# From noninterference to trust: some considerations in the setting of the project NiRvAna

**Alessandro Aldini**
**University of Urbino, Italy**


Kickoff meeting progetto PRIN *Noninterference and Reversibility Analysis in Private Blockchains*, Fano 9-11/02/2022

# Noninterference

## Original idea

Definition A group of *high*-level agents, performing *high* operations only, is not interfering with a group of *low*-level agents, observing *low* operations only, if what the first group can do with the *high* operations has no effect on what the second group can see

- Example: in the security setting, noninterference analysis can reveal direct and indirect information flows, called *covert channels*, that violate the access policies based on the different access clearances assigned to different groups
- Not only in security, but also in dependability and performability analysis

# Noninterference

## Original idea

Definition A group of *high*-level agents, performing *high* operations only, is not interfering with a group of *low*-level agents, observing *low* operations only, if what the first group can do with the *high* operations has no effect on what the second group can see

- Formalized in process algebra, imperative languages, ...
- Various noninterference conditions and properties: (non-)deterministic, compositional, intransitive, local, ...
- Based on different formalizations of equivalence: trace, bisim., ...
- Extended in quantitative settings (observing frequency/duration of observations, exact/approximate measurements, ...)
- Example: `https://www.researchgate.net/publication/222566657_Component-oriented_verification_of_noninterference`

# Noninterference and reversible computing

## Issues to consider

- Do the reversibility operations cause information flows? And do the mechanisms allowing for reversibility interfere with the normal execution whenever reversibility is not necessary?
- Vice versa, which noninterference conditions do we need in the scenario above?
- What noninterference properties ensure that the low-level agents cannot distinguish which, if any, high operation has occurred at some point in the past
- Performance-oriented perspective: exact quantitative noninterference may be not satisfied, measure performance metrics to estimate the capacity of the interference channel

# Trust and reversible computing

**Other issues to consider**

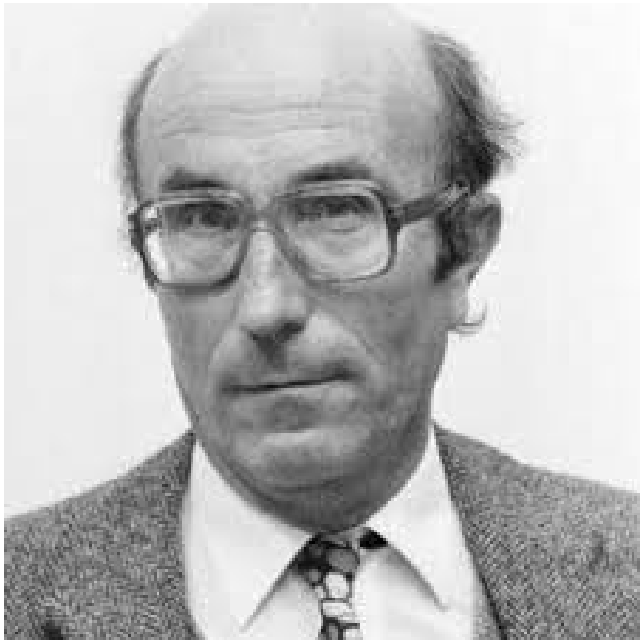
- Who is authorized to enable reversibility?

# Trust

**"Trust is a solution to specific problems of risk"**

*Familiarity confidence trust: problems and alternatives*

Niklas Luhmann, 1988



- Trust fosters cooperation
- Trust reduces the complexity of decision making under uncertainty
- Trust supports the development of an environment perceived as secure

# What is (*computational*) TRUST

**Trust as a relation . . .**

. . . between an agent/entity (the trustor) and another agent/entity (the trustee) *estimating* the expectation of the trustor about the future behavior of the trustee on which the trustor depends

. . . characterized by some degree of (*epistemic*) uncertainty and nondeterminism, as opposed to the notion of trustworthiness, which refers to the inherent, objective quality of the trustee

. . . related to risk (but also opportunity)

# Trust in digital environments

## Trust and security

Authentication *trust* models to support pass-through authentication and digital identity trust ecosystems and federations

Authorization *trust* models to support distributed authorization systems

## Trust dimensions

WHAT Simplex vs. Multiplex form of trust

HOW Moralistic vs. Strategic form of trust

WHOM Particular vs. General form of trust

## Trust components

- Computing component: explaining how trust is generated
- Manipulating component: explaining the dynamics of trust

# A logic for computing trust from personal evidence

Models of trust concentrated on the manipulating component, based on a computational treatment of facts and experience, based on incentive/punishment mechanisms, variably suffering from attacks such as bad mouthing and ballot stuffing, collusion, on-off, white-washing, sybil, ...

