Perspektiver om trust

Mark Burgess,
Høgskolen i Oslo

Hva vet du om naboen?

Sikkerhet dreier seg om “trust management”

Ingen entydig definisjon

- **Trust** (engelsk) = ?
  - Tillit, ha tillit til, tillitsforhold
  - Tiltro
  - Kreditt, forvaring, varetekt.
  - Mål på plikt oppfyllelse
  - Å stole på
  - Pålitelighet (Forutsigbarhet, forståelighet)

Hvorfor er vi så opptatt av trust?

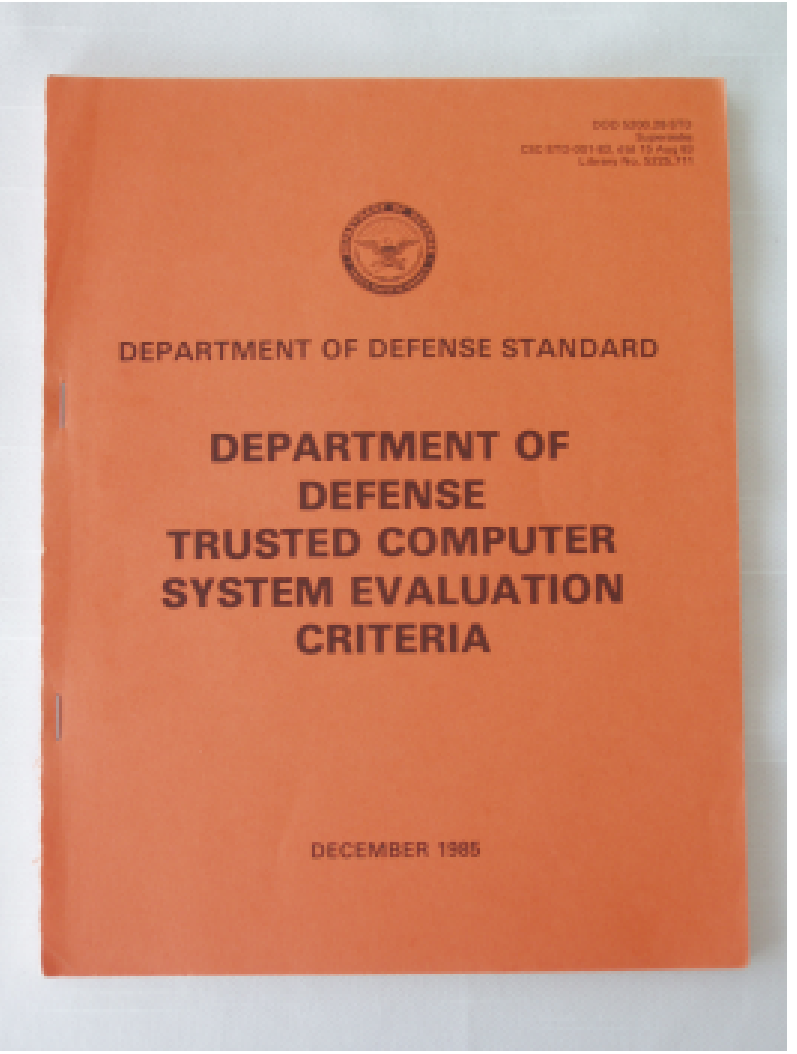
- Mennesker har et nesten utrolig behov for å underordne seg en tillitsfigur, autoritet – for trygghet?
- Basis for individuell handel (utveksling)
- Basis for samfunn (delegering)

Trust “Models”

- Det er mange “protokoller” som påstar å implementere “trust”
  - Webs of trust
  - Trusted 3rd parties (TLS,Kerberos etc)
- De er unyanserte
  - Trust er normalt boolsk (1/0, -1/+1)
  - Ikke knyttet til noen emne
- Generalisert modell (Bergstra & Burgess)
  - Forene de ulike syn med en “naturlig” definisjon

Modeller om trust

- Bell Lapadula
- Clark-Wilson etc.
- TSEC --->
- Secure Linux etc etc
- Trusted Computing Initiative (HP,Dell,IBM)
- Promise theory



Promise Theory – en nyttig modell

- Frivillig samarbeid – ellers trust = naturkrefter
- Holder agenter løfter? => tillitsverdig, til å stole på
- En agents forventning måler dens "trust"
- Grafisk, logisk, økonomisk og statistisk teori

Definition 1 (Promise) *A promise is an autonomous specification of future behaviour. It involves two agents, a promiser and a promisee, and is announced only to the promisee. Each promise contains a promise body b that describes the content of the promise. A typical promise from an agent a to an agent c, with body b is written:*

$$a \xrightarrow{\pi:b} c \tag{1}$$

Må kunne *spesifiere* trust

Proposal 1 (Trust) *Trust can be defined as an* agent's expectation *that a promise will be kept. It is thus a probability lying between 0 and 1.*

Vi bruker begreper løst og slapt, selv i datasikkeret,
f.eks. "I trust a public key" - hva betyr det?

