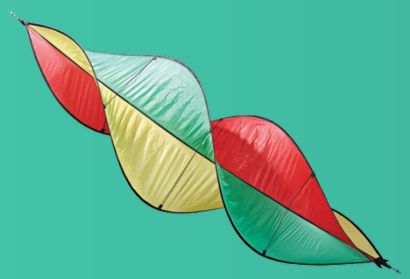
KU LEUVEN

TECHNOLOGIECAMPUS GENT



Inspecting Privacy in Electronic Services

Koen Decroix - Mobile and Secure

April 2015

Outline

- Introduction
- Methodologies
- Approach
- Privacy Modeling Concepts
- A Logic Based Modeling Framework for Analyzing Privacy
- Conclusions
- Questions

KU LEUVEN

Introduction

Complex Electronic Services

KU LEUVEN

Ever wondered what companies know about you?

KU LEUVEN

… Max Schrems, an Austrian student, did!

Now he sues Facebook for their data practices on the personal data they collected about him.

KU LEUVEN

A popular game platform from the late 70’s until the early 90’s

KU LEUVEN

… evolved to multi-service platforms offering social gaming experience

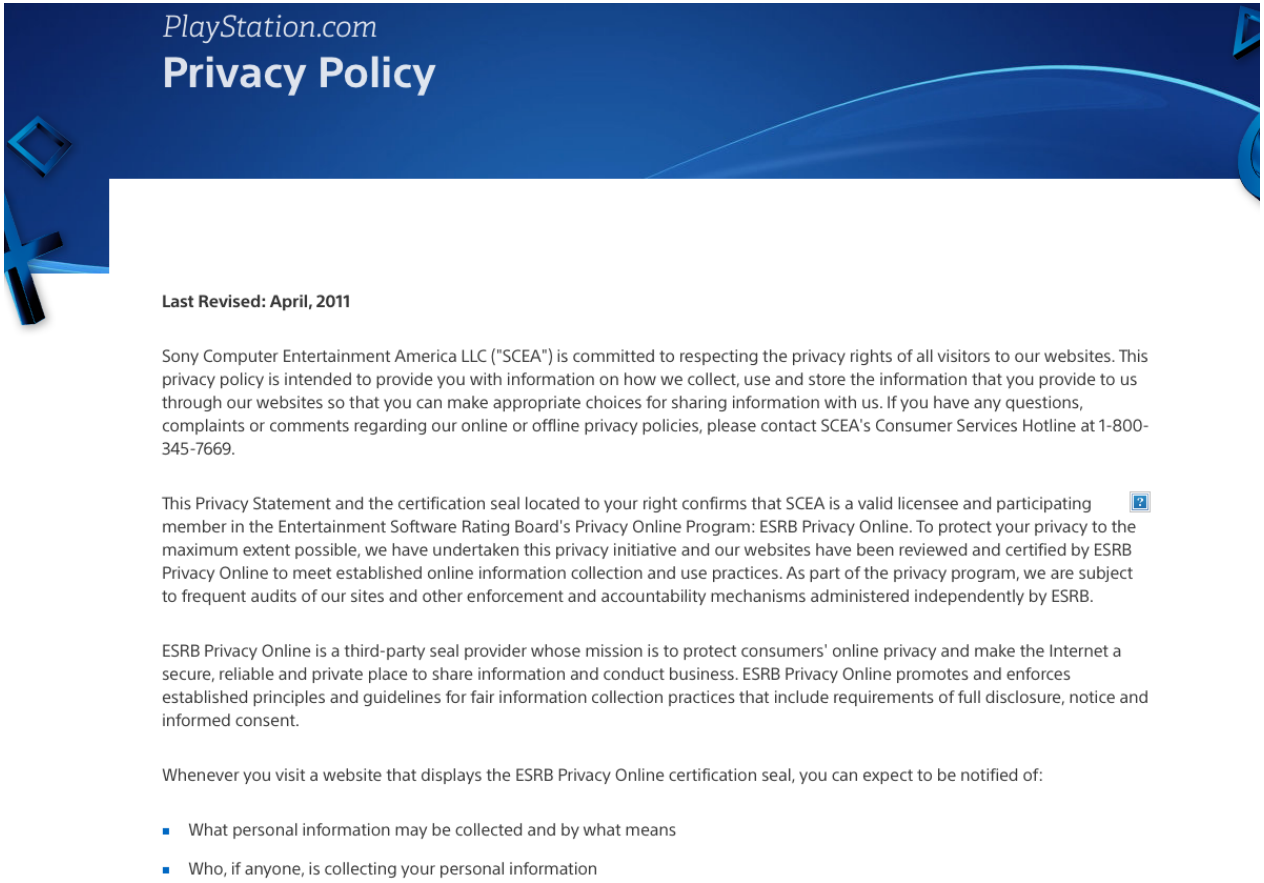
SHARE Epic Moments

Show Off Your Greatness

Why keep your successes to yourself? Immortalise your favourite gaming triumphs and share them with your friends instantly at the tap of a button.

amazon
NETFLIX
hulu PLUS
NBA GAME TIME
IGN
MLB.TV PREMIUM

KU LEUVEN



PlayStation.com

Privacy Policy

Last Revised: April, 2011

Sony Computer Entertainment America LLC ("SCEA") is committed to respecting the privacy rights of all visitors to our websites. This privacy policy is intended to provide you with information on how we collect, use and store the information that you provide to us through our websites so that you can make appropriate choices for sharing information with us. If you have any questions, complaints or comments regarding our online or offline privacy policies, please contact SCEA's Consumer Services Hotline at 1-800-345-7669.

