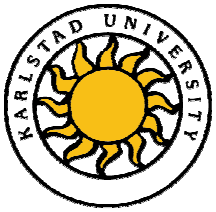
Privacy and Identity Management for Distributed Systems

Prof. Simone Fischer-Hübner

Karlstad University/Sweden

Keynote @ IEEE SRDS Symposium 2009

Niagara Falls / NY, 29. September 2009



Overview

I. Privacy Challenges & PETs

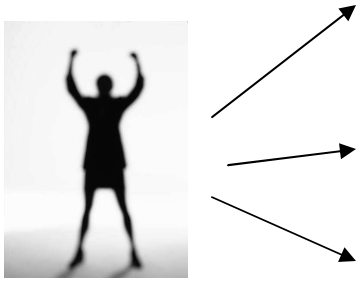
II. Identity & Anonymity in Ad Hoc Networks

- Self-certified, unlinkable, Sybil-free identifiers
- Chameleon anonymous protocol

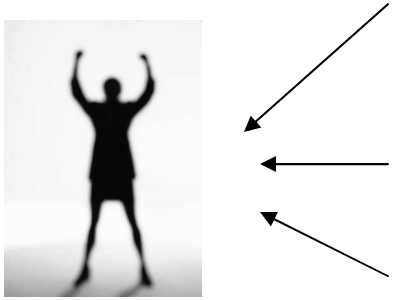
III. PrimeLife - Privacy and Identity Management for Life

I. Privacy Challenges & PETs: Privacy Dimensions

- Informational self-determination



- Spatial privacy

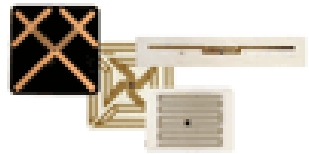


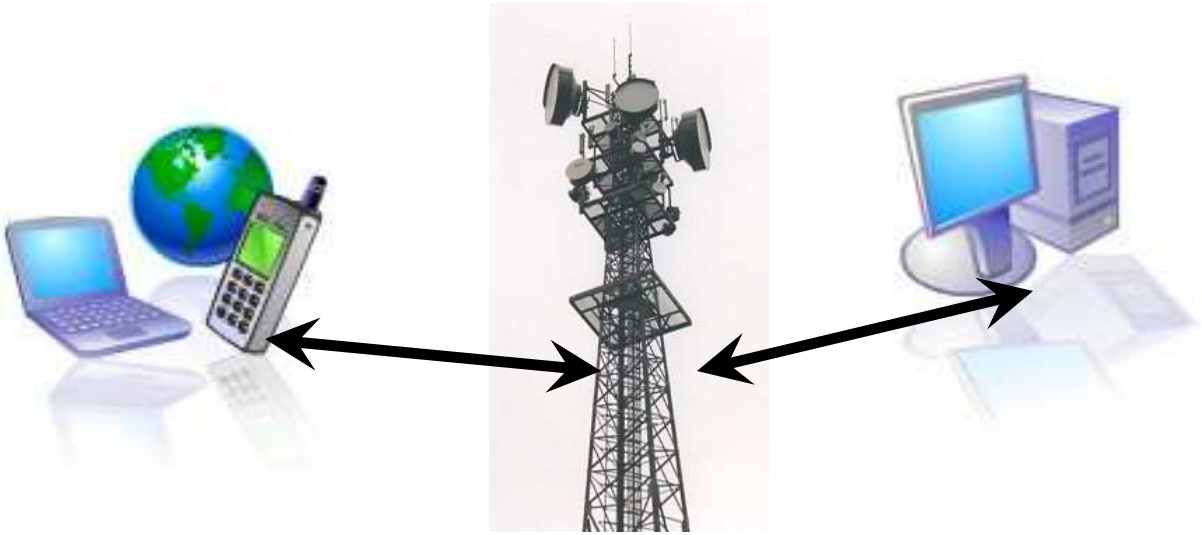
Basic Privacy principles
(implemented in EU-Directive 95/46/EC)

- Legitimisation by **law, informed consent** (Art. 7 EU Directive)
- **Data minimisation** (Art. 6 I c, Art. 7)
- **Purpose specification** and **purpose binding** (Art. 6 I b)
  - ”Non-sensitive” data do not exist !
- **Transparency**, rights of data subjects

Privacy Challenges

- Global networks, cookies, webbugs, spyware,...
- Location-based Services (LBS)
- Ambient Intelligence, RFID...
- Social Networks





Location Data /LBS – Privacy Risks

Privacy Risks:

- Unsolicited tracking of users' position, movements
- Unsolicited Profiling
- Disclosure of the user's current context
- Disclosure of social networks

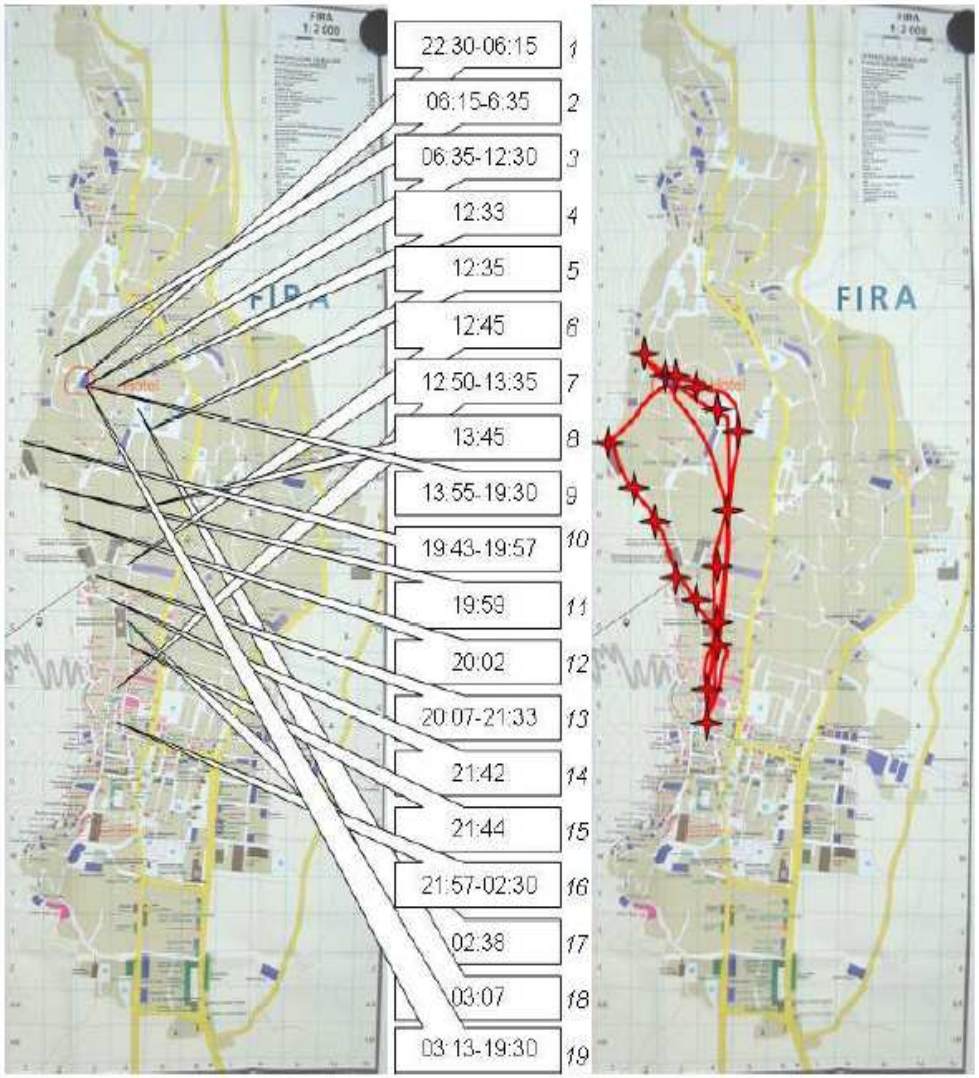


Image source: Rannenberg, Goethe Univ. Frankfurt

Privacy Risks of Social Networks

Uppdaterad 2007-10-25 19:01 Skriv ut Skicka

Enisa, det europeiska organet för nätverkssäkerhet, går i dag ut med en varning till dem som är med i nätverken på internet. Bland annat varnar man för att tagga, ansiktsidentifiera, sina vänner och anhöriga på bilder.

