Security and Trust I: 6. Trust

Dusko Pavlovic

UHM ICS 355
Fall 2014

Outline

Outline

Trust on the Web

Trust on the Web: Adverse selection

	TRUSTE-certified	uncertified
honest	94.6%	97.5%
malicious	5.4%	2.5 %

Table: Trustworthyness of TRUSTE [Edelman 2007]

Trust on the Web: Adverse selection

Google		
	sponsored	organic
top	4.44%	2.73%
top 3	5.33%	2.93 %
top 10	5.89%	2.74 %
top 50	5.93%	3.04 %

Table: Malicious search engine placements [Edelman 2007]

Trust on the Web: Adverse selection

Yahoo!		
	sponsored	organic
top	6.35%	0.00%
top 3	5.72%	0.35 %
top 10	5.14%	1.47 %
top 50	5.40%	1.55 %

Table: Malicious search engine placements [Edelman 2007]

Trust on the Web: Adverse selection

Ask		
	sponsored	organic
top	7.99%	3.23%
top 3	7.99%	3.24 %
top 10	8.31%	2.94 %
top 50	8.20%	3.12 %

Table: Malicious search engine placements [Edelman 2007]

Problem of trust

"Pillars of the society" phenomenon

- social hubs are more often corrupt
- the rich are more often thieves
- …

Problem of trust

- Why does adverse selection happen?
- Can it be eliminated? Limited?
- Can we hedge against it?
- Is there a rational trust policy?

Paradox of trust

- Trust is not transferrable.
- Trust services must transfer trust.

Paradox of trust

- "I should only trust those that I know."
- "I often need to trust those that I don't know."

Outline

What is trust?

Alice trusts that Bob will act according to protocol Φ.

What is trust?

Alice trusts that Bob will act according to protocol Φ.

Examples

- shopping: Bob will deliver goods
- marketing: Bob will pay for goods
- access control: Bob will not abuse resources
- key infrastructure: Bob's keys are not compromised

What is trust?

Trust vs honesty

- Alice is an *honest* participant for the role A of protocol Φ is she acts according to this role in this protocol.
- Bob *trusts* Alice for the role A in the protocol Φ if he believes that she is honest.

What is trust?

Trust vs honesty

- Alice is an *honest* participant for the role A of protocol Φ is she acts according to this role in this protocol.
- Bob *trusts* Alice for the role A in the protocol Φ if he believes that she is honest.

Trust is Bob's *internal belief* in Alice's honesty.

What is trust?

Trust vs reputation

- Alice's *reputation* is the total (or average) trust that she has accumulated within a network.
- Bob's *trust* for Alice is a part of her overall reputation.

What is trust?

Trust vs reputation

- Alice's *reputation* is the total (or average) trust that she has accumulated within a network.
- Bob's *trust* for Alice is a part of her overall reputation.

Feedback services (e.g. on Amazon or eBay)

- specify seller's reputation as the percentage of satisfied customers
- display seller's trust ratings within in the individual customer's reviews

Modeling trust

Trust relation $A \xrightarrow[r]{\Phi} B$

- A: trustor
- B: trustee
- Φ: entrusted concept (protocol, task, property)
- r: trust rating

Views of Trust

Local: trust logics

$A \stackrel{\Phi}{\longrightarrow} B$ means that

- A requires Φ
- B guarantees Φ

Views of Trust

Global: trust networks

$A \xrightarrow[r]{d} B \xrightarrow[s]{d} C \xrightarrow[t]{d} D \xrightarrow[u]{b} K$ means that

- A has a delegation certificate for B
- B has a delegation certificate for C
- C has a delegation certificate for D
- D has a binding certificate for the key K

Views of Trust

Global: trust networks

$A \xrightarrow[r]{d} B \xrightarrow[s]{d} C \xrightarrow[t]{d} D \xrightarrow[u]{b} K$ means that

- A has a delegation certificate for B
- B has a delegation certificate for C
- C has a delegation certificate for D
- D has a binding certificate for the key K
- thus A can use the key K
  - even compute its trust rating *rstu*
- although they had no direct contact

Network dynamics

Networks are built upon networks:

- session keys upon long term keys
- strong secrets upon weak secrets
- crypto channels upon physical or social channels

