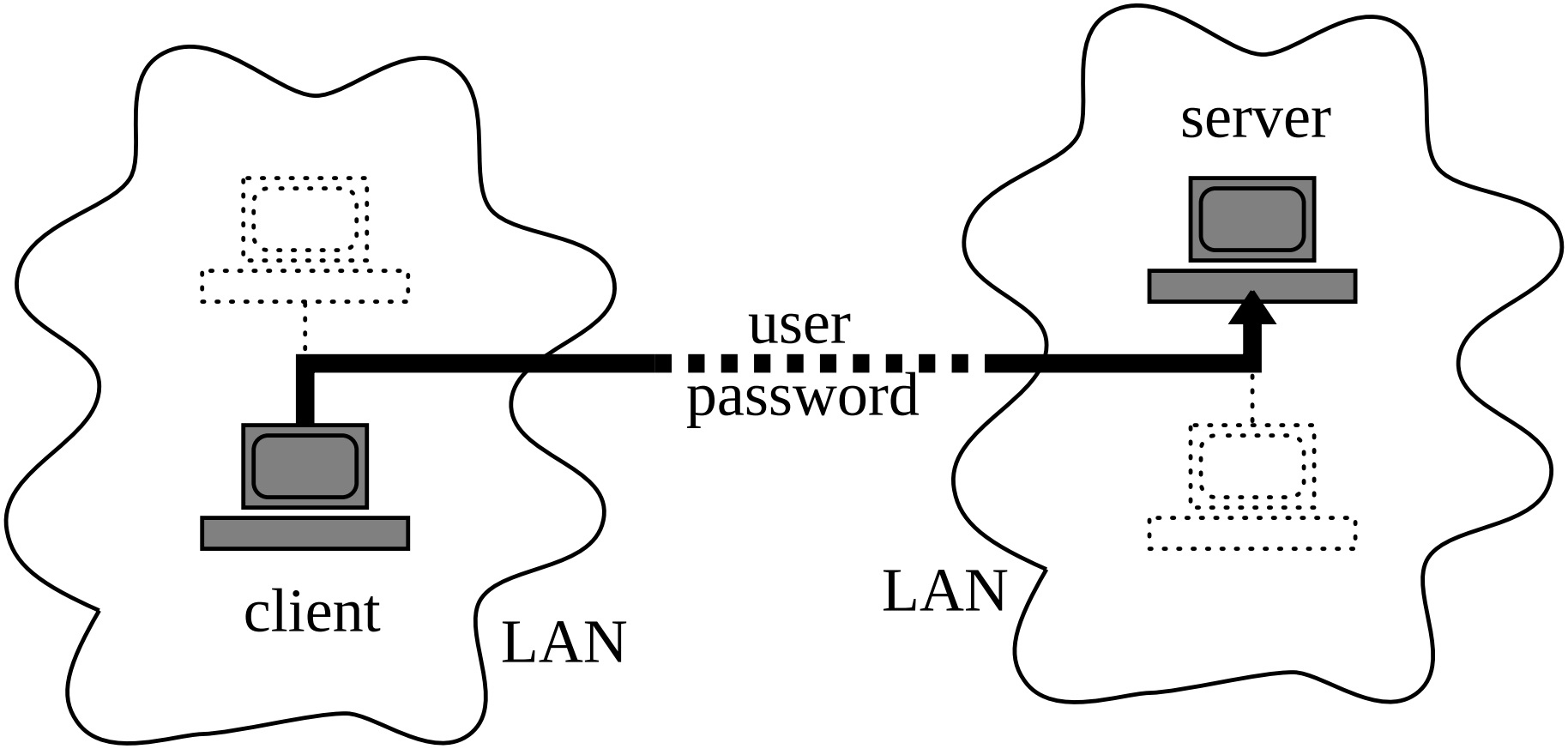
lokale-login.fig

Hacker op lokaal ethernet

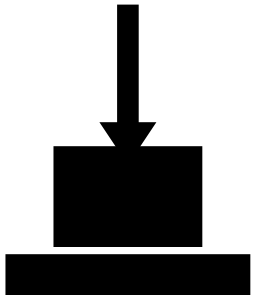


lokale-hacker.fig

Login via extern netwerk



externe-login.fig



hacker

hacker.fig

Februari 1994: persbericht CERT/CC

- Ongeveer 10.000 wachtwoorden afgeluisterd in de voorafgaande maanden.
- Inbraken via bekende lekken in de beveiliging. Bugfixes worden te vaak niet geinstalleerd.
- Subtiele aanpassingen systeemsoftware om sporen te verbergen.

cert-cc.fig

Eenmalige wachtwoord technologie

- Niet-programmeerbare smartcard (SecurID).
  Elke minuut een nieuw wachtwoord.

