Wie ben jij, en wat ga jij daar doen?

Bart Jacobs

bart@cs.kun.nl **http://www.cs.kun.nl/~bart**.

Nijmeegs Instituut voor Informatica & Informatiekunde

Overzicht

I. Inleiding Computer Beveiliging

Belang van computer beveiliging

- Sinds 11/9 is algemene aandacht voor beveiliging toegenomen
- Ook binnen informatica ***high profile*** onderwerp:
  - Mislukte chat van Willem-Alexander & Maxima
  - Pinpas fraude
  - Problemen met browsers & internet bankieren
- Overheid, bedrijven en burgers worden steeds meer afhankelijk van: veilige verbindingen, privacy, bescherming van informatie/copyright, digitale handtekening, identificatie, electronisch stemmen, etc.
- Nijmeegse nadruk op chipkaarten.

Waar gaat beveiliging eigenlijk over?

beveiliging = regulering van toegang

In the Engels:

Security is about regulating access to assets

Voorbeeld

Een **computervirus** vormt een beveiligingsprobleem als het ongeoorloofde toegang weet te krijgen tot informatie en programma's.

Hoe reguleer je toegang?

1. **Authentificatie**:
   Controleer wie je tegenover je hebt:
   "wie ben jij?"
2. **Authorisatie**:
   Controleer wat diegene mag:
   "wat ga jij daar doen?"

Dit vakgebied heeft een hoog ***Ausweis!*** gehalte, maar **…**

… gelukkig gaat meestal over computers onderling.

II. Chipknip (demo)

Chipknip schaduwboekhouding

Postbank voorwaarden Chipknip, artikel 2.8:

Een Chipknip die onbruikbaar is geworden geeft, na inlevering van de Kaart, alleen recht op terugbetaling aan de Chipkniphouder van het Chipknipsaldo. Indien de Bank de Kaart door een technisch defect daarvan niet kan onderzoeken, en de Chipkniphouder de Kaart binnen twaalf maanden na de laatste laad- of betaalhandeling heeft ingeleverd bij de Bank, zal de Bank na verloop van acht weken na inlevering het Chipknipsaldo berekenen ***aan de hand van de laad-betaalgegevens van de Chipknip***. Het aldus berekende Chipknipsaldo zal de Bank aan de Chipkniphouder ter beschikking stellen.

Chipknip aansprakelijkheid

Postbank voorwaarden Chipknip, artikel 8.2 d:

In geval van opzet, grove schuld of grove nalatigheid aan de zijde van de Chipkniphouder is de Chipkniphouder ***onbeperkt aansprakelijk***, een en ander onverminderd de verplichting van de Bank om (de mogelijkheid van) schade te beperken.

Chipknip lessen

Beveiliging (van computers) vraagt om de juiste mix van:

- **Technische** maatregelen:
  cryptografische protocollen, beveiligde hardware
- **Organisatorische** maatregelen:
  schaduwboekhouding, maximum bedrag op de kaart
- **Juridische** maatregelen:
  aansprakelijkheid van kaarthouder

Vergelijk: gewone / electronische handtekening, credit cards, bankpassen, . . .

Security is ***multi-disciplinair***.
Typisch in **Informatiekunde** opleiding.

III. Authentificatie van personen

Wie ben jij?

Identiteit van personen wordt vastgesteld op basis van:

- ***Iets wat je hebt***
  Voorbeeld gewone sleutel, airmilespas
  Risico (on)vrijwillige overdracht, copieëren
- ***Iets wat je weet***
  Voorbeeld paswoord, PIN
  Risico afkijken, raden, beheer
- ***Iets wat je bent***
  Voorbeeld vingerafdruk, irisscan, DNA
  Risico false positives/negatives, privacy

Minstens twee hiervan nodig!

IV. Authentificatie van computers

Cryptografie

- Cryptografie is de wiskunde van het onleesbaar en weer leesbaar maken van boodschappen.
- Voorbeeld: **...**
- Standaard manier: twee partijen hebben gemeenschappelijke "cryptografische" sleutel K, en kunnen daarmee
  - ***coderen***: boodschap m wordt $\{m\}_K$
  - ***decoderen***: $n = \{m\}_K$ wordt m
- Geeft confidentialiteit & integriteit
- Ook mogelijk ***public key crypto***: ieder partij heeft publieke en privé sleutel.

Crypto authentificatie

- Stel A en B zijn computers met gemeenschappelijke sleutel K
- A wil iets van B, maar B wil eerste zeker weten dat het verzoek van A komt
- ***Idee:*** B geeft eerst een "raadsel", dat alleen met K op te lossen is — en dus alleen door A.
- ***Protocol / Scenario:***

$A \longrightarrow B$: "hi, I'm A; please do ..."
$B \longrightarrow A$: $\{R\}_K$
(R is groot random getal)
$A \longrightarrow B$: R

B vertrouwt het nu, en doet ...

V. Voorbeelden

Chipknip betaling (versimpeld)

- Het hele systeem heeft een ***Master Key*** M.
  M zit in alle betaalterminals, maar niet in kaarten.
- Iedere chipknip C heeft "gediversificeerde" sleutel, bijv.

  $$K_C = \{\text{Kaartnr. van } C\}_M$$

  Iedere terminal T kan K_C dus berekenen.
- ***Betaal protocol fragment:***

  $C \longrightarrow T$: "hoi, ik ben een chipknip met kaartnr. p"
  $T \longrightarrow C$: $\{R\}_{K_C}$
  $C \longrightarrow T$: R
  $T \longrightarrow C$: "schrijf af: *bedrag*", $\{\textit{bedrag}\}_{K_C}$

Identiteit & Integriteit zijn beveiligd

Voorbeeld: 4 protocollen voor electronische autosleutel

Lees **A** = Auto, **S** = Auto Sleutel in:

(1) Identificatie nummer	**(2) Versleutelde versie van (1)**
S $\longrightarrow$ A : IdNr	S $\longrightarrow$ A : $\{\text{IdNr}\}_K$ (K is gedeelde crypto sleutel)
(3) Sequence nummer	**(4) Challenge-response**
S $\longrightarrow$ A : $\{N+1\}_K$ (N is laatst gebruikte nummer)	S $\longrightarrow$ A : "open" A $\longrightarrow$ S : $\{N\}_K$ S $\longrightarrow$ A : $\{N+1\}_K$

Conclusies

Computer security is:

- Leuk en spannend,
- breed (van wiskunde tot rechten)
- hoogst actueel
- Sterk vertegenwoordigd in Nijmegen!

Slides beschikbaar op:
`www.cs.kun.nl/~bart/TALKS/`