Identity Management in Social Networks

DistTrust Workshop

April 28, 2006 in Barcelona, Spain

Andreas Pfitzmann

Dresden University of Technology, Department of Computer Science, D-01062 Dresden
Phone: +49 351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de

Marit Hansen

Independent Centre for Privacy Protection Schleswig-Holstein, Holstenstr. 98, D-24103 Kiel
Phone: +49 431/988-1214, e-mail: marit.hansen@acm.org

Distrust is the organizing principle, not trust (1)

Collaboration *without* the need of mutual trust

is the basis of organizing modern societies.

Separation of powers, checks and balances etc. illustrate that mutual distrust should be the basis.

Confidentiality vs. integrity / availability :

You can't check whether your trust has been justified

vs. you can check whether your trust has been justified.

Distrust is the organizing principle, not trust (2)

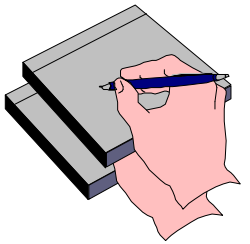
If you can check whether your trust has been justified, collaboration often works like this:

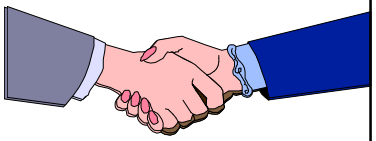
Invest some little trust in collaborating in a first step, but then check whether your trust and collaboration has been honored by the other parties involved.

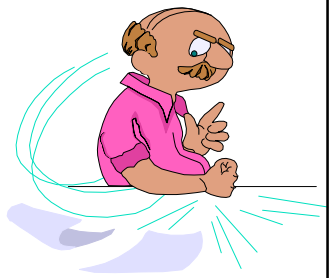
But since trust w.r.t confidentiality cannot be checked, this works w.r.t. integrity and availability at best.

Multilateral security

- Each party has its particular protection goals.
- Each party can formulate its protection goals.
- Security conflicts are recognized and compromises negotiated.
- Each party can enforce its protection goals within the agreed compromise.







Security with minimal assumptions about others

Kai Rannenberg, Andreas Pfitzmann, Günter Müller: IT Security and Multilateral Security; in: G. Müller, K. Rannenberg (Eds.): Multilateral Security in Communications, Addison-Wesley 1999, 21-29

Andreas Pfitzmann: Multilateral Security: Enabling Technologies and Their Evaluation; in: R. Wilhelm (Ed.): Informatics – 10 Years Back, 10 Years Ahead, August 27-31, 2000, Schloss Dagstuhl, LNCS 2000, Springer-Verlag, Heidelberg 2001, 50-62

Protection Goals

	Content	Circumstances
Prevent the unintended	Confidentiality Hiding	Anonymity Unobservability
Achieve the intended	Integrity	Accountability
	Availability	Reachability Legal Enforceability

Necessary assumptions about others:
Content: Communication partner cooperates
Circumstances: Even if communication partner does not cooperate

Dynamic coalitions: For and/or against protection goals

Gritta Wolf, Andreas Pfitzmann: Properties of protection goals and their integration into a user interface; Computer Networks 32 (2000) 685-699

Golden rule

Since tamper-resistance of HW is all but good and organizations are far from perfect keeping secrets:

> Correspondence between organizational and IT structures

Personal data should be gathered, processed and stored, if at all, by IT in **the hands of the individual concerned**.

Privacy-enhancing identity management

Privacy-enhancing identity mgmt (PE-IDM): Each user decides which of his/her partial identities (named by pseudonyms) to use in which interactions with others.

PE-IDM is only possible w.r.t. parties which don't get widely used GUIDs anyway, by

- the communication network (e.g. network addresses)
- the user device (e.g. serial numbers, radio signatures), or even
- the user him/herself (e.g. by biometrics).

Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; The IPTS Report 67 (September 2002) 8-16

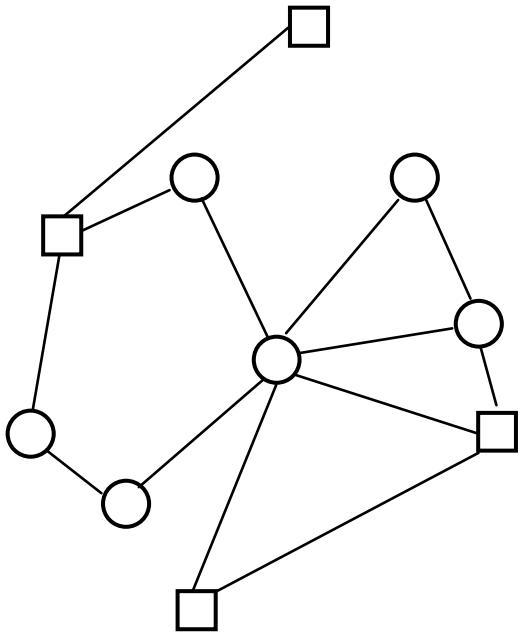
Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, Michael Waidner: Privacy-enhancing identity management; Information Security Technical Report 9/1 (Jan.-March 2004) 35-44