This Privacy Statement and the certification seal located to your right confirms that SCEA is a valid licensee and participating member in the Entertainment Software Rating Board's Privacy Online Program: ESRB Privacy Online. To protect your privacy to the maximum extent possible, we have undertaken this privacy initiative and our websites have been reviewed and certified by ESRB Privacy Online to meet established online information collection and use practices. As part of the privacy program, we are subject to frequent audits of our sites and other enforcement and accountability mechanisms administered independently by ESRB.

ESRB Privacy Online is a third-party seal provider whose mission is to protect consumers' online privacy and make the Internet a secure, reliable and private place to share information and conduct business. ESRB Privacy Online promotes and enforces established principles and guidelines for fair information collection practices that include requirements of full disclosure, notice and informed consent.

Whenever you visit a website that displays the ESRB Privacy Online certification seal, you can expect to be notified of:

- What personal information may be collected and by what means
- Who, if anyone, is collecting your personal information

When registering to a service, you **agree** with the service provider's terms and policies and give him your **explicit consent** for collecting, processing, and forwarding your personal information to collaborating third-parties.

KU LEUVEN

… Non-transparent data handling practice declarations

Who is “who”?

WHO WE SHARE WITH:
We may share the personally identifying information of our website users with our affiliates in the Sony group family of companies and other third parties who assist us with fulfilling your requests, clear and verify transactions, deliver and administer products, content or services, manage and enhance customer data, store and maintain our database records, provide customer service, detect fraud or illegal activities, conduct customer research and surveys, develop new products and services and sell products and services to you.

… and what is “who” doing with your data ?

We do not control our affiliates’ or third parties’ use of your information after we share it, but we use reasonable efforts to obtain our affiliates’ and third parties’ agreement to protect the confidentiality, security, and integrity of any personal information we share with them or that we permit them to collect directly. If consumers do not want their personal information made available to others in these ways, they should not provide their personal information to us.

KU LEUVEN

… but do you realize what is declared?

… and what the consequences are concerning your privacy?

KU LEUVEN

Many people do not !

KU LEUVEN

The upcoming EU General Data Protection Regulation protects the privacy of EU citizens by means of different data protection principles.

KU LEUVEN

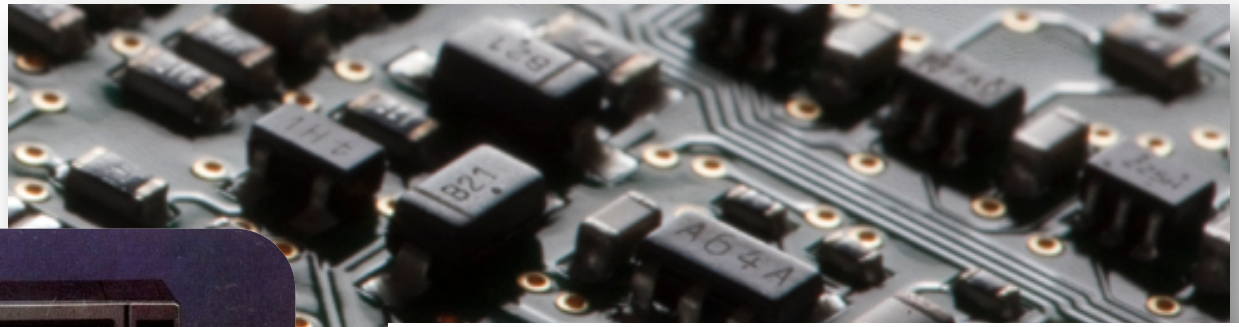
Privacy is not a mere afterthought, but privacy safeguards must be built into all steps of the design process from the earliest design stage, i.e. **privacy by design**

KU LEUVEN

Obligation of data controllers to comply with regulations and to demonstrate this compliance and to implement mechanisms that ensure this compliance, i.e. **service provider accountability**