Verification of trust models based on simulation, model checking, ...

Computing trust values from scratch *next slides*

# A logic for computing trust from personal evidence

## Syntax

- atomic propositions: set $At$ ranged over by $p, q, \ldots$ (e.g., "This access is SSL-VPN protected", "Alice is trustworthy")
- syntax of the language of trust LT:

$$\phi \ ::= \ p \mid \neg\phi \mid \phi \wedge \phi \mid T(\phi)$$

where the *trust formula* $T(\phi)$ is read as "the agent trusts that $\phi$ holds"

# A logic for computing trust from personal evidence

## Semantics

A **trust model** is a tuple $M = (S, \pi, b, \theta, \Delta)$, where:

- $S$ is a finite set of states
- $\pi : At \mapsto \mathcal{P}(S)$ (*valuation function*) assigns to each $p \in At$ the set of states in which $p$ holds
- $b : S \mapsto (\mathcal{P}(S) \setminus \emptyset)$ (*belief function*) assigns to each $s \in S$ the consistent set of states that are *compatible* with what is believed by the agent in $s$
- $\theta : At \mapsto ]0, 1[$ (*trust threshold function*) assigns to each $p \in At$ the threshold needed to trust $p$

# A logic for computing trust from personal evidence

## Semantics

A **trust model** is a tuple $M = (S, \pi, b, \theta, \Delta)$, where:

- $\Delta$ (*trust relevance set*) is a family of trust relevance functions:

$$\delta_p : \mathsf{LT} \mapsto [0, 1] \qquad \forall p \in At$$

such that the relevance set of $p$, defined as $Rel_p = \{\phi \mid \delta_p(\phi) > 0\}$, is finite and satisfies the additivity condition:

$$\sum_{\phi \in Rel_p} \delta_p(\phi) = 1$$

# A logic for computing trust from personal evidence

## Semantics of trust

Ideally, the trust towards a proposition $p$ in $s$ is based on the relevant information holding in $s$:

$$\tau_p(s) = \sum_{(M,s)\models\phi} \delta_p(\phi)$$

To deal with trust towards composite formulas, we need some extensions:

## $\theta^e$: extending $\theta$ to formulas

- $\theta^e(p) = \theta(p)\ \forall p \in At$
- $\theta^e(\neg\phi) = 1 - \theta^e(\phi)$
- $\theta^e(\phi \wedge \psi) = \max(\theta^e(\phi), \theta^e(\psi))$
- $\theta^e(T(\phi)) = \theta^e(\phi)$

# A logic for computing trust from personal evidence

## Semantics of trust

Ideally, the trust towards a proposition $p$ in $s$ is based on the relevant information holding in $s$:

$$\tau_p(s) = \sum_{(M,s)\models\phi} \delta_p(\phi)$$

To deal with trust towards composite formulas, we need some extensions:

## $\tau^e_\phi$: extending $\tau_p$ to formulas

- $\tau^e_{(p)}(s) = \tau_{(p)}(s)\ \forall p \in At$
- $\tau^e_{(\neg\phi)}(s) = 1 - \tau^e_{(\phi)}(s)$
- $\tau^e_{(\phi\wedge\psi)}(s) = min(\frac{\tau^e_{(\phi)}(s)\cdot\theta^e(\phi\wedge\psi)}{\theta^e(\phi)}, \frac{\tau^e_{(\psi)}(s)\cdot\theta^e(\phi\wedge\psi)}{\theta^e(\psi)})$
- $\tau^e_{T(\phi)}(s) = \tau^e_\phi(s)$