Pseudonyms: Linkability in detail

Distinction between:

1. **Initial linking** between the pseudonym and its holder
2. Linkability due to the **use** of the pseudonym **in different contexts**

The World today



person

organization

relationship

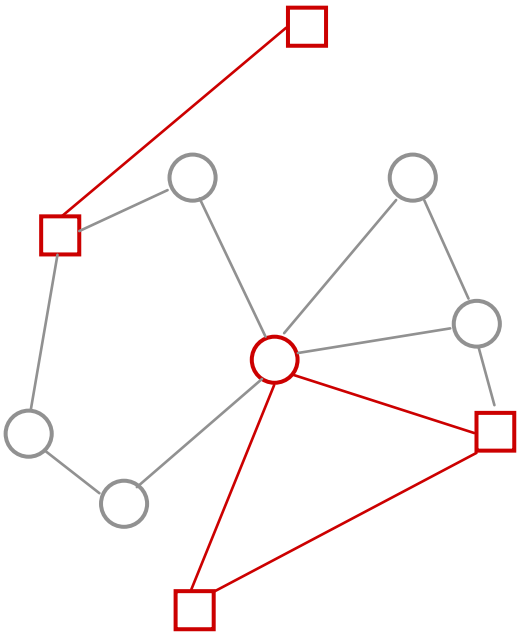
Many persons and many organizations have both direct and indirect relationships.

Persons and organizations talk with each other and about each other.

Organizations may require disclosure of (certified) PII before granting access to their services.

Trust in others comes in different shades of grey and evolves over time.

Chaum's World (1985)



person

organization

relationship

Isolated persons have both direct and indirect relationships with many organizations.

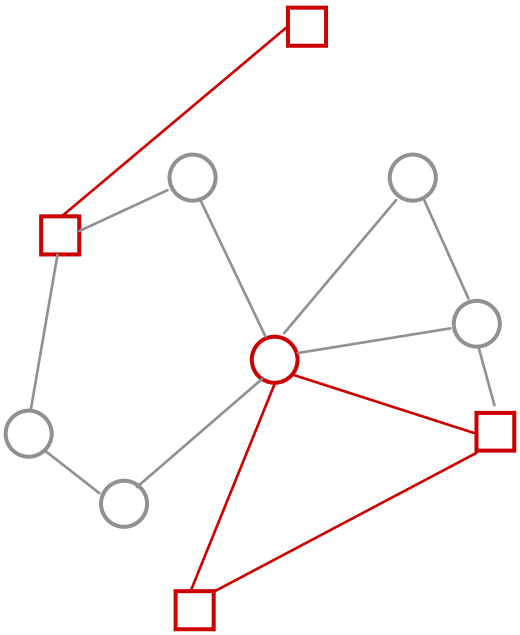
The persons talk with organizations, organizations cannot talk about individuals.

In particular, persons don't talk to persons and organizations have no common names for individuals.

W.r.t. privacy, the surrounding of each person is uniformly untrusted, i.e. no trust in organizations, no trust in computers of others (and by inference, no trust in other persons).

David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044

Chaum's World (1992)



person

organization

relationship

Isolated persons have both direct and indirect relationships with many organizations.

The persons talk with organizations, organizations cannot talk about individuals.

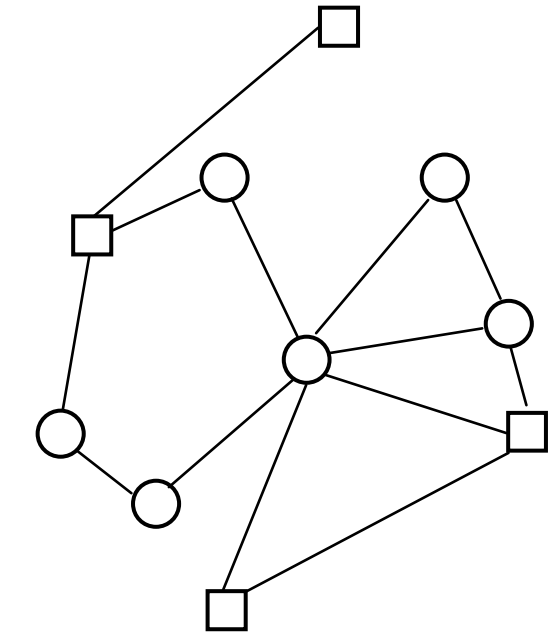
In particular, persons don't talk to persons and organizations have no common names for individuals.