KU LEUVEN

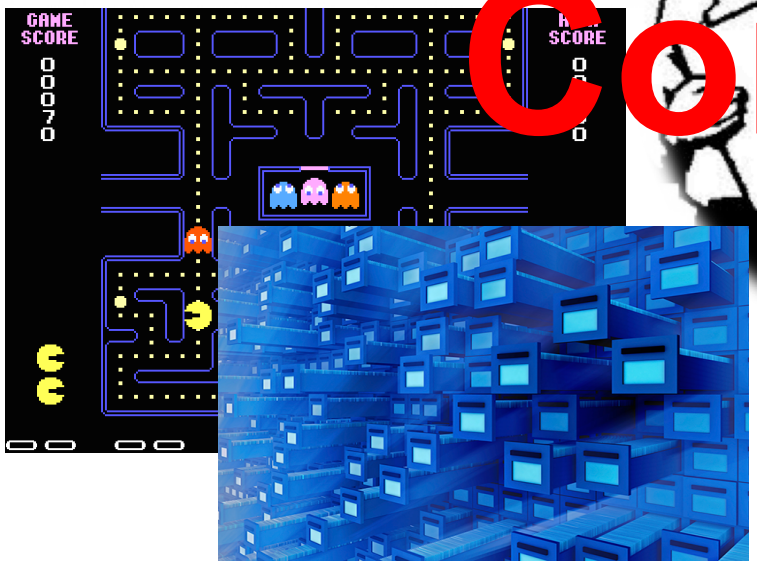
In the past, only functionality had to be considered during game development. Developers were able to handle this.




```
00000000  push    ebp
00000001  mov     ebp, esp
00000003  movzx   ecx, [ebp+arg_0]
00000007  pop     ebp
00000008  movzx   dx, cl
0000000C  lea     eax, [edx+edx]
0000000F  add     eax, edx
00000011  shl     eax, 2
00000014  add     eax, edx
00000016  shr     eax, 8
00000019  sub     cl, al
0000001B  shr     cl, 1
0000001D  add     al, cl
0000001F  shr     al, 5
00000022  movzx   eax, al
00000025  retn
```

KU LEUVEN

Today, system design is multi-disciplinary and requires expert-knowledge



Complex

KU LEUVEN

Need for computer-aided tools supporting the design of complex services.

KU LEUVEN

Methodologies

A State-of-the-Art of Privacy Modeling Approaches

KU LEUVEN

Privacy Requirement Engineering – identifying privacy requirements

- Threat models
  - STRIDE/DREAD (Microsoft) – Data flow diagram
  - CORAS
- Misuse cases – use cases
- Attack trees
- Problem frames

Quantitative approaches: metrics → measuring degree of anonymity

- Anonymity networks
  - Anonymity sets
  - Information theoretic approaches – entropy based
- Databases
  - *k*-anonymity → *l*-anonymity → *t*-closeness
- Statistical databases:
  - Differential privacy→ focus on used query algorithm

Quantitative Approaches

- ***Policy-agnostic programming:*** verification of program code compliance with privacy policies
  - ➢ E.g. Jeeves, Hoare logic
- ***Logic based modeling approaches:***
  - Conflict detection between privacy policies of entities in multi-tier systems
    - ➢ E.g. Facebook apps
  - Conflict detection between privacy policies and privacy regulatory frameworks
  - Protocol verification
  - **Reasoning on impact of architectural design decisions**
  - **Privacy analysis at application level**
  - Compliance verification of high-level architectural privacy requirements with underlying privacy properties of used protocols.
- ***Markov chains:***
  - Verification if data collection serves certain goals
- ***Process Algebras:*** Applied π-calculus - ProVerif
  - Automated privacy analysis for protocols based on PETs
    - ➢ E.g. e-voting system, e-auction system, electrical vehicle charging
- ***Multi-paradigm:***
  - Designing controlled anonymous applications using ABCs.