Network dynamics

Networks are built upon networks:

- session keys upon long term keys
- strong secrets upon weak secrets
- crypto channels upon physical or social channels
- secure interactions upon trust
- trust upon secure interactions

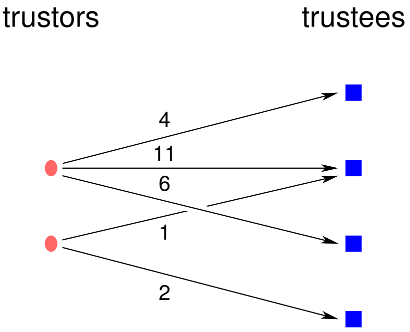
Outline

Trust dynamics

For a moment, we assume that the entrusted property Φ is fixed, and analyze dynamics of trust rating

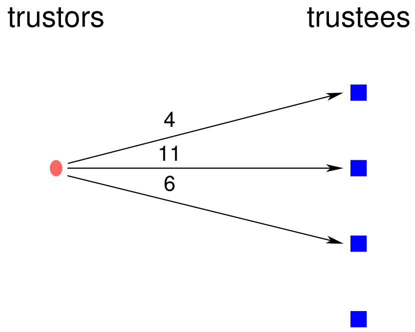
$$A \underset{r}{\longrightarrow} K$$

Trust rating matrix



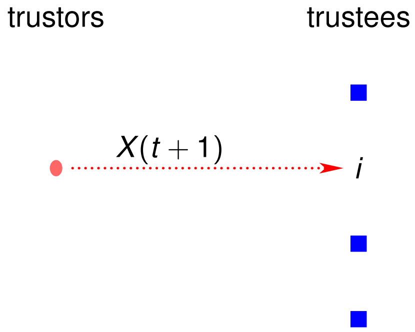
τ^1	4	11	6	0
τ^2	0	1	0	2

Private trust dynamics



$\tau(t)$	4	11	6	0

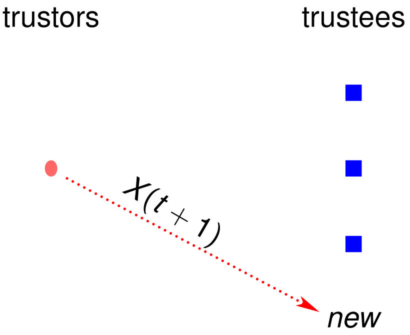
Private trust dynamics



$$\mathrm{Prob}\Big(X(t+1) = i\Big) = C(t)\tau_i(t)$$

(where $C(t) = \frac{1-\alpha}{\sum_{i\in J}\tau_i(t)}$)

Private trust dynamics



$$\mathrm{Prob}\Big(X(t+1) = \mathit{new}\Big) \quad = \quad \alpha$$

Private trust dynamics

Trust updating process

$$\tau_i(t+1) \quad = \quad \begin{cases} \tau_i(t) & \text{if } i \neq X(t+1) \\ 0 & \text{if } i = X\text{, not satisfactory} \\ 1 & \text{if } i = X\text{, satisfactory, new} \\ 1 + \tau_i(t) & \text{if } i = X\text{, satisfactory, not new} \end{cases}$$

Trust distribution

Task

Estimate

$$w_\ell(t) \quad = \quad \#\{i \in \mathsf{J} \mid \tau_i(t) = \ell\}$$

Trust distribution

$$
\begin{aligned}
w_1(t+1) - w_1(t) &= J \cdot \mathrm{Prob}\big(X(t+1) = i \mid i \text{ new}\big) \cdot \gamma_\perp \\
&\quad - w_1(t) \cdot \mathrm{Prob}\big(X(t+1) = i \mid \tau_i(t) = 1\big) \\
&= J\alpha\gamma_\perp - w_1(t)C(t)
\end{aligned}
$$

Trust distribution

$$
\begin{aligned}
w_\ell(t+1) - w_\ell(t) &= w_{\ell-1}(t) \cdot \mathrm{Prob}\Big(X(t+1) = i \mid \tau_i(t) = \ell - 1\Big) \cdot \gamma_{\ell-1} \\
&\quad - w_\ell(t) \cdot \mathrm{Prob}\Big(X(t+1) = i \mid \tau_i(t) = \ell\Big) \\
&= w_{\ell-1}(t) C(t) (\ell - 1) \gamma_{\ell-1} - w_\ell(t) C(t) \ell
\end{aligned}
$$