Facebook äger dig

"Det är ett slavkontrakt"

Samtliga 400 000 svenskar som registrerat sig på Facebook har skrivit över rättigheterna till sina bilder och hemligheter på det amerikanska företaget – för all evighet.

De har själva godkänt detta i ett 13-sidigt kontrakt

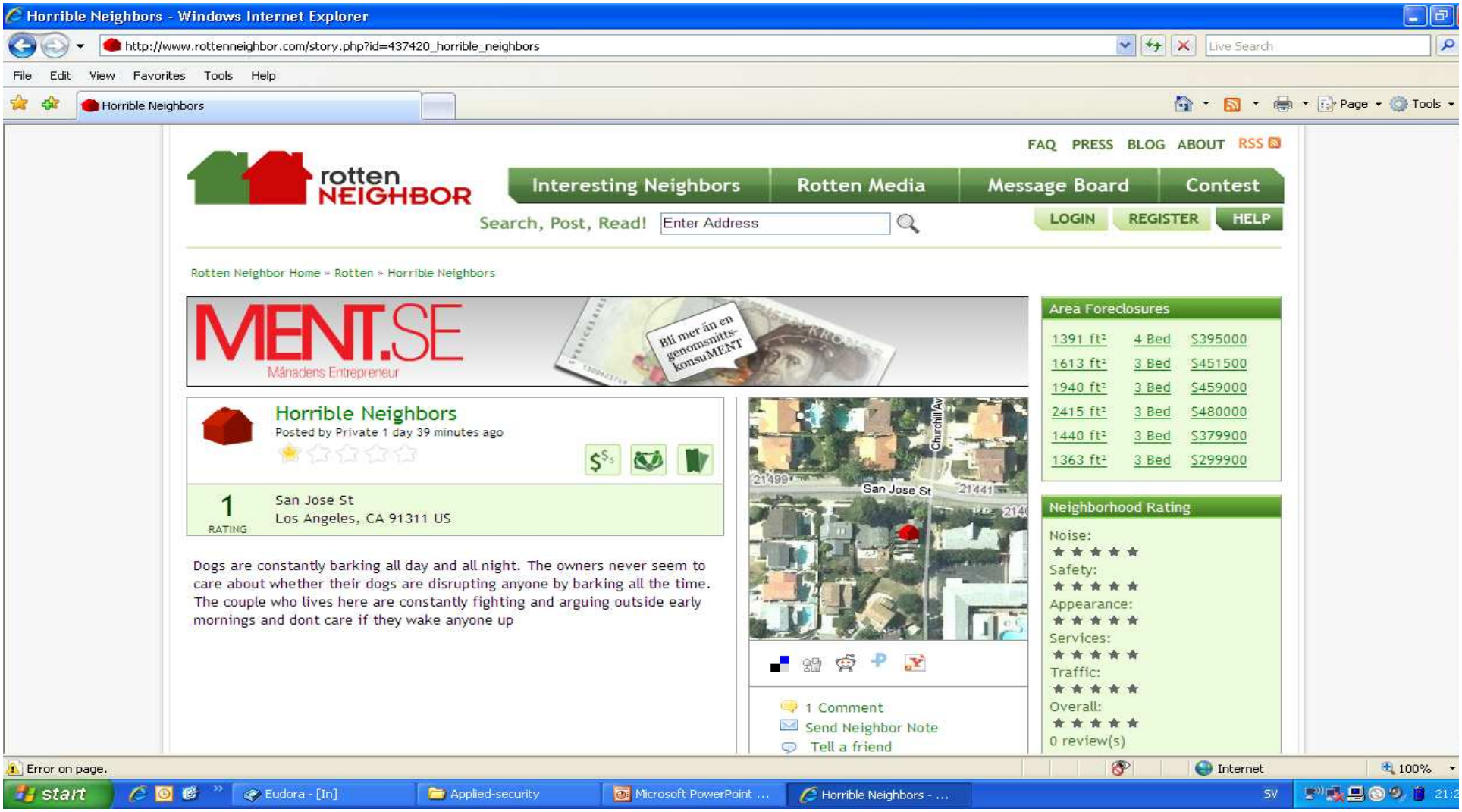
FACEBOOK ÄGER

- Dina mejl
- Dina bilder
- Dina intressen
- Dina filmer
- Dina kontaktuppgifter

- Intimate personal details about social contacts, personal life, etc.
- The Internet never forgets completely....
- Not only accessible by ”friends”

Freddi Staur (ID fraudster)

Privacy Risks of Social Networks –
Personal data/photos inserted by others



Privacy Risks of Social Networks – Social Network Analysis


The Stanford Daily

FRIDAY January 20, 2006

Home

OTHER ISSUES

«Prev Next»

Archives

Cool Jobs

FULL SCHOLARSHIPS FOR SCIENCE & TECHNOLOGY STUDENTS

KAUST Discovery Scholarship

READ MORE >

Employers snoop on Facebook

January 20, 2006

msnbc

Powered by Bing

MSN Home | Mail

featuring TODAY | Nightly News | Dateline | Meet the Press

Technology & science / Internet

Categories

U.S. news

World news

Politics

Business

Entertainment

Sports

Health

Tech & science

Space

Science

Tech and gadgets

Games

Oxford using Facebook to snoop

University e-mailing students fines of $80 to $200 for breaking rules

Oxford University students jump into the river from Magdeline Bridge to celebrate May Day. Officials at the university are now using Facebook as a way to find — and fine — troublemakers.

cebook.com began as a

ests, the site has now b

rin of some young job-seekers.

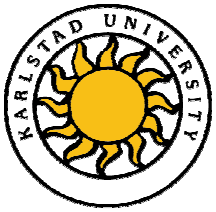
nent Center (CDC) Lance Choy confirmed that

eb searches to find background information on job

thered this practice by using Facebook.

Social Network Analysis/Profiling by:

- Employers
- Schools/Universities
- Direct Marketing
- Hackers
- Law Enforcement
- Tax authorities
- …..



Need for Privacy-Enhancing Technologies (PETs)

- Law alone is not sufficient for protecting privacy in our Network Society
- PETs needed for implementing Law
- PETs for increased transparency & user control

Classifications of PETs

1. PETs for minimizing/ avoiding personal data
(-> Art. 6 I c., e. EU Directive 95/46/EC)
(providing Anonymity, Pseudonymity, Unobservability, Unlinkability)

- At communication level:
  - Mix nets, Onion Routing, TOR
  - DC nets
  - Crowds,…
- At application level:
  - Anonymous Ecash
  - Anonymous Credentials,…

2. PETs for the safeguarding of lawful processing
(-> Art. 17 EU Directive 95/46/EC)

- P3P, Privacy policy languages
- Encryption,…

3. Combination of 1 & 2

- Privacy-enhancing Identity Management (PRIME, PrimeLife)

Platform for Privacy Preferences Initiative

PRIME Privacy and Identity Management for Europe

II. Identity & Anonymity in Ad Hoc Networks

Objective

How to obtain reliable anonymous communication?