Approach

A Logic Based Privacy Modeling Appraoch

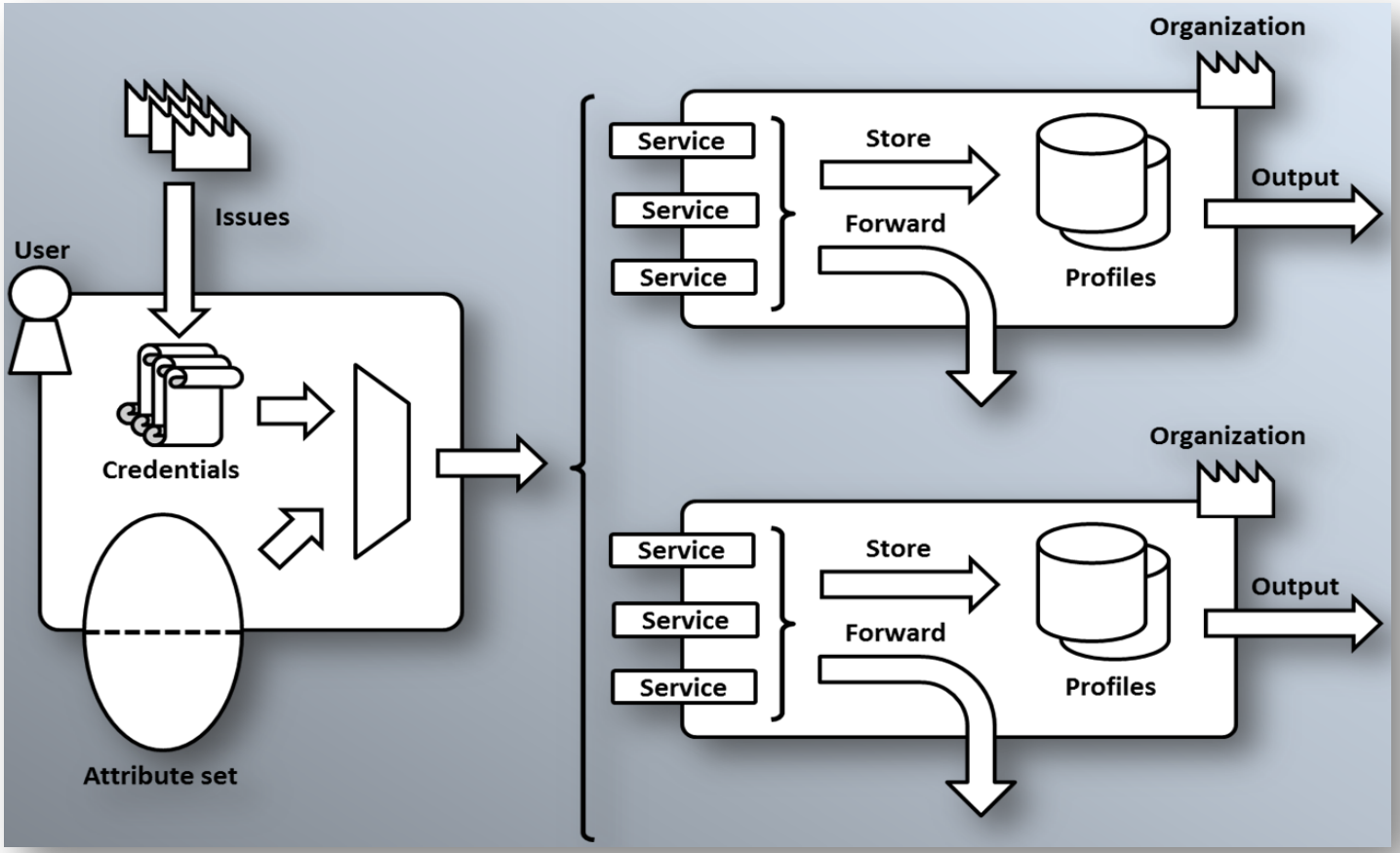
KU LEUVEN

A logic based modeling approach is used for the privacy analysis based on **user profiles** built from formal models representing the service under consideration. The feedback must be useful for **system designers** and **end-users** as well.