W.r.t. privacy, the surrounding of each person is uniformly untrusted, i.e. no trust in organizations, no trust in computers of others (and by inference, no trust in other persons).

W.r.t. integrity, based on tamper-resistant modules within computers of persons, organizations trust these computers.

David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101

The World today – a closer look



Many persons and many organizations have both direct and indirect relationships.

Isolating persons is suitable for some applications only, other applications need direct communication between persons and might even need some awareness about the situation of the other person(s).

Persons and organizations talk with each other and about each other.

Preventing organizations from talking about individuals might work, but hindering individuals to talk about each other at least to a certain degree prevents some applications, e.g. group discussions.

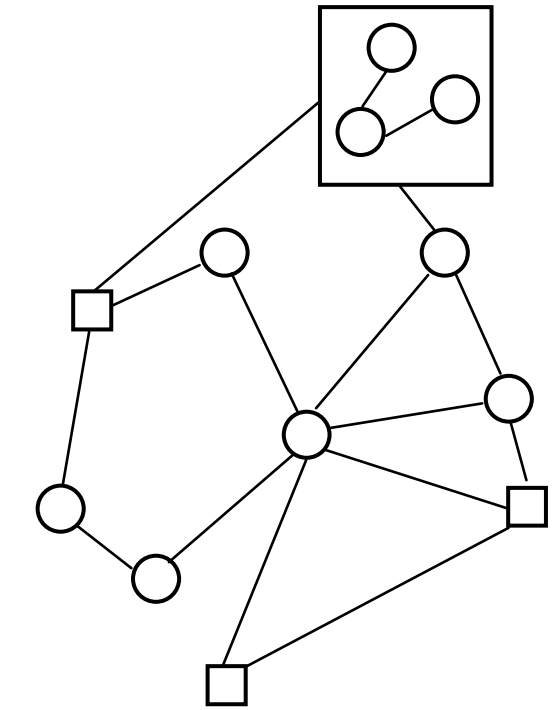
Organizations may require disclosure of (certified) PII before granting access to their services.

How to enable persons to exercise more control on their disclosed PII? How to enable organizations to handle these data in a privacy-aware way, based on the data subject's requirements and privacy preferences?

Trust in others comes in different shades of grey and evolves over time.

Not trusting the surrounding of each person uniformly may be inadequate, both socially and technically. E.g. it prevents any kind of team spirit and does not reflect technical opportunities, e.g. TPMs, to improve trustworthiness of computers.

The World tomorrow – a comprehensive approach needed



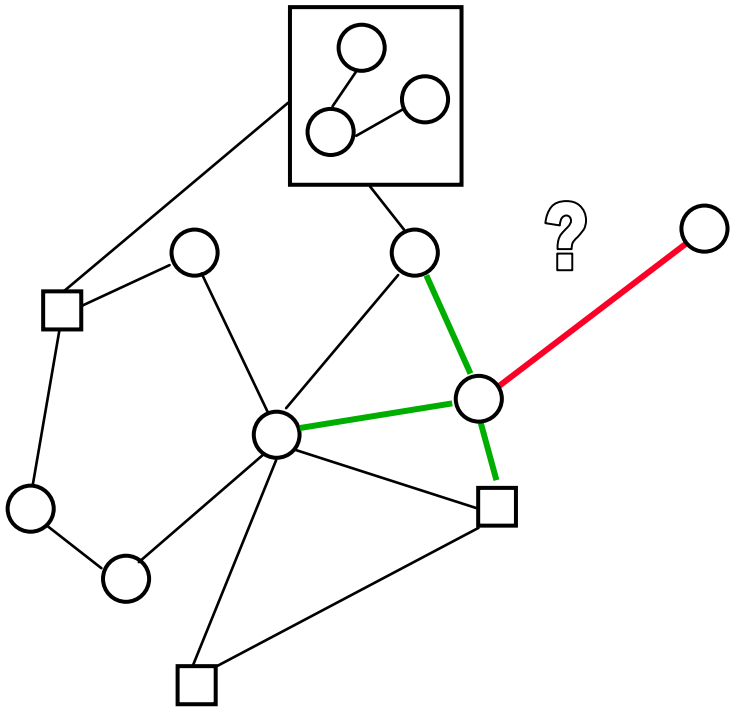
Persons (and usually also organizations - or persons representing organizations or persons within organizations) decide, when and how to isolate and when and what to share.