⇩

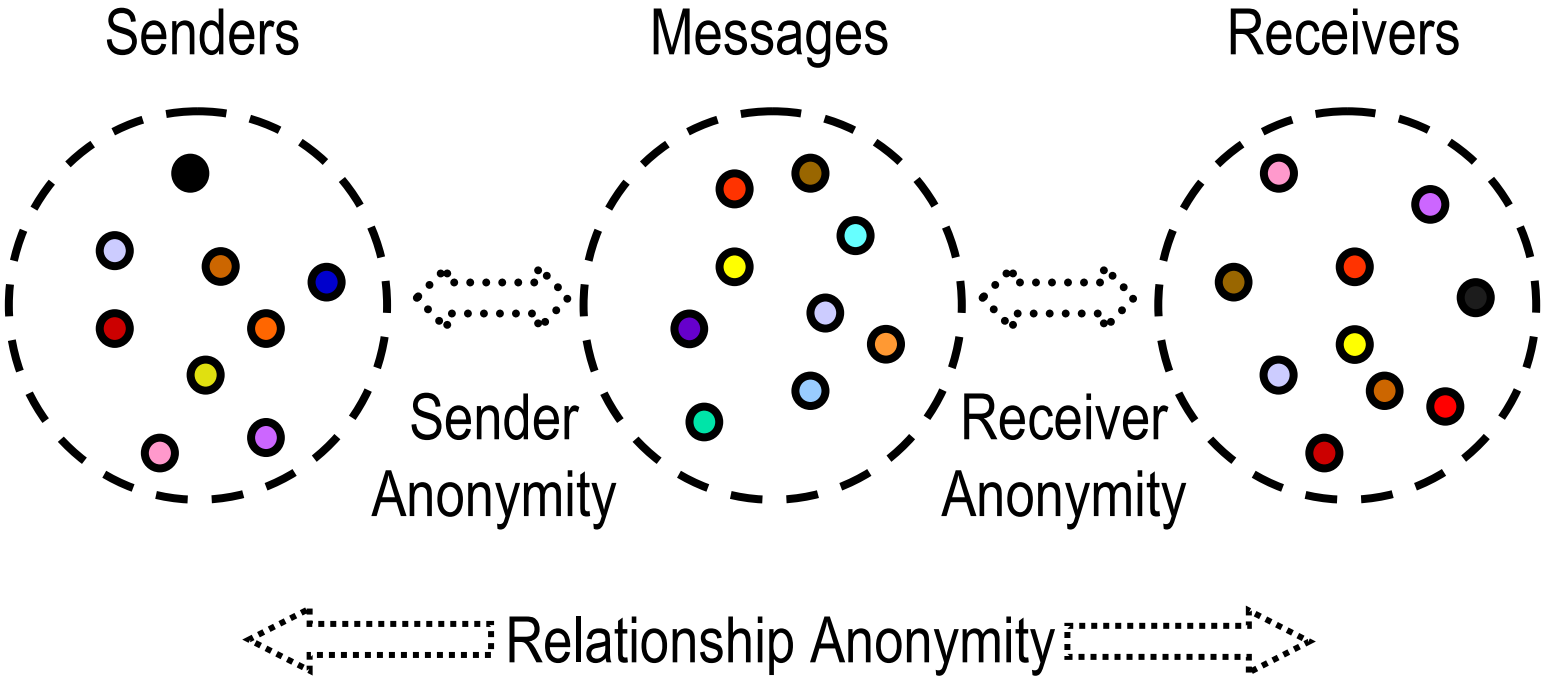
PRIVACY

is best protected with anonymity

ANONYMITY

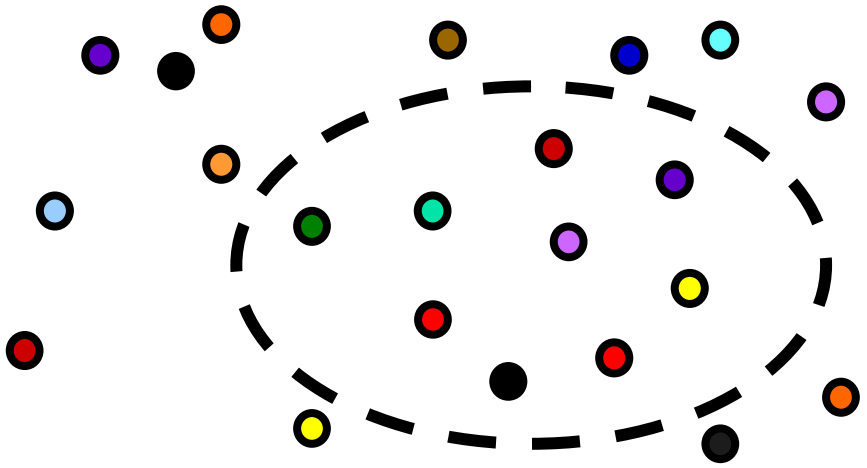
Is the basis for Privacy-Enhancing Applications

Goal: Anonymity - Unlinkability between items of interest



Anonymous Communication Functions

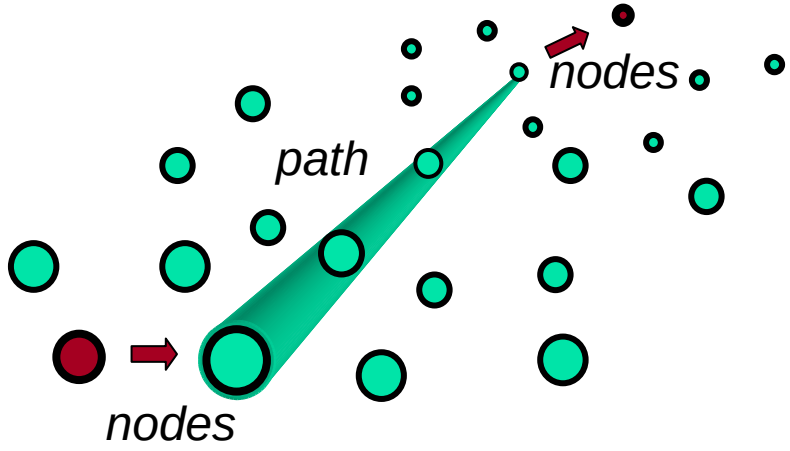
(1) Grouping Function



The anonymity set

How to design privacy-friendly identifiers?

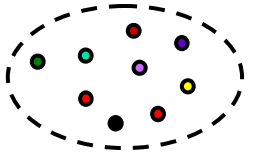
(2) Embedding Function



The anonymous path

How to establish an anonymous (virtual) path?

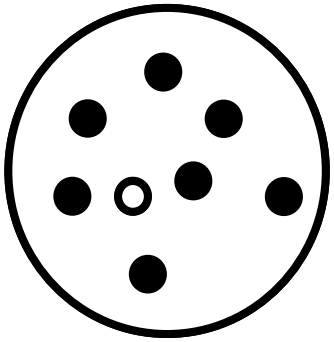
Source: Martucci et al. 2008



The anonymity set

Ad (1): Grouping Function

- Identifiers in Ad Hoc Networks
  - No native trustworthy identification scheme in ad hoc networks
  - Perfect environment for achieving anonymity?