- Programmeerbare encryptie box (Digital Pathways).
  Elke keer een pseudorandom wachtwoord.

- Residente PC utility (S/Key).
  Herhaalde toepassing van eenwegs functie.

one-time.fig

Veilig informatietransport

- Bescherm het netwerk tegen ongewenste toegang.
- Bescherm de informatie door middel van versleuteling.
- Privacy: bescherming tegen onbevoegde inzage.
- Herkomst: bescherming tegen oplichterij.
- Integriteit: bescherming tegen onbevoegde wijziging.

secure-transport.fig

Encryptie en de politiek

- USA: encryptie valt onder de munitie wet.
- Frankrijk: encryptie is verboden.
- Nederland: vergunningen (wetsvoorstel).
- enzovoort.

Gevolg: encryptie nog lang geen standaardvoorziening.

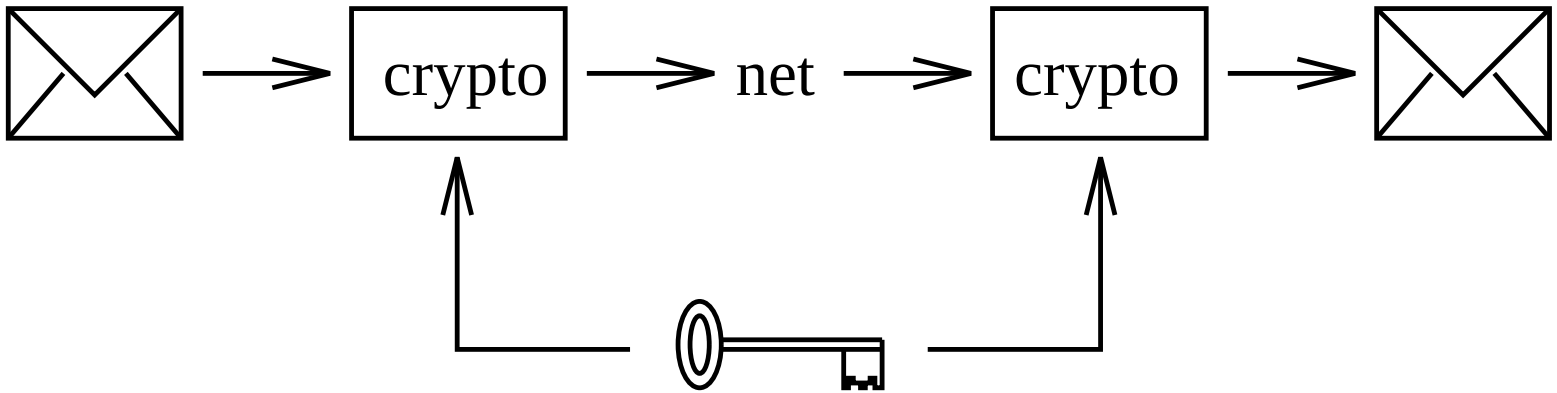
encryptie.fig

Encryptie op uiteenlopende niveaus

- Per systeem: alle informatie versleuteld het net op.
- Per netwerk: versleuteling bij verlaten lokaal netwerk. Voorbeeld: koppeling prive netwerken via internet.
- Per applicatie. Voorbeeld: secure electronic mail.

cypt-level.fig

Traditionele versleuteling

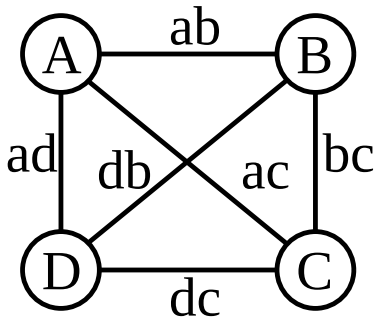


- Privacy: alleen sleutel bezitter kan bericht leesbaar maken.
- Herkomst: alleen sleutel bezitter kan bericht versleutelen.
- Integriteit: ontcijfering mislukt als bericht is verminkt.

trad-crypt1.fig

Tekortkomingen traditionele versleuteling

- Vooraf op een veilige manier sleutel afspreken.
- Een sleutel per paar partijen: N(N-1)/2.