This means **framework** and **tools** have to support isolation and sharing (and everything in between) equally well:

- *Privacy policies* to ease understanding what personal data are needed for which services
- Simple to use, but powerful *usage interface*
- Different kinds of pseudonyms, with both very *secure and computationally efficient crypto* (anonymous credentials on small devices!).
- Means for *group-awareness and –interactions,* establishing and maintaining the *membership to both ad-hoc groups and organizations.*

Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, Sandra Steinbrecher:
What User-Controlled Identity Management Should Learn from Communities;
submitted to: Information Security Technical Report, 2006

The World tomorrow – interactions



person

organization

relationship

possible new relationship

relationships to build on

Interactions between persons and organizations build on existing or newly established relationships. This needs trust:

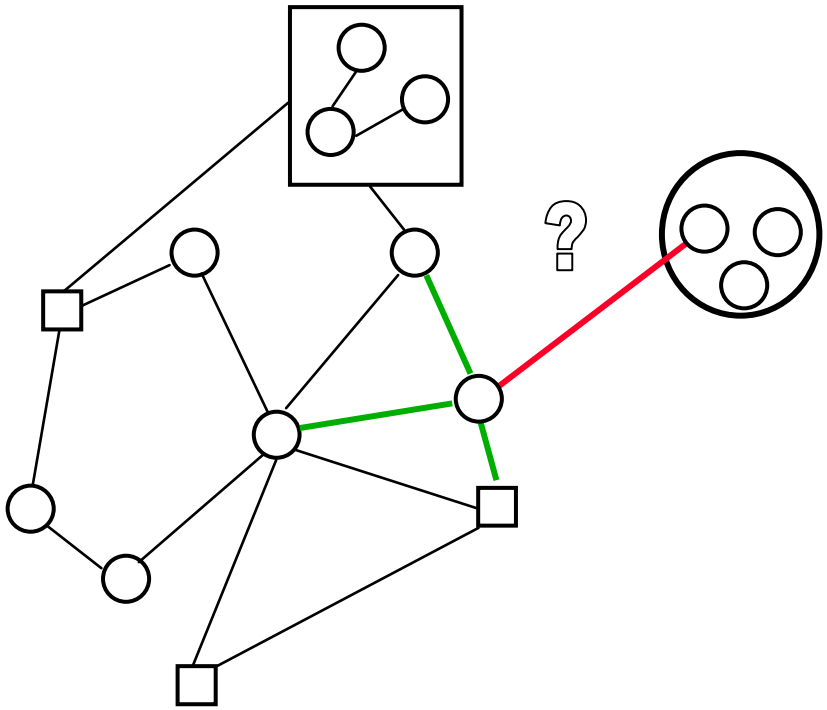
- technical trust in the devices and network used (TPM for *increasing trust in one's own computer*, for *remote attestation* and for *remote policy enforcement*)
- trust in the interactor.

This should be integrated in pseudonymous communication and applications!

If no pseudonymous relationship between the interactors had been established, both have to build on others' trust in the interactor. These others are the ones the interactors have a relationship to.

Technically this can be reached by pseudonymous trust management, e.g. by pseudonymous reputation systems.

The World tomorrow – protecting privacy and establishing trust



person

organization

relationship

possible new relationship

relationships to build on

Pseudonymous interactions need:

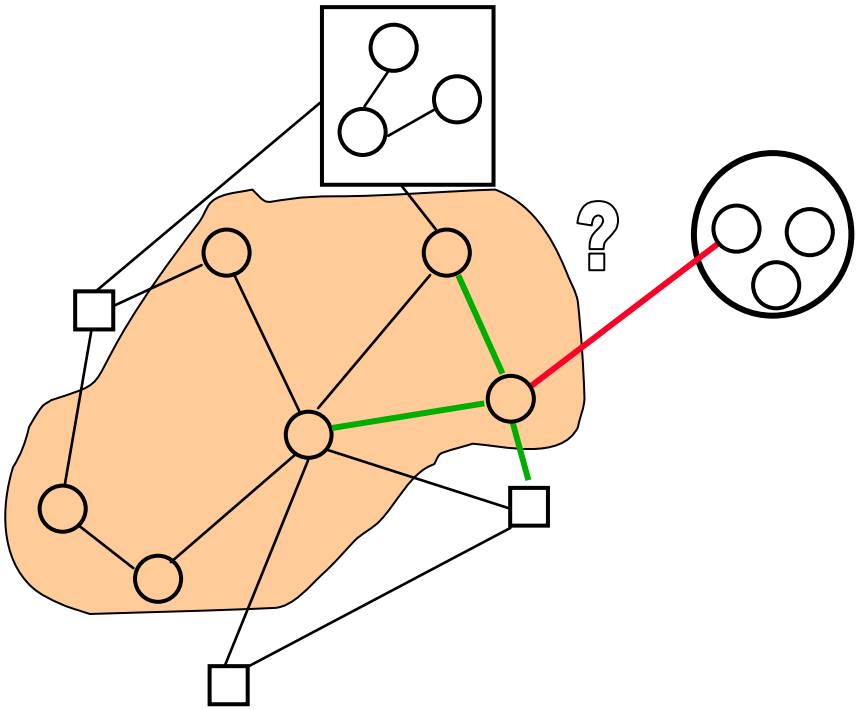
- trust in the other interactors,
- interacting under a pseudonym.