Sybil Attacks

Identifiers are needed to provide anonymity

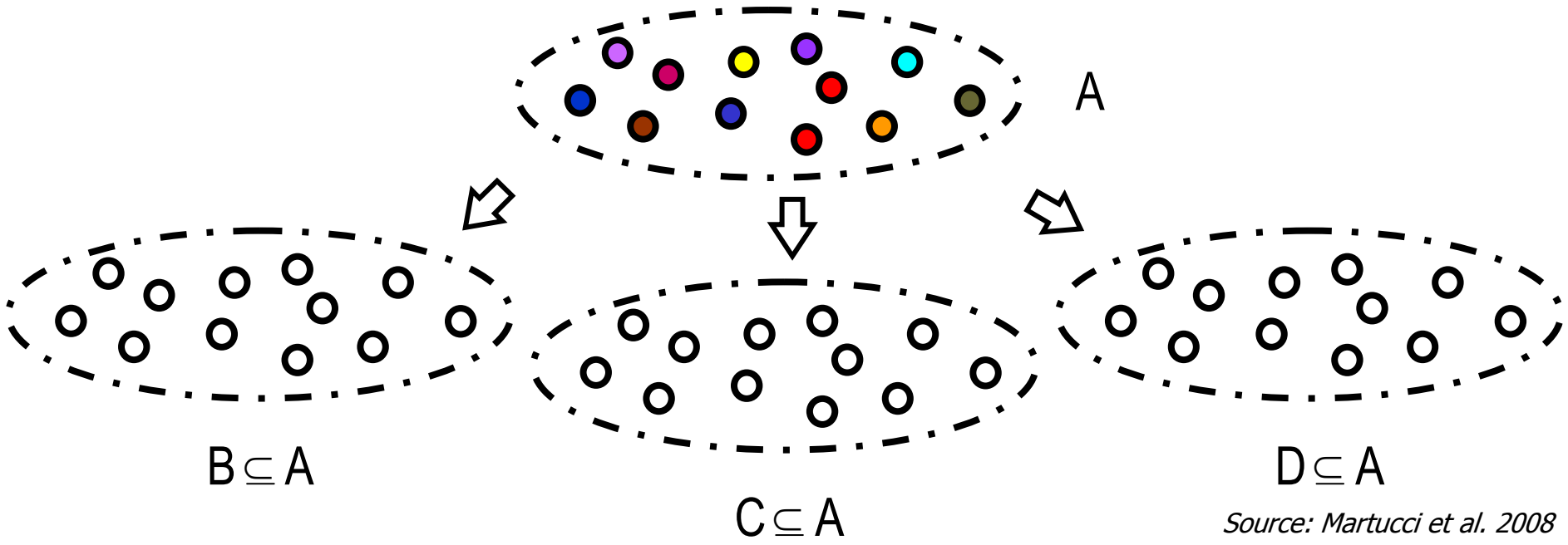
⇩

The Identity-Anonymity Paradox

Source: Martucci et al. 2008

Self-Certified, Unlinkable Sybil-Free Identifiers

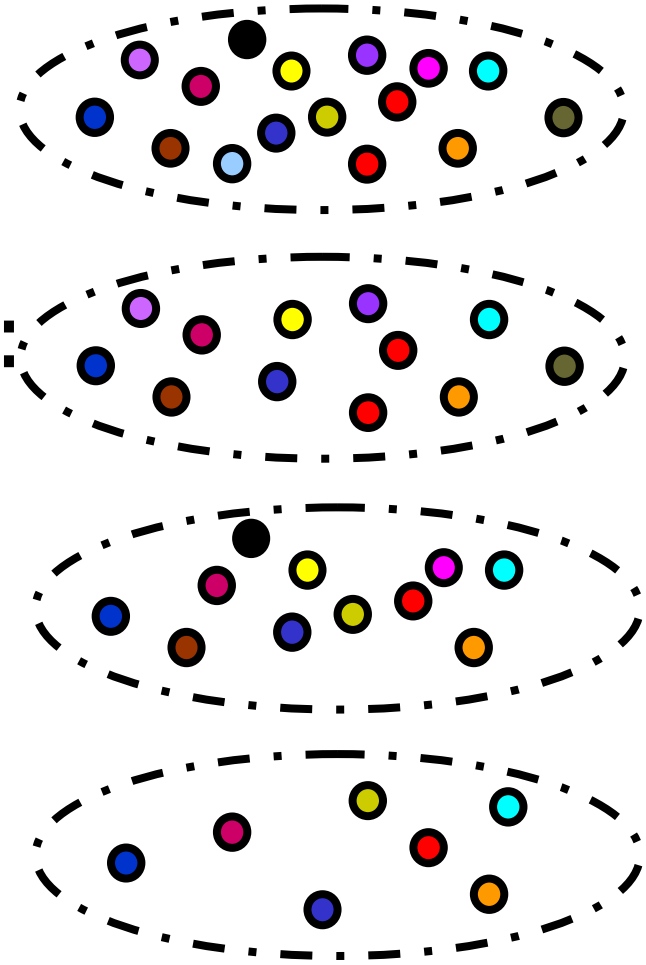
- Given: Initial Sybil-free Identity Domain
- How to propagate Sybil-freeness to arbitrary many identity (sub) domains, such as
  - In every identity domain each user is known under a different unique pseudonym (-> unlinkability)



Source: Martucci et al. 2008

Application Example: Sets and e-Voting

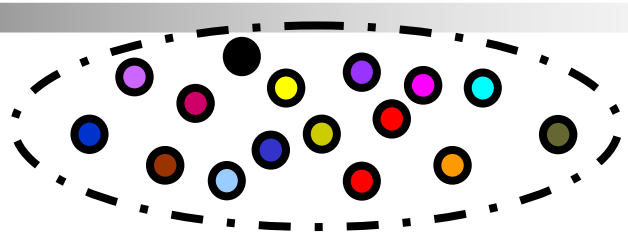
- a set of voters:
- a subset that votes:
- next election:
- next election:



Source: Martucci et al. 2008

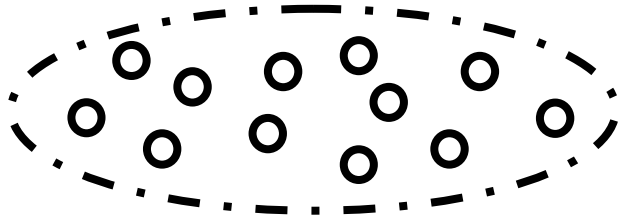
Anonymous e-Voting

- a set of voters:



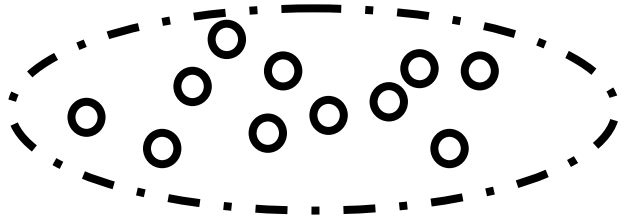
A

- a subset that votes:



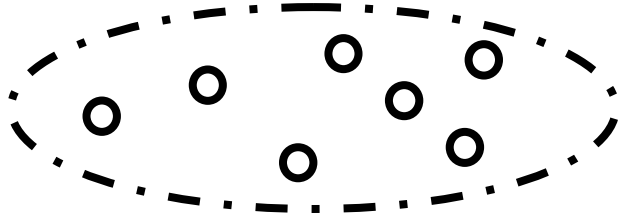
B $B \subseteq A$

- next election:



C $C \subseteq A$

- next election:

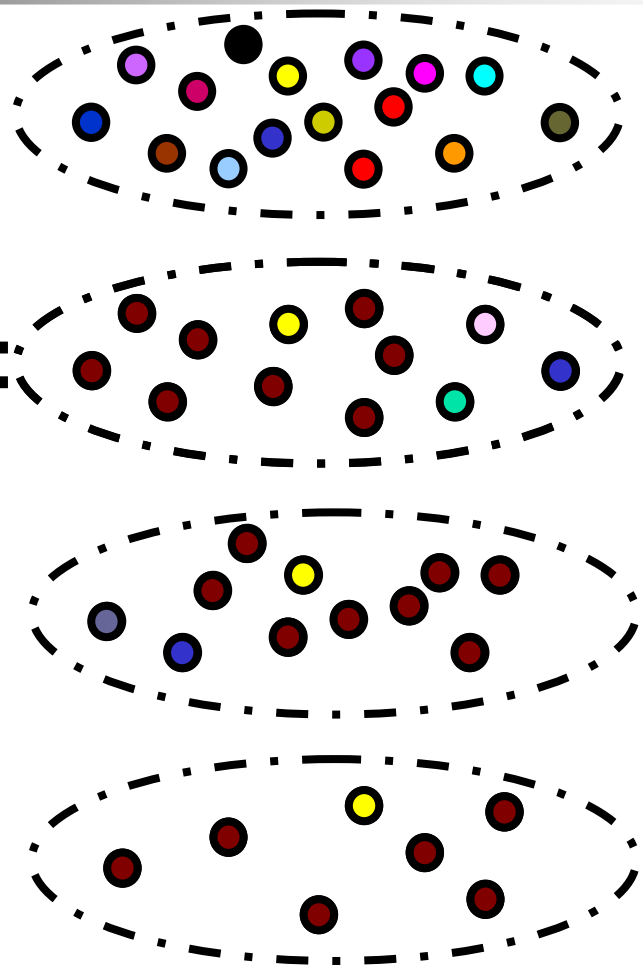


D $D \subseteq A$

Source: Martucci et al. 2008

Sybil Attack and e-Voting

- a set of voters:
- a subset that votes:
- next election:
- next election:



A

B $B \subseteq A$

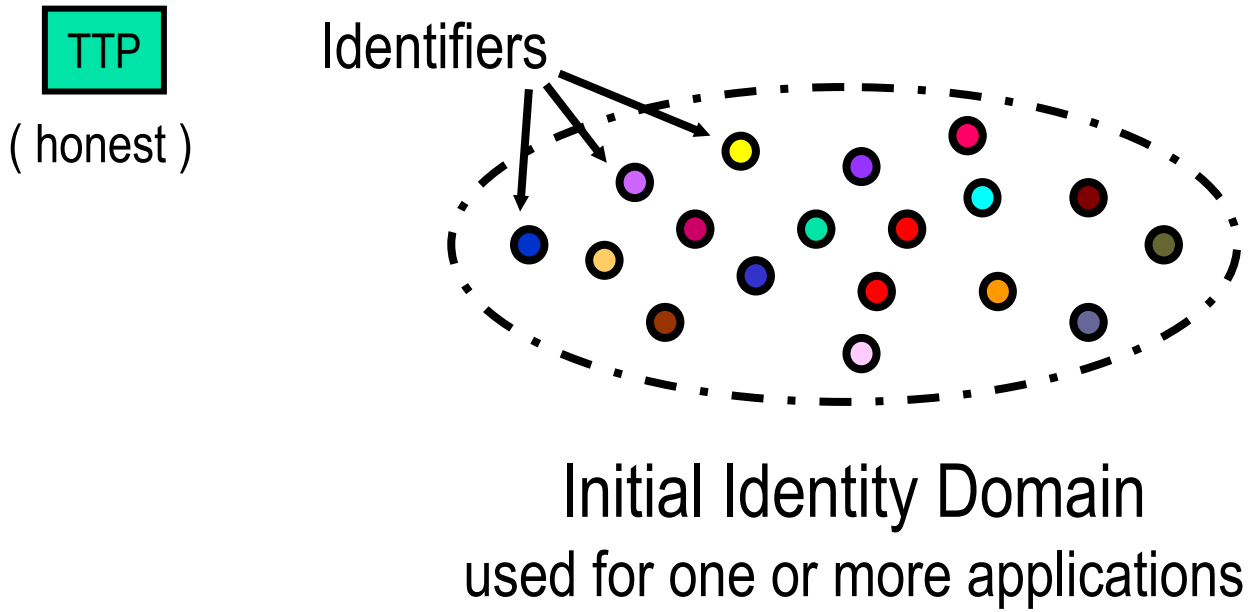
C $C \subseteq A$

D $D \subseteq A$

Source: Martucci et al. 2008

The Initial Assumption

- TTP (temporarily) available for bootstrapping
- The initial identity domain is Sybil-free



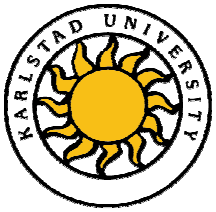
Source: Martucci et al. 2008

Assumptions and Construction

- Assumption:
  - Every user U has obtained a (pseudonymous) membership certificate $cert_U$ from TTP. TTP stores pk_U and revocation information under U's identity
  - Each (sub) identity domain, created by a so-called domain controller, has a unique context identifier ctx, which is publicly announced

- Construction
  - Variation of Camenisch et al. periodically spendable e-token*

*Camenisch et al. How to Win the Clone Wars: efficient periodic n-times anonymous authentication. In: ACM CCS 2006



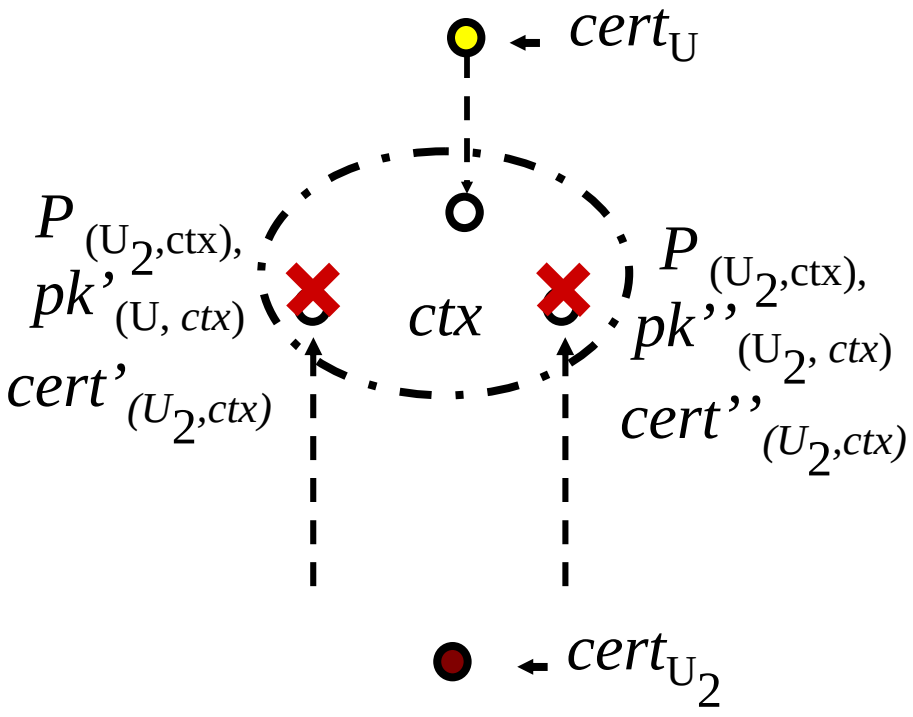
Solution Overview

- For each (sub) identity domain *ctx*, U can create with $cert_U$ one self-certified pseudonym° consisting of:
  - Pseudo-random pseudonym $P_{(U,ctx)}$
  - New public key $pk_{(U,\ ctx)}$
  - Pseudonym certificate $cert_{(u,ctx)}$
- Pseudonyms are mutually unlinkable