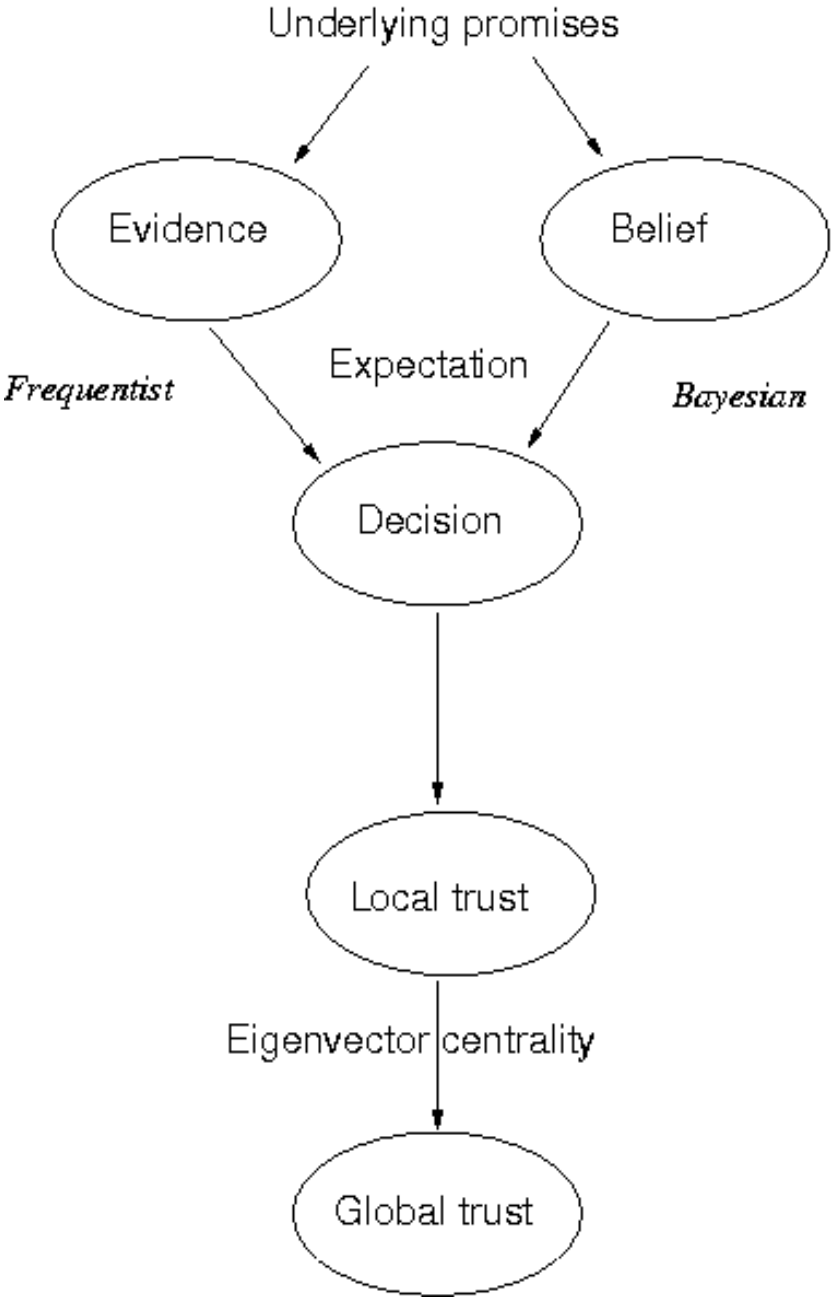
$$\mathrm{Me} \overset{\tau:\mathrm{Authentic}}{\longrightarrow} \mathrm{Signature} \overset{P}{\equiv} E_{\mathrm{Me}}(\mathrm{Signature} \overset{\pi:\mathrm{Authentic}}{\longrightarrow} \mathrm{Me})$$