KU LEUVEN

Privacy Modeling Concepts

KU LEUVEN



Conceptual model of a composite service

KU LEUVEN

Modeling properties of authentication technologies

X.509 Certificates

Calypso cards

Idemix

U-Prove

E.g. access to a service is only permitted if individual is older than 18y

Revealed attributes:
DoB, First name, Surname, SSN, Address, Gender, Card SN, …

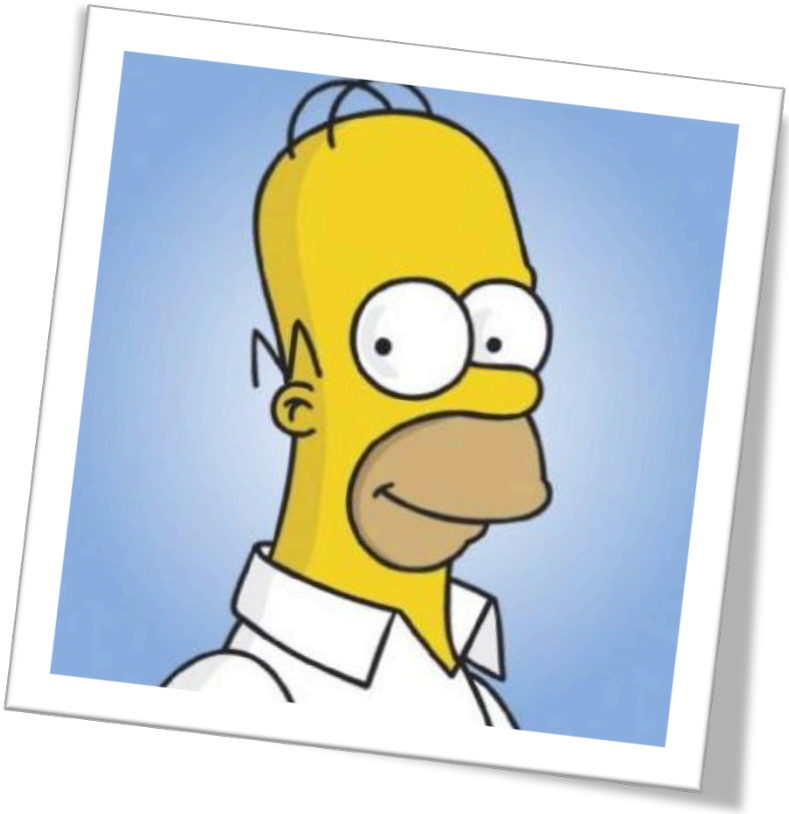
Idemix

U-Prove

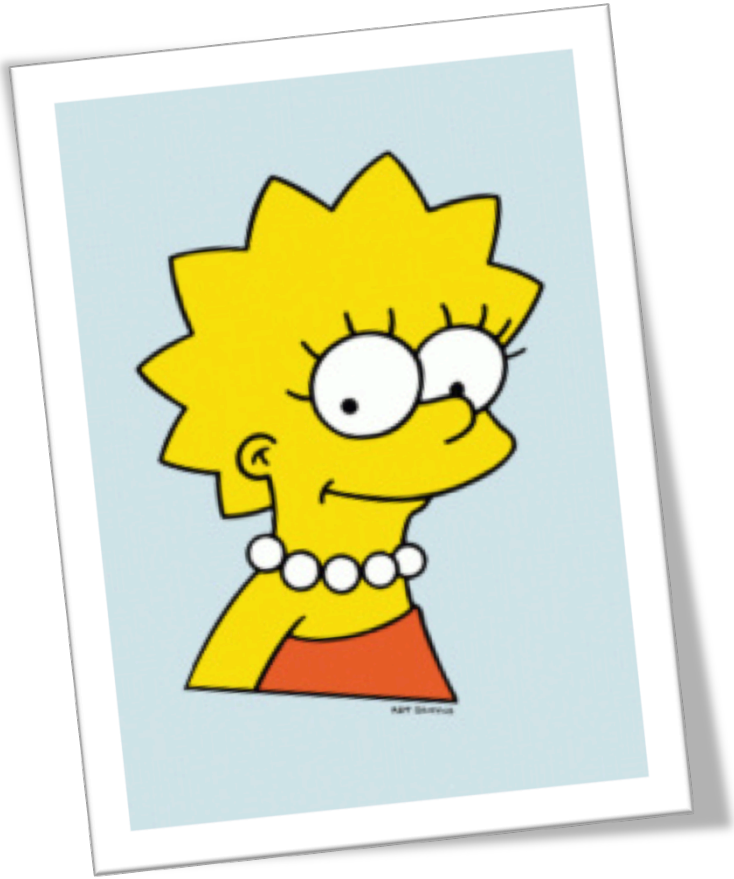
Revealed attributes:
e.g. DoB
e.g. Age > 18
e.g. 20 < Age < 25

KU LEUVEN

Different types of users → Different trust perceptions

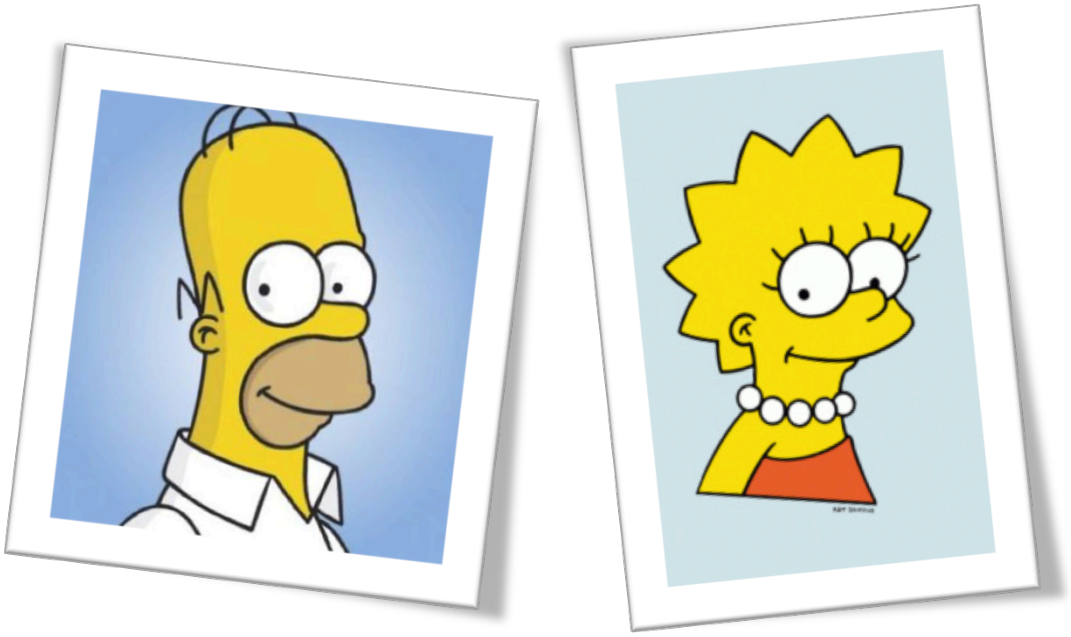


He just don’t care about his privacy, he trusts everybody



She cares about her privacy, only trusts companies with a good reputation

KU LEUVEN



Trust perceptions are modeled in terms of storage and data forwarding (i.e. distribution)

An organization part of the **set of storage/distribution trusted organizations**, only stores/forwards the attributes that are declared in storage/distribution policy, else the organization is supposed to store/ distribute all attributes it can collect.