Source: Martucci et al. 2008

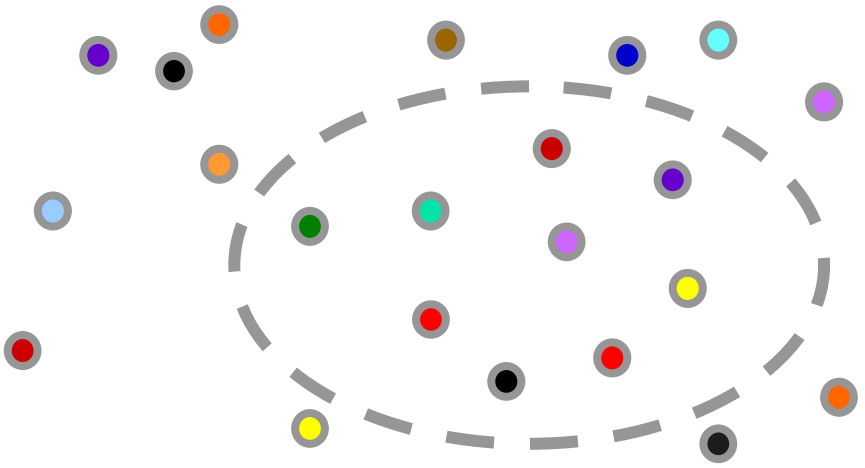
Sybil node detection

- Detection of multiple $P_{(U_2,\, ctx)}$
- obtain the user permanent pk_{U_2}
- $cert_U$ is revoked by TTP



Anonymous Communication Functions

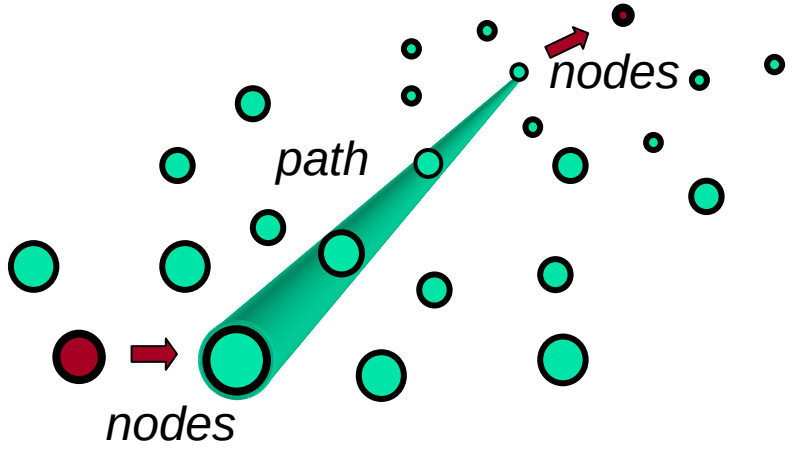
(1) Grouping Function



The anonymity set

How to design privacy-friendly identifiers?

(2) Embedding Function

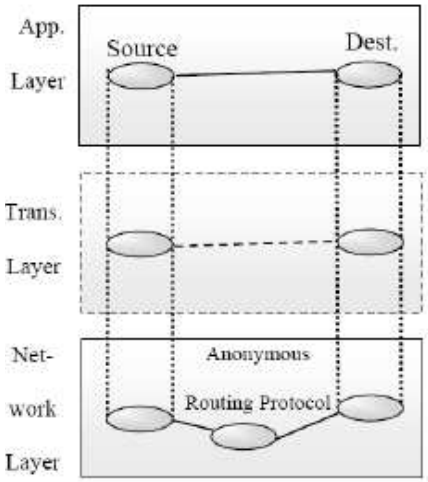


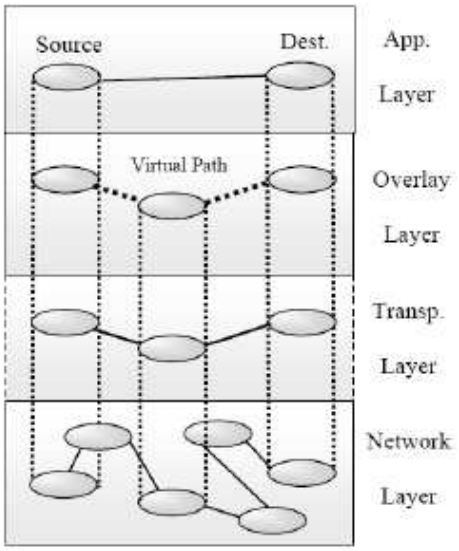
The anonymous path

How to establish an anonymous (virtual) path?

Source: Martucci et al. 2008

Ad (2): Embedding Function

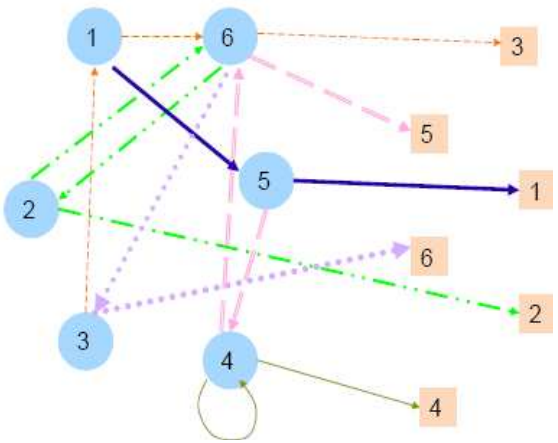




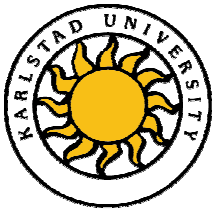
Anonymous Communication in Ad Hoc Networks

- Routing layer
  - + transparency towards application
  - - incompatibility with standard ad hoc routing
- Overlay applications
  - + independency from routing layer
  - - not transparent to applications

The Chameleon Protocol – Mobile Ad Hoc Crowds



- Low-latency overlay anonymous communication mechanism, inspired by the Crowds protocol [Reiter/Rubin]
- Anonymous virtual path establishment:
  - Every node selects its next hop
  - First, path initiator forwards message to arbitrary Chameleon member
  - Further forwarding is determined by a toss of a biased coin (with pf >0.5)
- Multiple directory servers instead of one centralized "blender"
- Self-certified Sybil-free pseudonyms to distinct the elements of the anonymity set

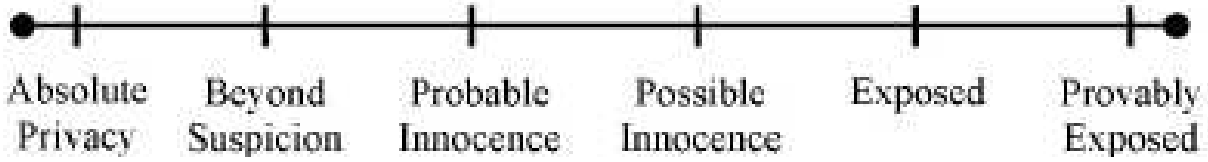


Propagating self-certified, unlinkable Sybil-free identifiers

- Chameleon users have to obtain membership certificate $cert_U$ from a (temporarily available) TTP
- One user acts as the domain controller, to which Chameleon users may register
- The domain controller periodically broadcasts the certified pseudonyms of enrolled users (incl. temporal network addresses)
- Users check that other users possess valid certified pseudonyms
- Pseudonym certificates stored at the domain controller automatically become invalid after the validity period of *ctx*