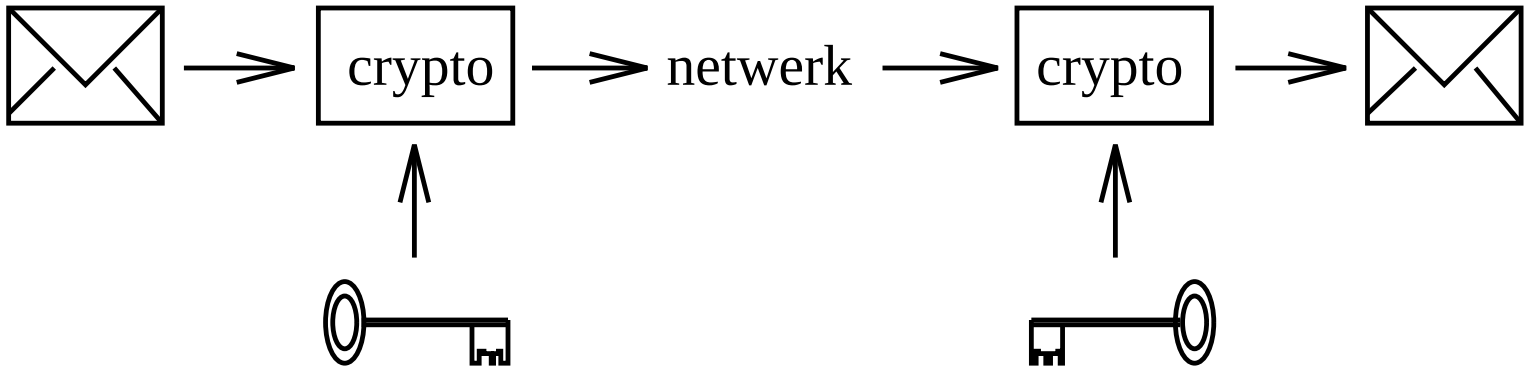


4 partijen, 6 sleutels

- Geen multicast mogelijkheid.

trad-crypt2.fig

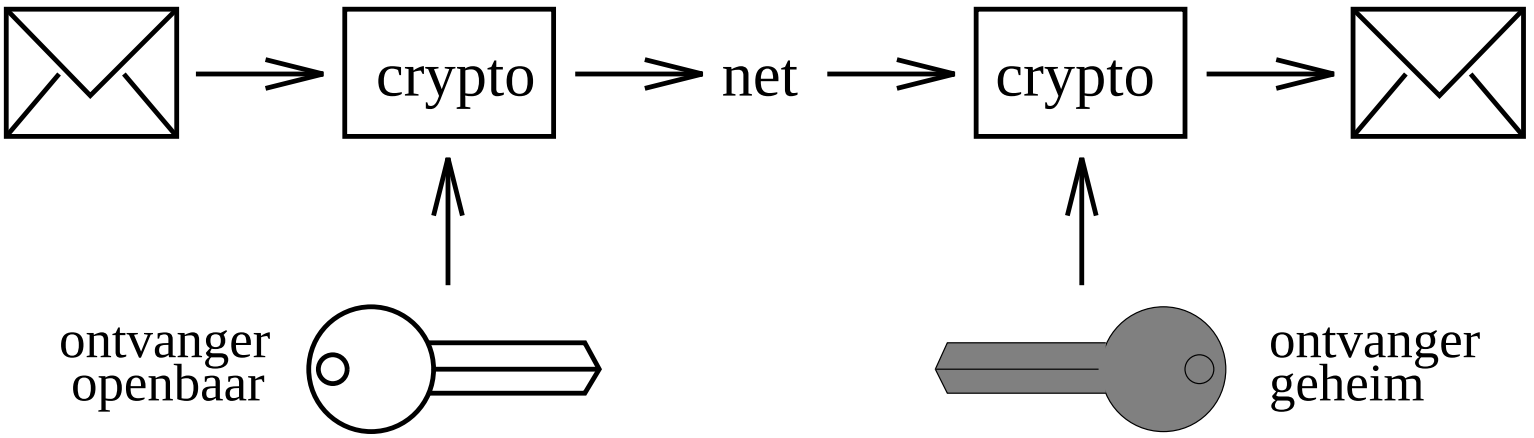
Encryptie met complementaire sleutels



- Complementaire sleutels: openbaar en geheim.
- Een openbare sleutel per gebruiker in plaats van een geheime sleutel per gebruikerspaar.
- Beveiliging op maat: privacy, herkomst of beide.