Trust distribution

The system

$$
\begin{aligned}
\Delta_t w_1(t) &= J\alpha\gamma_\perp - C(t)w_1(t) \\
\Delta_t w_\ell(t) &= w_{\ell-1}(t)C(t)(\ell-1)\gamma_{\ell-1} - w_\ell(t)C(t)\ell
\end{aligned}
$$

Trust distribution

. . . divided by J becomes

$$\begin{aligned}\Delta_t v_1(t) &= \alpha\gamma_\perp - C(t)v_1(t)\\ \Delta_t v_\ell(t) &= v_{\ell-1}(t)C(t)(\ell-1)\gamma_{\ell-1} - v_\ell(t)C(t)\ell\end{aligned}$$

where $v_\ell(t) = \frac{w_\ell(t)}{J} = \mathrm{Prob}(i \in \mathrm{J} \mid \tau_i(t) = \ell)$
form a stochastic process $v : \mathbb{N} \to \mathcal{D}\mathrm{R}$

Trust distribution

. . . and since $v : \mathbb{N} \to \mathcal{D}\mathrm{R}$ is a martingale,
it extends to $v : \mathbb{R} \to \mathcal{D}\mathrm{R}$ and the system becomes

$$\begin{aligned}\frac{dv_1}{dt} &= \alpha\gamma_\perp - \frac{c}{t} v_1\\ \frac{dv_\ell}{dt} &= \frac{\gamma_{\ell-1} c(\ell-1) v_{\ell-1} - c\ell v_\ell}{t}\end{aligned}$$

where $C(t) \approx \frac{c}{t}$, for $c = \frac{1-\alpha}{1+\alpha\gamma_\perp}$ (see Appendix)

Trust distribution

The steady state of $v : \mathbb{R} \to \mathcal{D}\mathrm{R}$ will be in the form $v_\ell(t) = t \cdot \upsilon_\ell$, where

$$
\begin{aligned}
\upsilon_1 &= \alpha\gamma_\perp - c\upsilon_1 \\
\upsilon_\ell &= \gamma_{\ell-1} c(\ell - 1)\upsilon_{\ell-1} - c\ell\upsilon_\ell
\end{aligned}
$$

Trust distribution

The steady state of $v : \mathbb{R} \to \mathcal{D}R$ will be in the form $v_\ell(t) = t \cdot \upsilon_\ell$, where

$$\upsilon_1 = \frac{\alpha\gamma_\perp}{c+1}$$

$$\upsilon_\ell = \frac{(\ell-1)\gamma_{\ell-1} c}{\ell c + 1} \upsilon_{\ell-1}$$

Trust distribution

...which expands into

$$\begin{aligned}
\upsilon_2 &= \frac{\alpha\gamma_\perp}{c+1}\cdot\frac{\gamma_1 c}{2c+1}\\
\upsilon_3 &= \frac{\alpha\gamma_\perp}{c+1}\cdot\frac{\gamma_1 c}{2c+1}\cdot\frac{2\gamma_2 c}{3c+1}\\
&\vdots\\
\upsilon_n &= \alpha\gamma_\perp\left(\prod_{\ell=1}^{n-1}\gamma_\ell\right)c^{n-1}\cdot\frac{(n-1)!}{\prod_{k=1}^{n}(kc+1)}\\
&= \frac{\alpha\gamma_\perp G_{n-1}}{c}\cdot\frac{(n-1)!}{\prod_{k=1}^{n}\left(k+\frac{1}{c}\right)}\\
&= \frac{\alpha\gamma_\perp G_{n-1}}{c}\cdot\frac{\Gamma(n)\Gamma\left(1+\frac{1}{c}\right)}{\Gamma\left(n+1+\frac{1}{c}\right)}\\
&= \frac{\alpha\gamma_\perp G_{n-1}}{c}\cdot B\left(n,1+\frac{1}{c}\right)
\end{aligned}$$