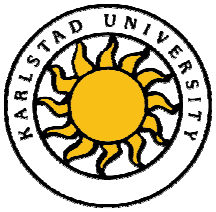
Chameleon - Anonymity Analysis

- Applying the Crowds metrics



- Attacker Model adjusted to ad-hoc networks

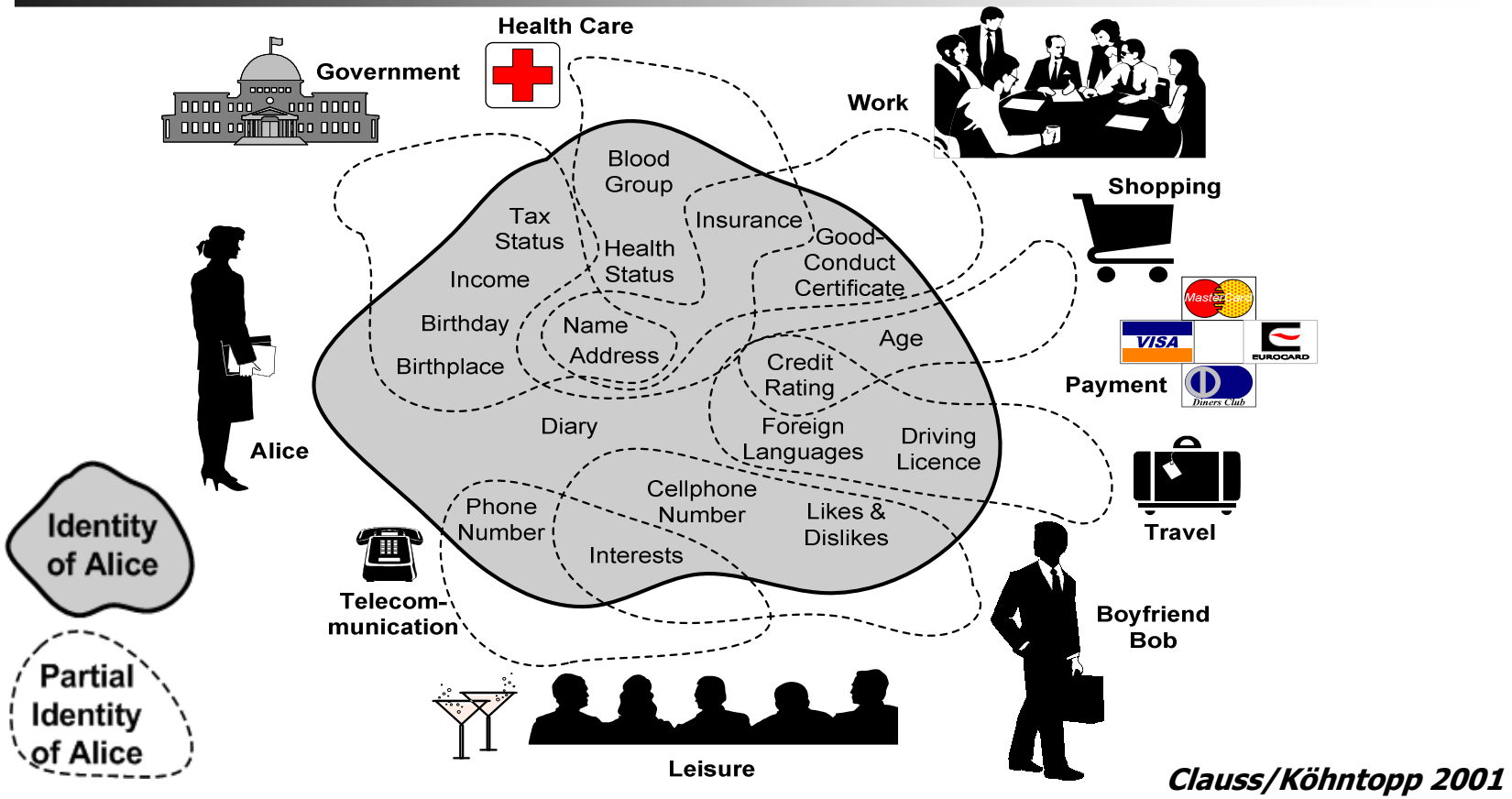
	Sender Anonymity	*Receiver Anonymity*
Malicious insiders (Γ')	probable innocence if $\lvert\Gamma\rvert \geq \frac{p_f}{(p_f-\frac{1}{2})} * (\lvert\Gamma'\rvert+1)$	P(absolute privacy) = $\left(\frac{\lvert\Gamma\rvert-\lvert\Gamma'\rvert}{\lvert\Gamma\rvert}\right)^{L_{exp}-1}$
Destination	beyond suspicion for $\lvert\Gamma\rvert \geq 3$	–



Chameleon - Performance Evaluation and Trade-offs

- Analytical Performance Properties
  - fair distribution of workload
  - scalability (same as Crowds)
  - few public key operations to set a path (2L)
- Simulation to obtain a cumulative distribution function (CDF) of percentage of packet arrivals in relation to the end-to-end delay and resistance against malicious insiders [Martucci 2009]
  - Example: For a tolerated 16.7% of malicious insiders (a probability of forwarding of 0.60):
    - the average end-to-end delay is 5.35 ms
    - 93.8% of the packets are expected to arrive within 10ms and
    - 99,7% within 20ms in our simulation setting

III. Privacy-enhancing Identity Management (IDM) for Life



Vision: Users can act *securely* in the Information Society while keeping *sovereignty* of their private spheres

Viability of privacy-enhancing IDM has been demonstrated

Integrated approach providing:

- Data Minimisation
  - Anonymous communication, anonymous credentials, privacy-enabling authorisation model
- Assurance & Life Cycle Management
  - Assurance control, privacy & trust policy negotiation & enforcement (sticky policies), obligation management
- Transparency
  - Data track,...

PRIME
Privacy and Identity Management for Europe

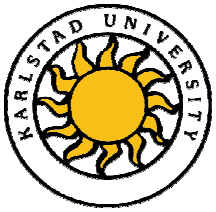
http://www.prime-project.eu/

PRIME/PrimeLife Architecture – Key Elements

1 Data Minimisation

2 Assurances & Data Life Cycle Management

The following slides were kindly provided by Dieter Sommer/IBM Research



1 Data Minimisation

How service providers can authorise users while users retain their privacy

Traditional Model

Request of service

Please log in!

Username = jane.doe

Password

Ok, the requestor is Jane Doe
Address = Paradeplatz, 8001 Zurich, Switzerland
Birth date = 01 June 1979
Email = Jane.doe@mail.provider-xyz.com
Credit card details = (VISA, 1234 5678 9012, …)
And so on…

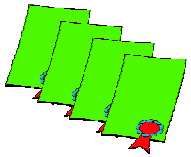
Other profiling data: Detailed interest profiles, browsing behavior, detailed mouse movement profiles, complete history of interactions over the last 3 years, derived data and much more

External linkable data: Potentially everything that is linkable to Jane Doe's identity

PRIME/PrimeLife Model

PRIME Console

PRIME Middleware

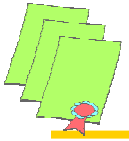


Request of service

Please provide us with either of the following
- Your pseudonym with us
- A valid service subscription
- A valid service subscription and

Pseudonym = X768932…86
Proof = 5634..u758

Statement = Subscription.Type
Proof = 7862…8970



Statement = Subscription.Type
Proof = 7658…5634

Ok, the … **X768932…86**

Ok, the … has a **valid** …

Ok, the requestor has a **valid subscription**. That means, she has paid for the service and can access it.

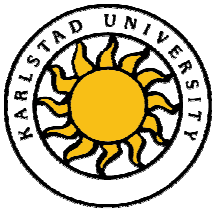
The requestor has provided relevant certified attributes to enable service customization.

In between the extremes!