KU LEUVEN

Modeling identifiers linkable to an individual

Pseudonymous: group of attributes referring to individual without actual revealing his identity

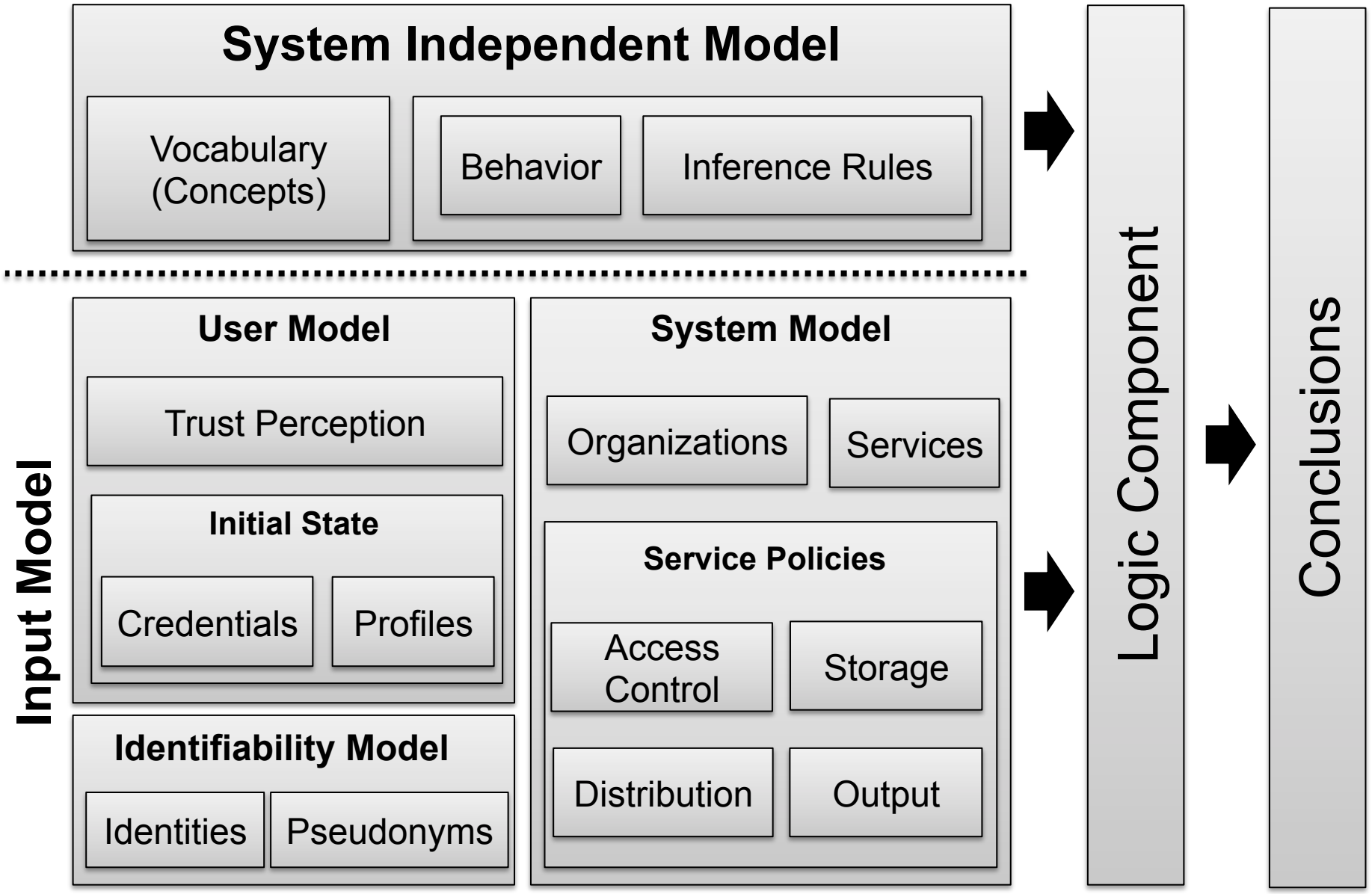
- e.g. e-mail address
- e.g. username,
- e.g. browser fingerprint, i.e. a unique combination of attributes representing browser configuration

Identity: group of attributes *sufficiently* revealing identity of an individual

- e.g. first name, surname and address (in case of Homer)
- e.g. first name, surname (in case of Lisa)

A Logic Based Modeling Framework for Analyzing Privacy

KU LEUVEN


System Independent Model
Vocabulary (Concepts)
Behavior
Inference Rules
Input Model
User Model
Trust Perception
Initial State
Credentials
Profiles
Identifiability Model
Identities
Pseudonyms
System Model
Organizations
Services
Service Policies
Access Control
Storage
Distribution
Output
Logic Component
Conclusions