Trust distribution

The solution

$$\begin{aligned} \upsilon_1 &= \frac{\alpha\gamma_\perp}{c+1} \\ \upsilon_n &= \frac{\alpha\gamma_\perp G_{n-1}}{c} \; B\left(n, 1+\frac{1}{c}\right) \\ &\stackrel{n\to\infty}{\longrightarrow} \frac{\alpha\gamma_\perp G}{c} \; n^{-\left(1+\frac{1}{c}\right)} \end{aligned}$$

where

$$G = \prod_{\ell=1}^{\infty} \gamma_\ell > 0 \text{ follows from}$$

$$\frac{1}{e^{s_\ell}} \leq \gamma_\ell \leq 1 \text{ for some}$$

$$\sum_{\ell=1}^{\infty} s_\ell < \infty$$

Trust distribution

Theorem

The described process of trust building leads, in the long run, to the power law distribution of the number of trusteess with the trust rating n

$$w_n \approx \frac{\alpha\gamma_\perp GJ}{c} n^{-\left(1+\frac{1}{c}\right)}$$

Trust distribution

Theorem

The described process of trust building leads, in the long run, to the power law distribution of the number of trusteess with the trust rating n

$$w_n \approx \frac{\alpha\gamma_\perp GJ}{c} n^{-\left(1+\frac{1}{c}\right)}$$

provided that the incidence of dishonest principals who act honestly long enough to accumulate a high trust rating — is low enough

Trust distribution

Theorem

The described process of trust building leads, in the long run, to the power law distribution of the number of trusteess with the trust rating n

$$w_n \quad \approx \quad \frac{\alpha\gamma_\perp GJ}{c} \; n^{-\left(1+\frac{1}{c}\right)}$$

provided that the incidence of dishonest principals who act honestly long enough to accumulate a high trust rating — is low enough (so that $\gamma_\ell \xrightarrow{\ell\to\infty} 1$ fast enough)

What does this mean?

Some things have a fixed scale

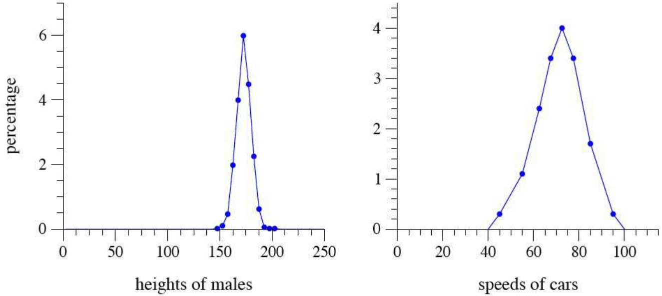


Figure: Normal distribution $f(x) = ae^{-bx^2}$

What does this mean?

Many social phenomena are scale-free

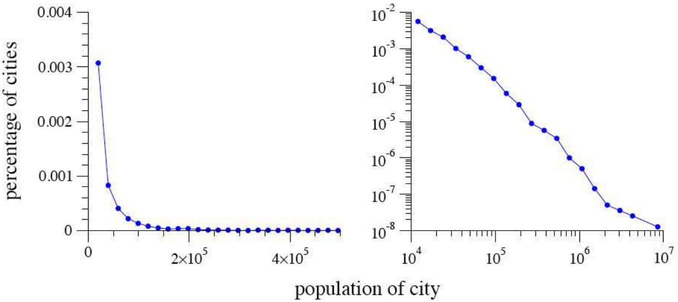


Figure: Power law $w(x) = ax^{-(1+b)}$

Dynamics → robustness → fragility

Dynamics of scale-free distributions

V. Pareto: "The rich get richer"

Dynamics → robustness → fragility

Dynamics of scale-free distributions

V. Pareto: "The rich get richer"

Robustness of scale free distributions

The market is stabilized by the hubs of wealth.

Dynamics → robustness → fragility

Dynamics of scale-free distributions

V. Pareto: "The rich get richer"

Robustness of scale free distributions

The market is stabilized by the hubs of wealth.

Fragility of scale free distributions

Theft is easier when there are very rich people.

Policy guidance

Change dynamics

Modify the process of accumulation to assure a less fragile distribution of trust.

Policy guidance

Change dynamics

Modify the process of accumulation to assure a less fragile distribution of trust, wealth, evolutionary fitness. . . .

Policy guidance??