asym-crypt0.fig

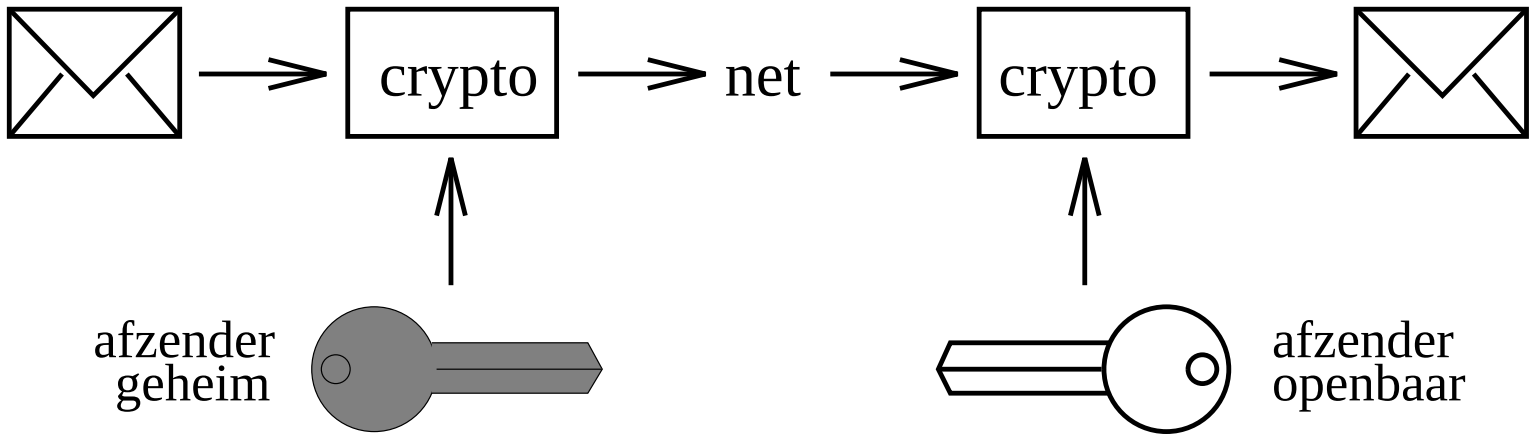
Bescherming op maat: privacy



- Alleen bezitter geheime sleutel kan bericht lezen.
- Iedereen kan dezelfde openbare sleutel gebruiken.
- Succesvolle ontcijfering is bewijs van integriteit.

asym-crypt1.fig

Bescherming op maat: herkomst



- Alleen bezitter geheime sleutel kan bericht aanmaken.
- Iedereen kan met publieke sleutel herkomst vaststellen.
- Succesvolle ontcijfering is bewijs van integriteit.

asym-crypt2.fig

Secure email standaarden

- Privacy Enhanced Mail: officiele internet standaard.
  Gebruik: pilot stadium.
  Handicap: sleutel distributie.

- Pretty Good Privacy: ‘de facto’ standaard.
  Gebruik: wijd en zijd, diverse platformen.
  Handicap: oude versie onderwerp juridische controverse.

Koppeling PEM-PGP nog onderwerp van studie.