Data minimisation

isn’t the answer to everything

[there are many scenarios where identifying data are just required]



2 Assurances & Data Life Cycle Management

How users establish trust in service providers and
how service providers enforce their promises for data handling

raditional Model

Well, I don't know anything about this service provider…

There's not much choice than just providing the data…

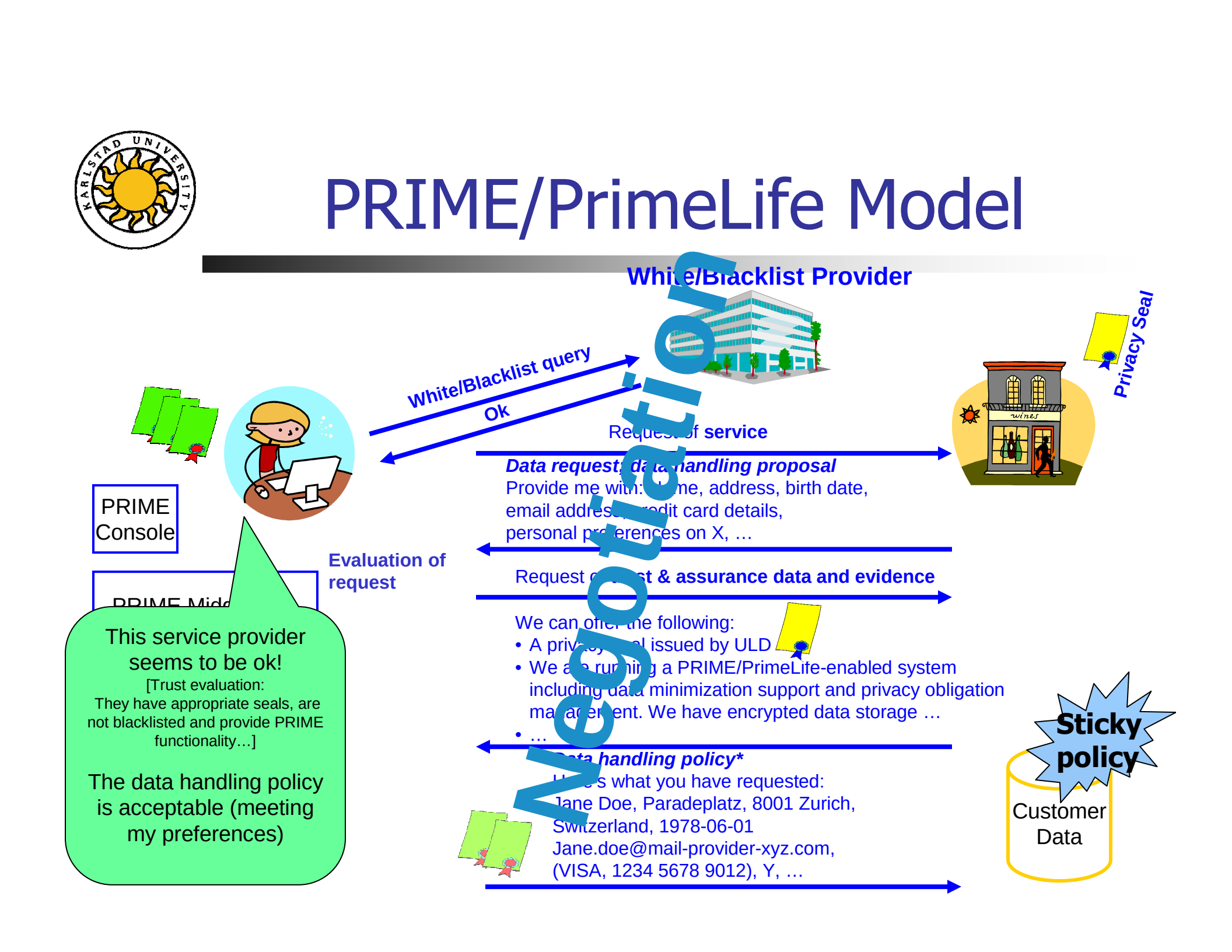
Let's hope that these are not those bad privacy-infringing guys one reads about in the news every other day…

reate an account

Please provide
Name, street, zip code & city, country,
birth date, email address, credit card
details, personal preferences on X, …

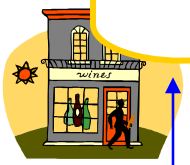
Here's what you have requested:
Jane Doe, Paradeplatz, 8001 Zurich, Switzerland, 1978-06-01
Jane.doe@mail-provider-xyz.com, VISA, 1234 5678 9012, …

PRIME/PrimeLife Model



Privacy Obligation Management

Notification on policy enforcement



Customer Profiles

Profile of **Jane Doe**
Address = Paradeplatz, 8001 Zurich, Switzerland
Birth date = 01 June 1979
Email = Jane.doe@mail-provider-xyz.com
Credit card details = (VISA, 1234 5678 9012, …)
And so on…

Other profiling data: Detailed interest profiles, browsing behavior, detailed mouse movement profiles, complete history of interactions over the last 3 years, derived data *and much more*

External linkable data: Potentially everything that is linkable to Jane Doe's identity

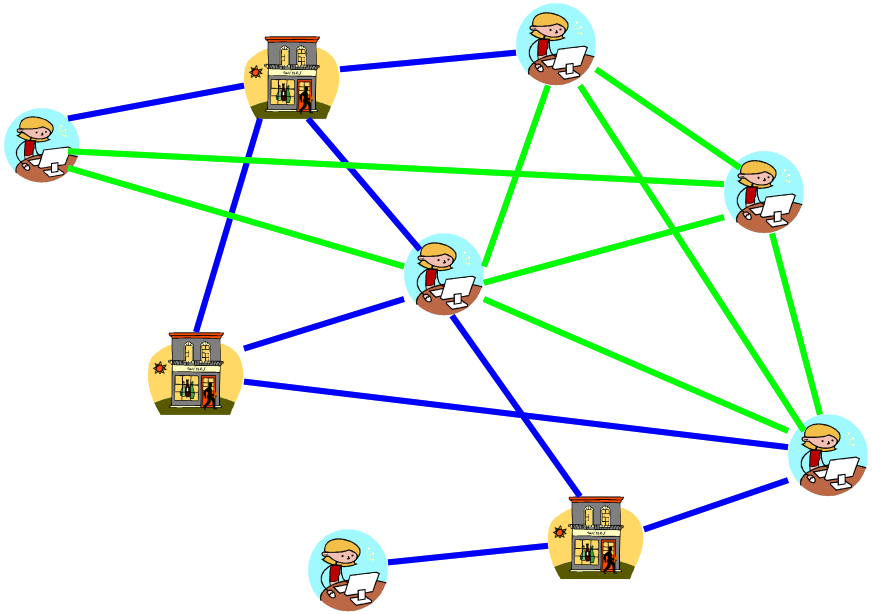
Delete,
Anonymise,
Aggregate …

Obligation Management System (OMS)

Workflow Plugin

User-to-server interactions

[discussed so far]



What about user-to-user interactions?

PRIME architecture is symmetric!

Open and expressive RDF-based data model

Technologies apply similarly

Humans on both sides of the negotiation

PrimeLife

http://www.primelife.eu/

Start date: 01 March 2008, **Duration**: 36 Months, **Total EC Funding**: 10.200,000 €

- Bringing Sustainable Privacy and Identity Management to Future Networks and Services
  - Fundamentally understanding privacy-enhancing identity management 'for life'
  - Bringing Privacy to the future web/social networks
  - Research on Policies, HCI, Infrastructures
- Beyond data minimization:
  - Address data-intensive scenarios and user-generated content (Web 2.0, virtual communities such as Friendster, SecondLife)
- Make privacy-enhancing identity management widely available:
  - Infrastructures, Open Source, and Standards
  - Cooperation with other Projects (Master, TAS3, SWIFT,...),
  - Education (summer schools, …)

SEVENTH FRAMEWORK PROGRAMME

KATHOLIEKE UNIVERSITEIT LEUVEN

JOHANN WOLFGANG GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Microsoft Innovation Center Europe

IBM

CURE

W3C®

SAP®

HCI Challenges addresed by PrimeLife

- User-friendly representation of complex technical privacy concepts
  - Unlinkability, pseudonymity, privacy policy management, anonymous credential selection,…
- Mapping legal privacy requirements
  - Informed consent, transparency,…
- Mapping social requirements
  - Mediating trust, raising awareness,…
- Providing security
  - Against phishing, spoofing,…

Conclusions

- Identity-Anonymity Paradox: Reliable Identifiers ⇨ Anonymity
- Anonymity ⇨ Privacy-enhancing Identity Management
- Holistic Approach to PETs is needed!

Questions ?

http://www.cs.kau.se/~simone/