Change dynamics

Modify the process of accumulation to assure a less fragile distribution of trust, wealth, evolutionary fitness. . . .

Policy guidance??

Change dynamics

Modify the process of accumulation to assure a less fragile distribution of trust, wealth, evolutionary fitness. . . .

Moral

Simple social processes lead to complex policy problems.

Private vs public trust

But we only talked about private trust vectors.

Private vs public trust

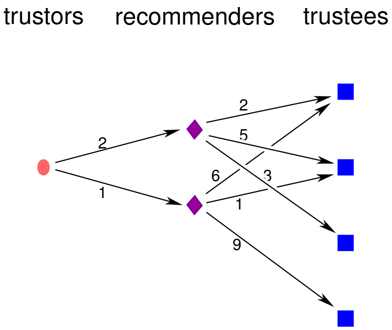
But we only talked about private trust vectors.

Why is private trust accumulation a social process?

Outline

Public trust process

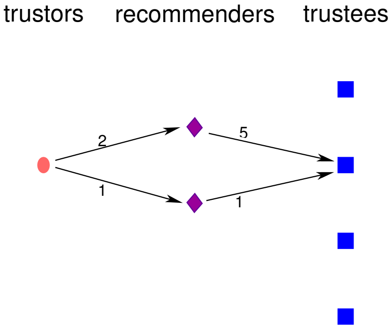
Using recommenders



2	A_1	2	5	3	0
1	A_2	6	1	0	9
σ	τ	10	11	6	9

Public trust process

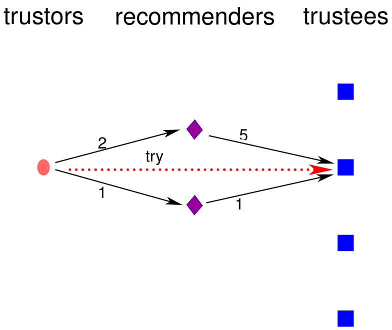
Using recommenders



2	A_1	2	5	3	0
1	A_2	6	1	0	9
σ	τ	10	11	6	9

Public trust process

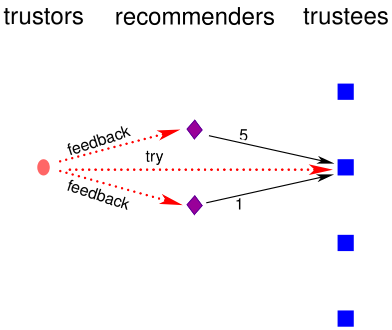
Using recommenders



2	A_1	2	5	3	0
1	A_2	6	1	0	9
σ	τ	10	11	6	9

Public trust process

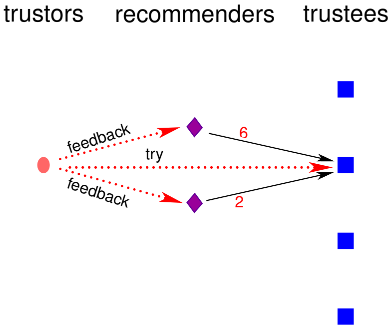
Using recommenders



2	A_1	2	5	3	0
1	A_2	6	1	0	9
σ	τ	10	11	6	9

Public trust process

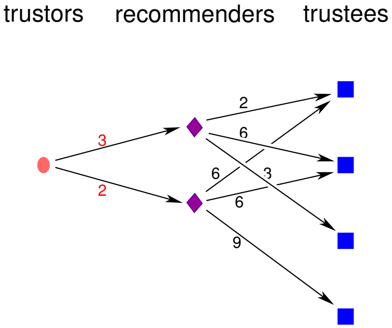
Using recommenders



2	A_1	2	6	3	0
1	A_2	6	2	0	9
σ	τ	10	14	6	9

Public trust process

Using recommenders



3	A_1	2	6	3	0
2	A_2	6	2	0	9
σ	τ	18	22	9	18

Public trust distribution

Upshot

Recommenders' public trust vectors also obey the power law distribution.

Recommenders' reputations obey the power law distribution.

Public trust distribution

Upshot

Recommenders' public trust vectors also obey the power law distribution.

Recommenders' reputations obey the power law distribution.