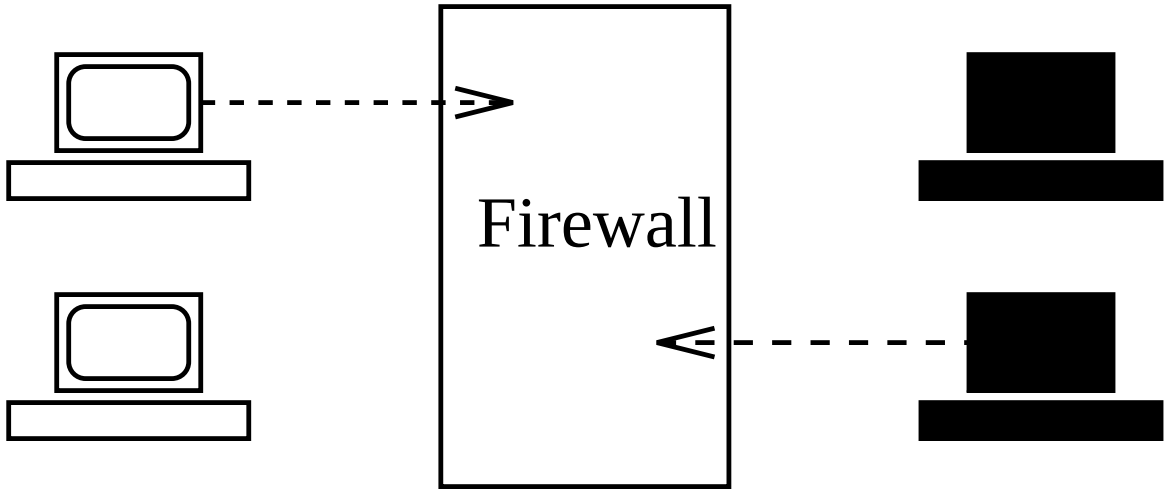
email-standards.fig

Firewall: het elektronische hek

<cartoon op voorzijde boek Cheswick/Bellovin>

firewall.fig

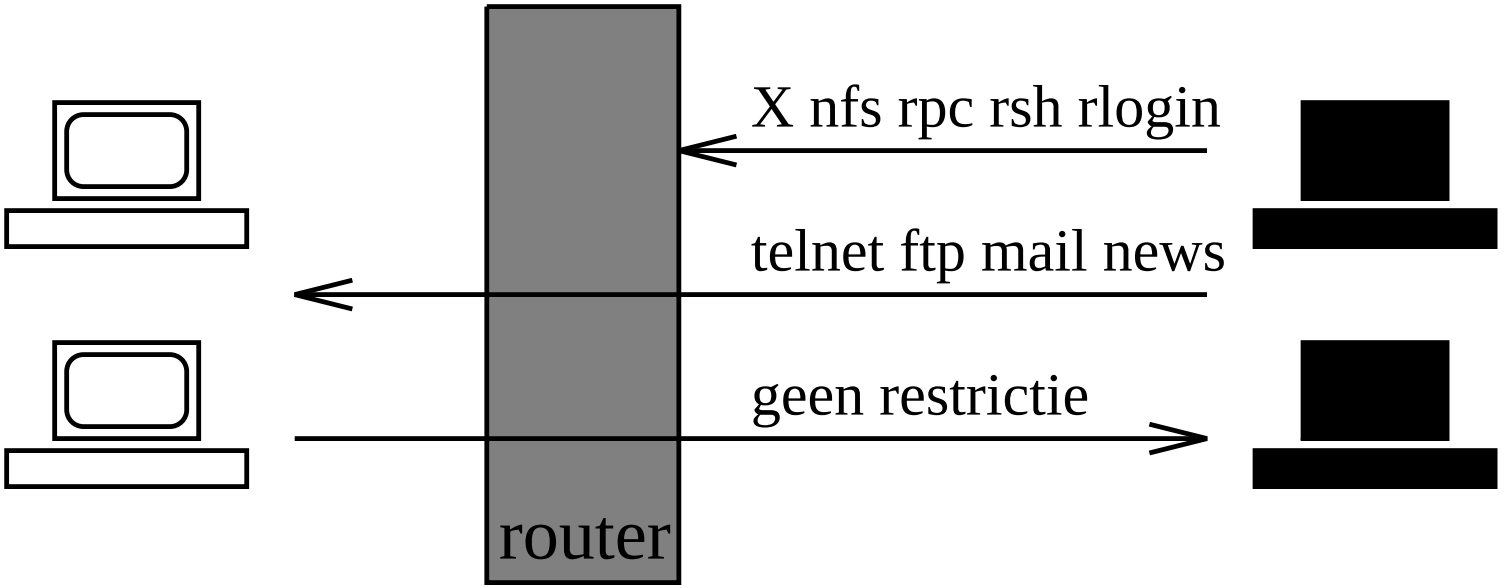
Firewall: de grens van het lokale netwerk