Logic Component

Properties

- Declarative logic programming system
- Knowledge base system
- Intuitive modeling using predicate logic
- IDP language: FO logic enriched with types, aggregate, inductive definitions, partial functions
- Supports reasoning on incomplete knowledge
- Supports modular programming
- Integrated Lua

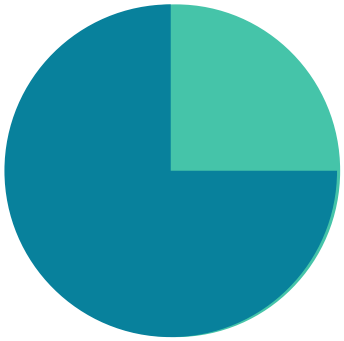
Structure of IDP program

- *Vocabulary*: contains non-logic modeling symbols = types, predicates, functions
- *Theory*: set of constraint rules and definitions
- *Structure over the vocabulary*: a partial valuation of the vocabulary elements that satisfies the theory

Theory:
Generic behavior
Inference

Input model =
partial structure
satisfying theory

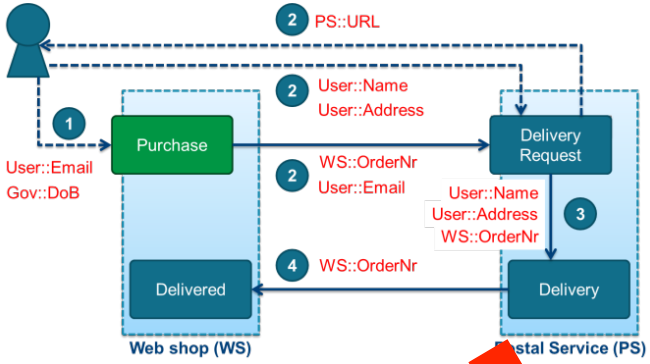
Model expansion
= extending input
model

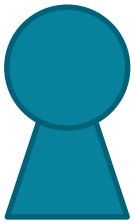


Output model =
complete structure
satisfying theory

KU LEUVEN

Computation of User Profiles

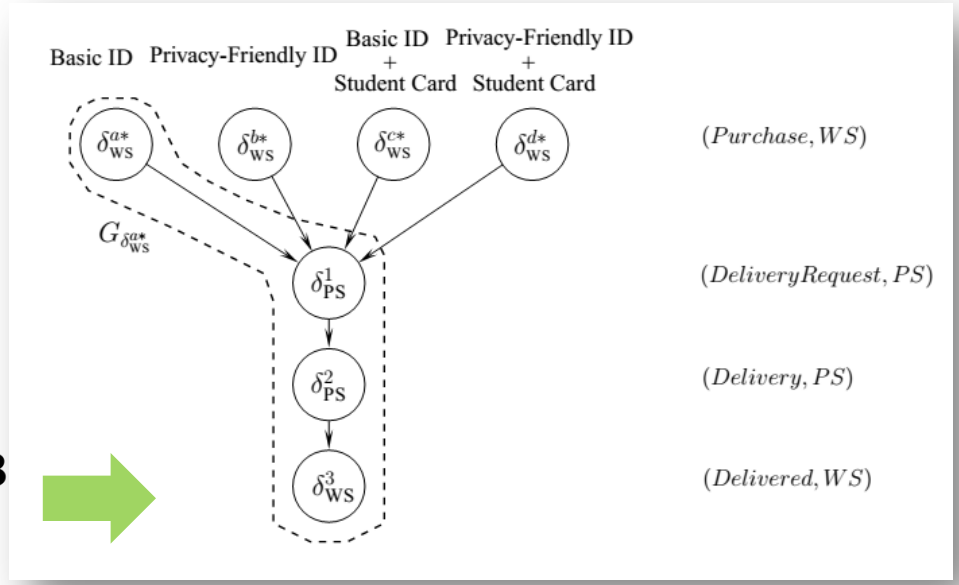




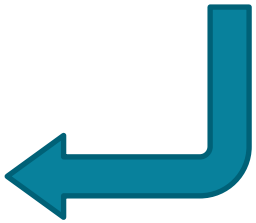
Behavior

Inference Rules

IDP3

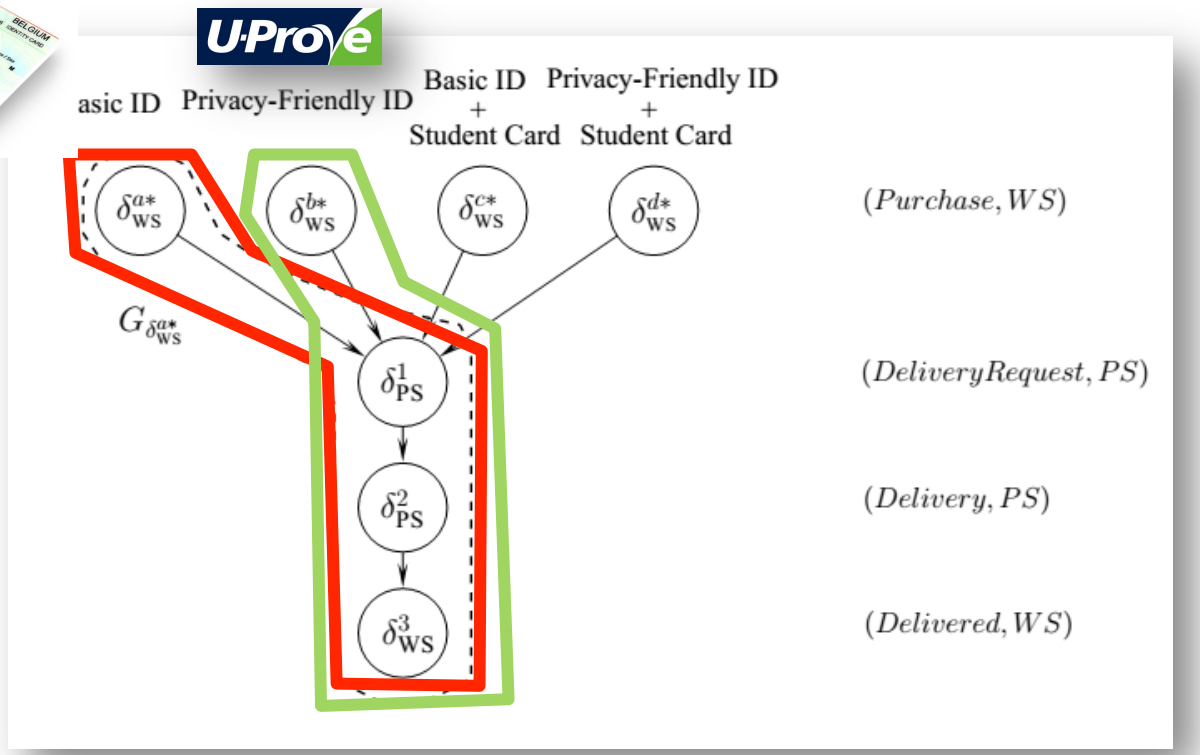


Service Invocation Graph



KU LEUVEN

Service Invocation Graph



Sub-graphs represent invoked services of different alternatives

KU LEUVEN

Feedback that can be derived from user profiles

Query the user's anonymity level:
→ Users is anonymous, pseudonymous, identifiable

Query the attributes released to organizations:
→ Detecting violations: e.g. an organization is not allowed to collect name and address
→ Verify if attributes required for the functionality can be collected by an organization

Query the impact of collaborations between organizations:
→ e.g. can a user be identified when organization x and y collaborate?

Querying the required trust between organizations:
→ e.g. Y receives name and address from X. X collects it from user's X.509 based identity card. Y must only trust the issuer of the identity card.

Conclusions

KU LEUVEN