Consequence

Adverse selection

Outline

Fragility of trust networks

Corollary

The hubs attract attacks as soon as the trust is

(a) public

(b) uniform

(c) abstract

Fragility of trust networks

Corollary

The hubs attract attacks as soon as the trust is

(a) public
- ratings available to all

(b) uniform
- all certificates equally secure

(c) abstract
- "trust laundering" (*"Non olet."*)

Defending trust networks

Policy

Possible defense strategies are:

(a) non-public: private trust vectors
- recommendations must be public

(b) non-uniform: higher security for higher trust
- complicated; contradicts (a).

(c) non-abstract: retain trust concepts
- "trust unlaundering": $A \xrightarrow[r]{\Phi} B$

Defending trust networks

Policy

Possible defense strategies are:

(a) non-public: private trust vectors
  - recommendations must be public

(b) non-uniform: higher security for higher trust
  - complicated; contradicts (a).

(c) non-abstract: retain trust concepts
  - "trust unlaundering": $A \xrightarrow[r]{\Phi} B$
    - record feedback ($\sim$ "marked money")

Defending trust networks

Policy

Possible defense strategies are:

(a) non-public: private trust vectors
  - recommendations must be public

(b) non-uniform: higher security for higher trust
  - complicated; contradicts (a).

(c) non-abstract: retain trust concepts
  - "trust unlaundering": $A \xrightarrow[r]{\Phi} B$
    - record feedback ($\sim$ "marked money")
    - credit rating

Defending trust networks

Policy

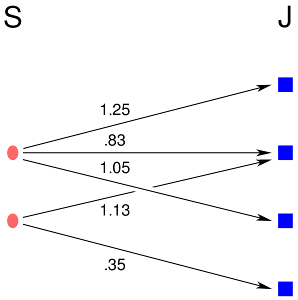
Possible defense strategies are:

(a) non-public: private trust vectors
- recommendations must be public

(b) non-uniform: higher security for higher trust
- complicated; contradicts (a).

(c) non-abstract: retain trust concepts
- "trust unlaundering": $A \xrightarrow[r]{\Phi} B$
  - record feedback ($\sim$ "marked money")
  - credit rating
  - trust concept **mining**

Find the spy



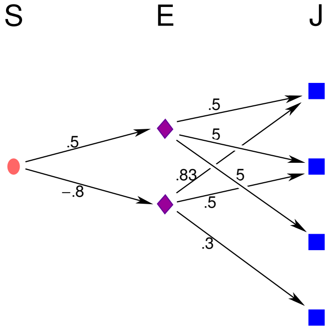
$$M = \begin{pmatrix} 1.25 & 1.05 & 1.12 & 1.57 \\ .83 & 1.13 & 1.02 & .35 \\ 0 & .35 & .21 & -.56 \end{pmatrix}$$

Spectral decomposition

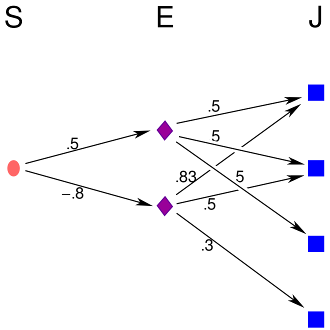
$$\begin{pmatrix} 1.25 & 1.05 & 1.12 & 1.57 \\ .83 & 1.13 & 1.02 & .35 \\ 0 & .35 & .21 & -.56 \end{pmatrix} =$$

$$\begin{pmatrix} .83 & -.4 \\ .55 & .6 \\ 0 & .7 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} .5 & .5 & .5 & .5 \\ 0 & .5 & .3 & -.8 \end{pmatrix}$$

Trust concepts

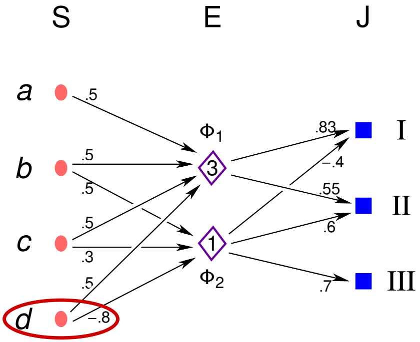


Trust concepts



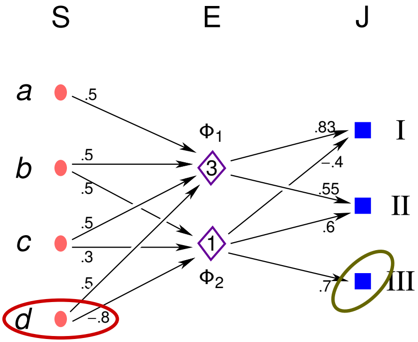
- traitor: $2\Phi_2 \leq -\Phi_1 \leq 0$