- Gecontroleerde toegang naar binnen.
- Gecontroleerde toegang naar buiten.
- Uitvoering hangt af van lokale policy.

firewall-pic.fig

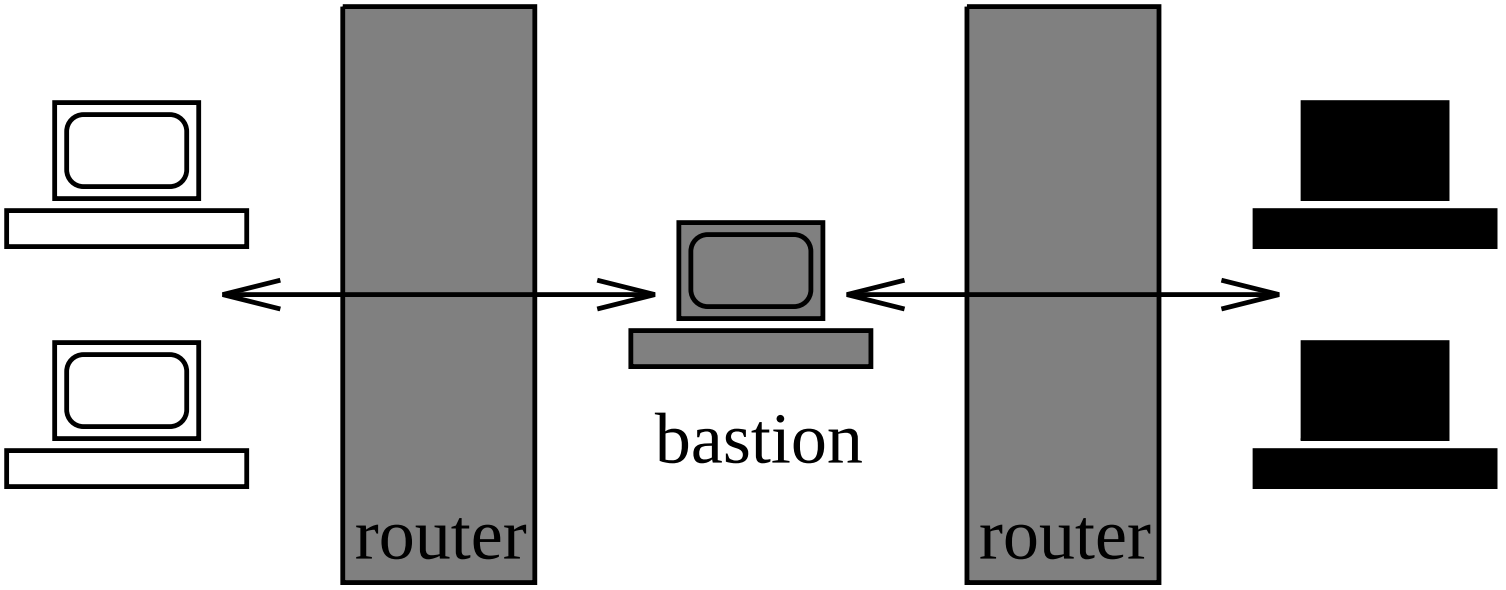
Policy 1: toegang vereist wachtwoord



- Blokkering van externe "trusted hosts".
- Onbeperkte toegang naar buiten.
- Filtering op netwerk niveau.

open-policy.fig

Policy 2: geen direct interlokaal verkeer



- Werking volgens principe van de luchtsluis.
- Maximale controle op interlokaal verkeer.
- Filtering op applicatie niveau.

closed-policy.fig

Conclusies en aanbevelingen

- Uitbreiding van een netwerk naar 3.000.000 aansluitingen vereist enige zorgvuldigheid.
- Stel een officiele (netwerk) security policy op. Dit voorkomt conflicten en/of ongelukken.
- Wed niet op een enkel paard: breng ook interne netwerk scheidingen aan (branddeur principe).

conclusie.fig

Referenties

Tekst en transparanten, inclusief literatuur verwijzingen, zijn beschikbaar via Internet.

- Anonymous ftp:
  wzv.win.tue.nl:/pub/security/surf-9411

- Moscaic en Netscape:
  ftp://wzv.win.tue.nl/pub/security/surf-9411

referenties.fig