- A qualitative modeling approach complementary to other approaches such as RE and quantitative approaches.

- Flexible approach → analyze privacy of services from different domains:
  - Travel reservation system
  - Web shop
  - Loyalty Systems
  - Ticketing systems in public transport

- Result are publicly available at: https://github.com/decroik/inspect-privacy-and-trust

- Privacy related feedback useful for designers
  - Impact of design decisions: e.g. using X.509 certificate instead of Anonymous credential (Idemix).
  - Impact of collaborations.
  - Automated conflict detection with privacy preferences of prototypical users.

- Privacy related feedback useful for end-users
  - Anonymity level
  - Conflict detection with personal privacy preferences. E.g. commercial organizations are not permitted to collect my SSN.

- Realization Accountability:
  - https://github.com/inferring-accountability/inferring-accountability

KU LEUVEN

Main Publications

- Decroix, K., Butin, D., Jansen, J., Naessens, V. (2014). Inferring Accountability from Trust Perceptions. In Prakash, A. (Ed.), Shyamasundar, R. (Ed.), *Information Systems Security: Vol. 8880*. ICISS 2014. Hyderabad, 16-20 December 2014 (art.nr. 29) (pp. 69-88) Springer-Verlag.

- Decroix, K., Lapon, J., De Decker, B., Naessens, V. (2013). A Framework for Formal Reasoning about Privacy Properties based on Trust Relationships in Complex Electronic Services. In Bagchi, A. (Ed.), Ray, I. (Ed.), *Information Systems Security: Vol. 8303*. ICISS 2013. Kolkata, 16-20 December 2013 (pp. 106-120). Berlin Heidelberg: Springer-Verlag.

- Decroix, K., Lapon, J., De Decker, B., Naessens, V. (2013). A Formal Approach for Inspecting Privacy and Trust in Advanced Electronic Services. In Jürgens, J. (Ed.), Livshits, B. (Ed.), Scandariato, R. (Ed.), *Engineering Secure Software and Systems: Vol. 7781* (5). ESSoS. Paris, 27 February 2013 - 1 March 2013 (pp. 155-170). Berlin Heidelberg: Springer-Verlag.

KU LEUVEN

Questions

KU LEUVEN