Trust concepts



- traitor: $2\Phi_2 \leq -\Phi_1 \leq 0$

Trust concepts



- traitor: $2\Phi_2 \leq -\Phi_1 \leq 0$
- dissident: $\Phi_2 \geq 2\Phi_1 \geq 0$

Trust concepts

Comment

The trust concepts are genuinely new information, generated by the network.

Trust concepts

Comment

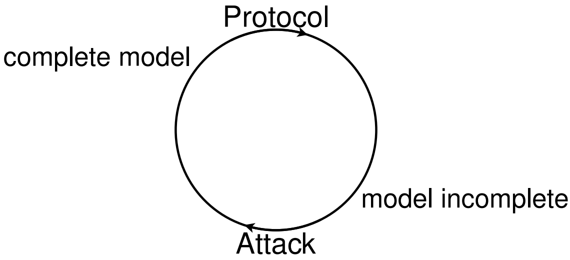
The trust concepts are genuinely new information, generated by the network.

A traitor is not recognized from a previously learned profile, but extracted from network dynamics as an intrinsic singularity.

Outline

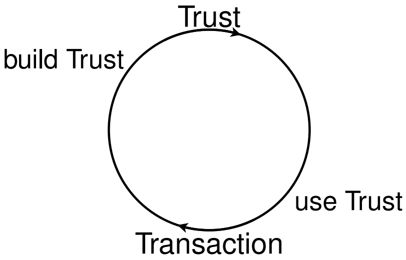
Security is an adversarial process

The life cycle of security

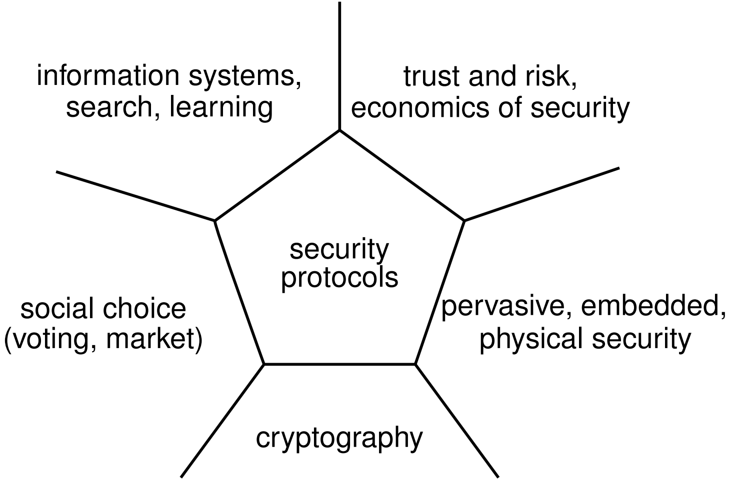


Trust is an adversarial process

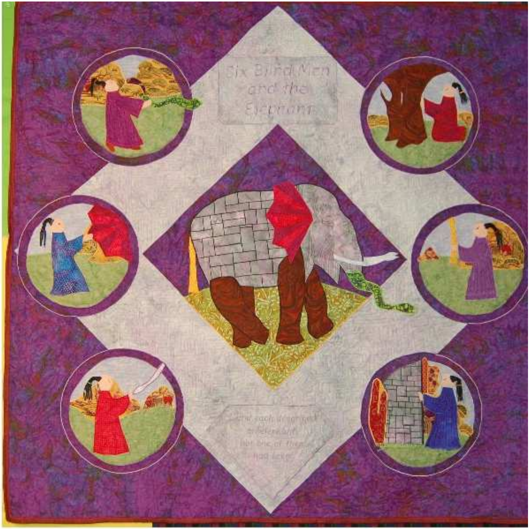
The life cycle of trust



Security is a collaborative process



Security and Trust Engineering



Six Blind Men and the Elephant