$$\mathrm{Me}[\mathrm{Signature}] \overset{\tau:\mathrm{Authentic}}{\longrightarrow} \mathrm{Certifier}[\mathrm{Me}] \overset{P}{\equiv} E_{\mathrm{Me}}(\mathrm{Certifier}[\mathrm{Signature}] \overset{\pi:\mathrm{Authentic}}{\longrightarrow} \mathrm{Me})$$

$$\mathrm{Me} \overset{\tau:\mathrm{verify\ key}}{\longrightarrow} \mathrm{Certifier} \overset{P}{\equiv} E_{\mathrm{Me}}\left(\mathrm{Certifier} \overset{\pi:\mathrm{verify\ key}}{\longrightarrow} \mathrm{Me}\right)$$

Trust er bare policy

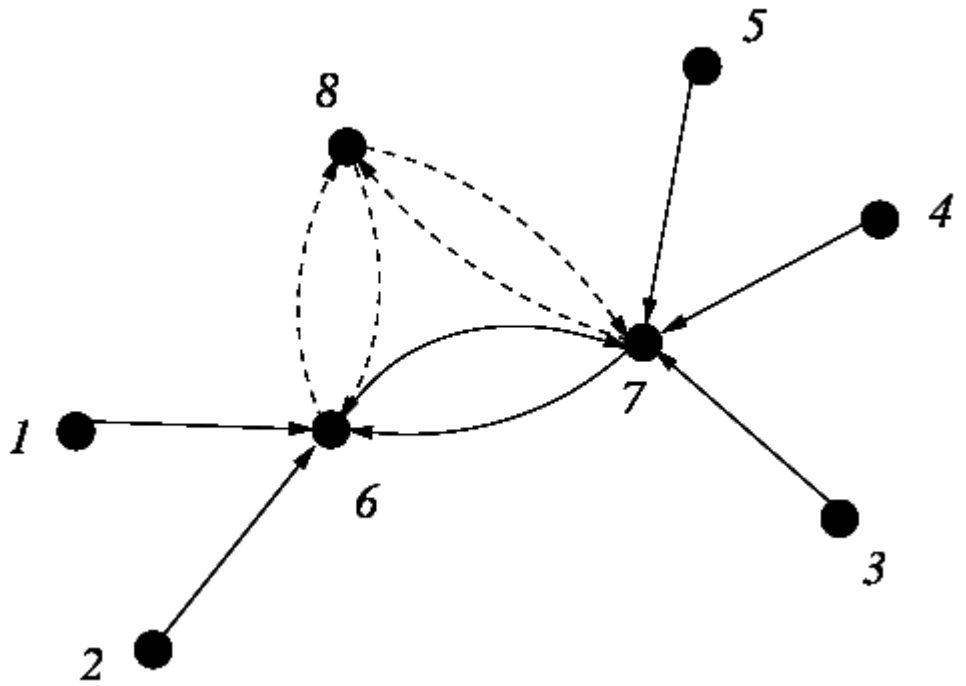
- Problemet er hvordan definerer vi forventning?
  - Basert på hvilken empiri?
  - Rent subjektivt
- Gitt at vi går inn for det får vi naturlig def.
  - Trust (lokalt/globalt)
  - Reputation (rykte)



Community Trust (Webs of etc...)

Self-consistent trust som en egenvektor av matrisen:

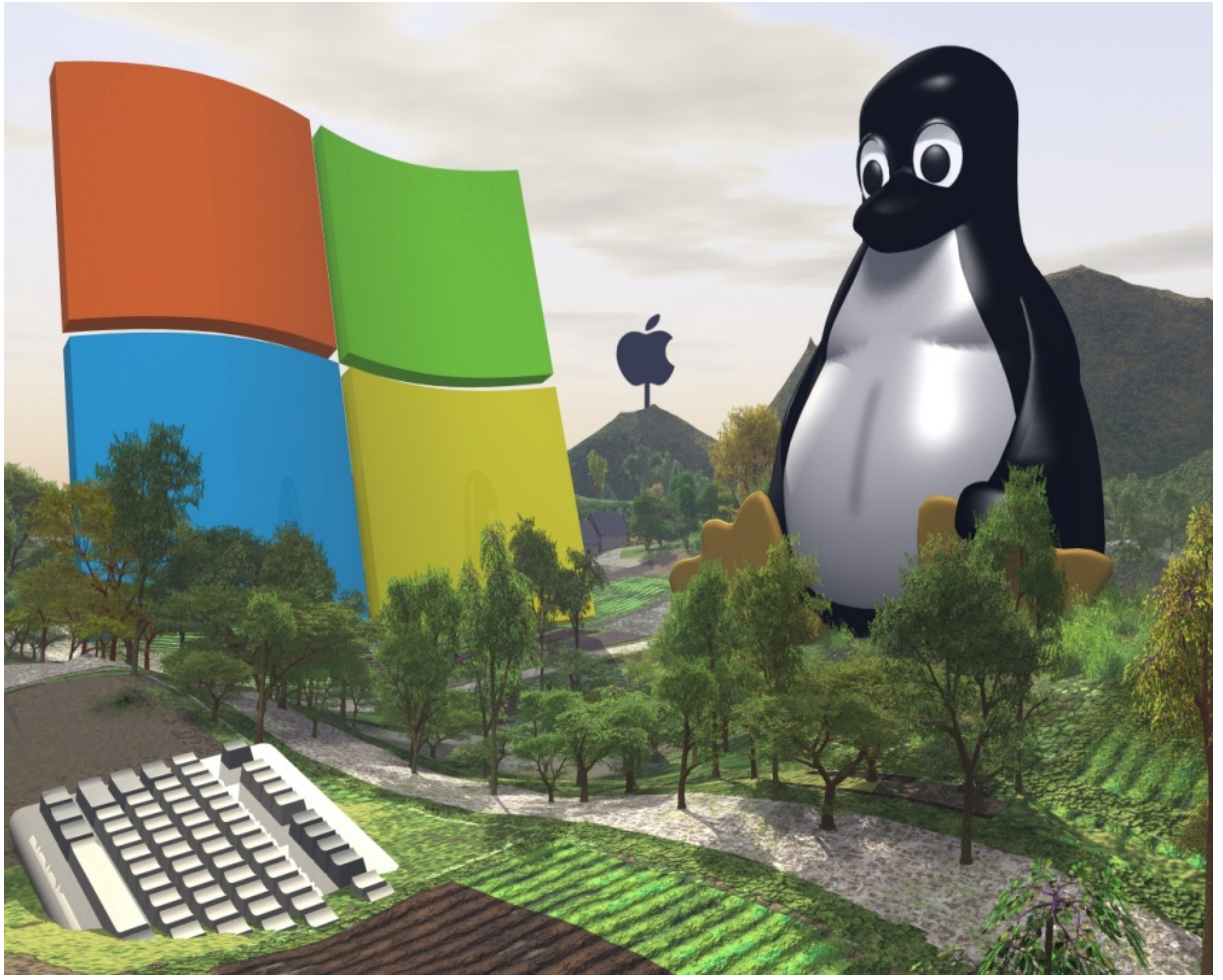
$$T_{AB}(b) \equiv E_A(B \xrightarrow{\pi:b} *)$$



$$\vec{S}_8 = \begin{pmatrix} 0.21 \\ 0.31 \\ 0.10 \\ 0.10 \\ 0.10 \\ 1.00 \\ 0.94 \\ 0.50 \end{pmatrix}, \quad \vec{W}_8 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.55 \\ 0.65 \\ 1.00 \end{pmatrix}$$

Trust Wars!

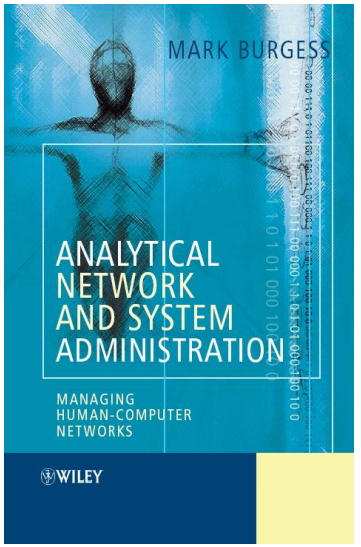
- Hvilken kampanje resonnerer best med folket?
- Begrepet er sannsynligvis tomt i vitenskapelig forstand.
- Trust er en ren policy avgjørelse



Sikkert/trusted system?

"Et sikkert system er et system hvor risikoen av hver eneste mulig hendelse er evaluert og godtatt som en del av systempolitikken."

POLICY



“Jeg stoler ikke på ham. Vi er venner.”

--Berthold Brecht

Questions?