# A logic for computing trust from personal evidence

## Satisfiability relation

Given a trust model $M = (S, \pi, b, \theta, \Delta)$ and $s \in S$, formula $\phi \in \mathrm{LT}$ holds in $s$, $(M, s) \models \phi$, if:

- $(M, s) \models p$ iff $s \in \pi(p)$ $\forall p \in At$
- $(M, s) \models \neg\phi$ iff $(M, s) \not\models \phi$
- $(M, s) \models \phi \wedge \psi$ iff $(M, s) \models \phi$ and $(M, s) \models \psi$
- $(M, s) \models T(\phi)$ iff $\forall s' \in b(s).\, \tau^e_\phi(s') > \theta^e(\phi)$

# A logic for computing trust from personal evidence

## Some properties of trust

| | |
|---|---|
| **K**: | $T(\phi \to \psi) \to (T(\phi) \to T(\psi))$ |
| **D**: | $\neg(T(\phi) \wedge T(\neg\phi))$ |
| **4**: | $T(\phi) \to T(T(\phi))$ |
| $dis_\wedge$: | $T(\phi \wedge \psi) \leftrightarrow T(\phi) \wedge T(\psi)$ |
| $dis_\vee$: | $T(\phi) \vee T(\psi) \leftrightarrow T(\phi \vee \psi)$ |
| *mp*: | If $\models \phi \to \psi$ and $\models \phi$, then $\models \psi$ |
| *nec*: | If $\models \phi$, then $\models \neg T(\neg\phi)$ |

# A logic for computing trust from reputation

## The notion to formalize

- Users provide (boolean) evaluations for certain behaviors
- Evaluations are combined to provide a reputation score, which is then used to feed the trust model

## Useful formalizations

- Graded modal logic: $\Diamond_n \phi$ holds whether $\phi$ holds in strictly more than $n$ accessible states of the system
- Majority logic: $W\phi$ holds whether $\phi$ holds in more than or equal to half of the accessible states of the system
- What do we obtain if we replace cardinalities with probabilities?

# A logic for computing trust from reputation

## Syntax

Given $At$ be a countable set of *propositional atoms* ranging over $\alpha, \beta, \gamma, \ldots$, and $A$ be a countable set of *labels* ranging over $a, b, c, \ldots$, the language of *trust evidence logic* $\mathcal{L}_{\mathbf{TEL}}$ is generated by:

$$\phi ::= \top \mid \alpha \mid \neg\phi \mid \phi \vee \phi \mid \langle a \rangle_p^{\geq} \phi$$

where $\alpha \in At$, $a \in A$, and $p \in \mathbb{Q}_{[0,1]}$

A logic such as this is classically interpreted over probabilistic (state/transition) labeled systems

# A logic for computing trust from reputation

## Interpretation for trust

- States represent agents
- Propositional atoms labeling the state associated with an agent represent the *evidences* that the agent believes to be true
- A transition from agent $s$ to agent $s'$ represents a connection from $s$ to $s'$ enabling the diffusion of opinions from $s'$ to $s$
- The transition label represents the context to which the connection is related
- The transition probability associated to a connection from agent $s$ to agent $s'$ represents the level of expertise of $s'$ as perceived by $s$ with respect to the related context
- The modal operator $\langle a \rangle_p^{\geq} \phi$ expresses that $\phi$ is subject to a trust estimation in the context of label $a$, so that the evaluation of such a formula for a given agent says whether the agent trusts $\phi$ or not with respect to a given trustworthiness threshold $p$

# A logic for computing trust from reputation

## Semantic model

Probabilistic Labelled State-Transition System Tuple $(S, At, A, \{\mathcal{D}_a\}_{a \in A}, v)$, where:

- $S$ is a non-empty countable set of states
- $At$ is the countable set of state labels
- $A$ is the countable set of transition labels
- $v$ is a *valuation function* $v : S \to \wp(At)$
- $\{\mathcal{D}_a\}_{a \in A}$ is a family of probabilistic transition functions of the form $\mathcal{D}_a : S \times S \to [0, 1]$ such that:

$$\forall s \in S : \quad \sum_{t \in S} \mathcal{D}_a(s, t) = 1$$

# A logic for computing trust from reputation

## Satisfiability relation

Given $\mathfrak{M} = (S, At, A, \{\mathcal{D}_a\}_{a \in A}, v)$, a formula $\phi \in \mathcal{L}_{\mathbf{TEL}}$ holds in a state $s \in S$, $s \models_{\mathfrak{M}} \phi$, if:

(a) $s \models_{\mathfrak{M}} \top$ iff true;

(b) $s \models_{\mathfrak{M}} \alpha$ iff $\alpha \in v(s)$, where $\alpha \in At$;

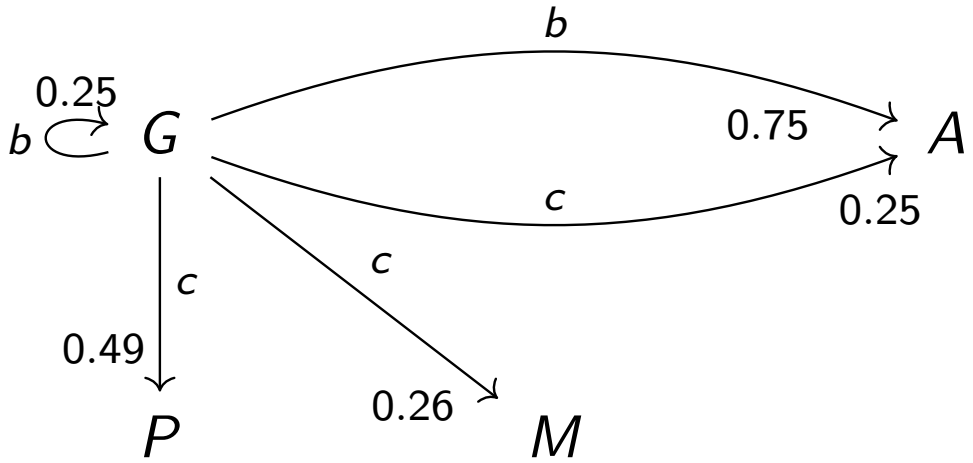
(c) $s \models_{\mathfrak{M}} \neg\phi$ iff $s \not\models_{\mathfrak{M}} \phi$;

(d) $s \models_{\mathfrak{M}} \phi \vee \psi$ iff $s \models_{\mathfrak{M}} \phi$ or $s \models_{\mathfrak{M}} \psi$;

(e) $s \models_{\mathfrak{M}} \langle a \rangle_p^{\geq} \phi$ iff $\mathcal{D}_a(s, S_\phi) \geq p$, where $p \in \mathbb{Q}_{[0,1]}$ and:

$$S_\phi \triangleq \{s' \in S \mid s' \models_{\mathfrak{M}} \phi\}$$

# Example




Let $G \models \neg\theta$, $P \models \phi \wedge \psi$, $M \models \phi \wedge \neg\psi$, and $A \models \neg\phi \wedge \neg\psi \wedge \theta$

Then, $G$ trusts $\phi$ w.r.t. $c$ and threshold 0.75, and distrusts $\psi$ w.r.t. $c$ and threshold 0.5, while $G$ trusts $\theta$ w.r.t. $b$ and threshold 0.75

# Meta-theory

## About soundness and completeness

- Given various classes of *normal* modal logics for our trust evidence logic (axiomatized by a given set $\Gamma$ of formulas),
- and given various classes of frames for PLSTSs (depending on the properties of the accessibility relation),
- it is provable which instances of the normal logics are sound and complete with respect to which classes of frames

# Conclusions

## Some challenges

- How noninterference theory can be employed in the setting of reversibility
- Which level of abstraction we need in real-world scenarios
- Security of blockchain technologies is sufficient or trust infrastructures can improve their diffusion

## Bibliography


- About the first logic: `https://www.researchgate.net/publication/358368349_From_belief_to_trust_a_quantitative_framework_based_on_modal_logic`
- About the second logic: `https://www.researchgate.net/publication/354727685_Trust_Evidence_Logic`