This needs the trust management used to support controlled transferability or convertability of trust in one pseudonym to another pseudonym belonging to the same person.

The convertability/transferability depends on

- who established the trust (whether an organization issued a credential or persons gave an input to a reputation system)
- in which context the interactor is trusted.

The World tomorrow – protecting privacy and establishing trust



person

organization

relationship

possible new relationship

relationships to build on

Distribution of tasks to a group of peers for realizing mechanisms such as

- anonymizing services (separation of knowledge) or
- exchange of reputation information (collection of knowledge).

Challenge:

Applying data protection principles to peers and their computers:

- Law addresses primarily organisations, not natural persons.
- What relationship to those whose data are processed?
- How to safeguard personal data of others?
- Minimisation of data is necessary.
- What about privacy of peers themselves?

Summing up: Dis(t)Trust

Requirements for multilaterally secure and privacy-enabling ICT:

- Make sure that **others cannot gather** “unnecessary data” (just not gathering it is not enough, as history tells us).
- Since trust in foreign infrastructures w.r.t. confidentiality properties (e.g. privacy) will be very limited at best, each human should have **his/her trusted device(s)** to provide for his/her security. This device might act in an ambient way in the interests of its owner.
- **Communication** of humans with their ICT-environment should be **by means of their trusted device** only.
- Develop trusted devices which have **no identifying radio signature**.
- **Minimize sensor abilities** w.r.t. sensing foreign human beings directly.

ANNEX

Excerpts from: Treaty Establishing a Constitution for Europe

Article I-2 The Union's values

The Union is founded on the values of respect for **human dignity**, **freedom**, **democracy**, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. ...

Article I-3 The Union's objectives

2. The Union shall offer its citizens an area of **freedom**, **security** and **justice** without internal frontiers, and an internal market where competition is free and undistorted.

Excerpts from: Treaty Establishing a Constitution for Europe

Article II-68 Protection of personal data

- Everyone has the right to the protection of personal data concerning him or her.

- Such data must be processed fairly for specified purposes and on the basis of the **consent of the person concerned** or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Threats and corresponding protection goals

threats:

protection goals:

1) unauthorized access to information

confidentiality

2) unauthorized modification of information

integrity

≅ partial correctness

≥ total correctness

3) unauthorized withholding of information or resources

availability for authorized users

no classification, but pragmatically useful

example: unauthorized modification of a program

1)	cannot be detected, but can be prevented;	cannot be reversed
2)+3)	cannot be prevented, but can be detected;	can be reversed

Protection Goals: Definitions

Confidentiality ensures the confidentiality of user data when they are transferred. This assures that nobody apart from the communicants can discover the content of the communication.

Hiding ensures the confidentiality of the transfer of confidential user data. This means that nobody apart from the communicants can discover the existence of confidential communication.

Anonymity ensures that a user can use a resource or service without disclosing his/her identity. Not even the communicants can discover the identity of each other.

Unobservability ensures that a user can use a resource or service without others being able to observe that the resource or service is being used. Parties not involved in the communication can observe neither the sending nor the receiving of messages.

Integrity ensures that modifications of communicated content (including the sender's name, if one is provided) are detected by the recipient(s).

Accountability ensures that sender and recipients of information cannot successfully deny having sent or received the information. This means that communication takes place in a provable way.

Availability ensures that communicated messages are available when the user wants to use them.

Reachability ensures that a peer entity (user, machine, etc.) either can or cannot be contacted depending on user interests.

Legal enforceability ensures that a user can be held liable to fulfill his/her legal responsibilities within a reasonable period of time.