Tools for Ubicomp Privacy

Marc Langheinrich
ETH Zurich

RESEARCH GROUP FOR
Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

What's Up?

- Privacy Enhancing Technologies (PETs)
  - Encryption & Authentication
  - Anonymization & Pseudonymization
  - Access & Control
  - Transparency & Trust
- Legal Aspects
  - US Privacy Landscape
  - European Privacy Laws

Solution Space Revisited

- Notice and Disclosure
  - Transparency Tools
- Choice and Consent
  - Anonymity and Pseudonymity Tools
- Security
  - Encryption and Authentication Tools
- Access and Control
  - PETs in the Enterprise
- Recourse
  - Laws and Regulations

Anonymity & Pseudonymity

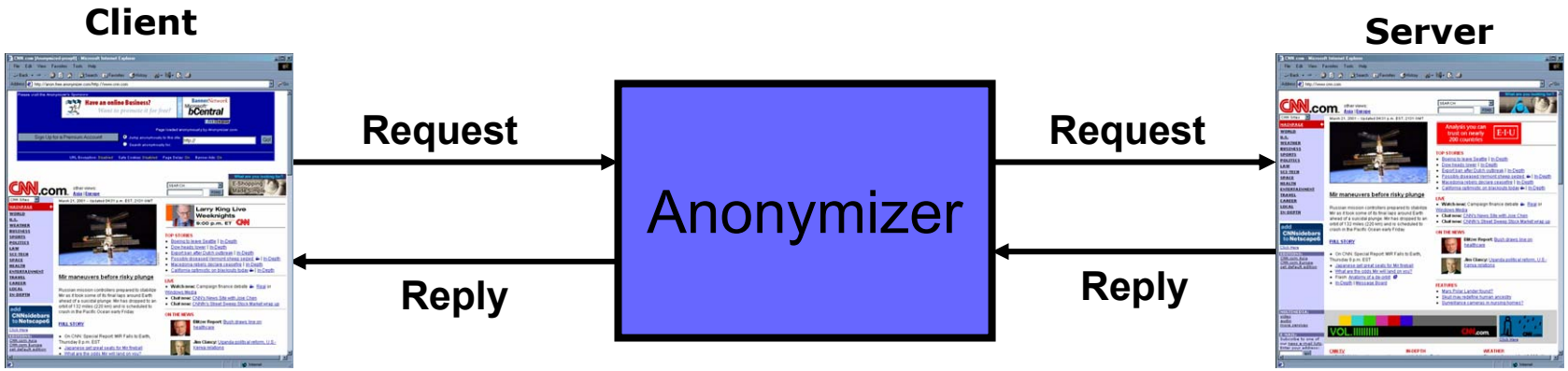
RESEARCH GROUP FOR

Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Anonymizing Proxies

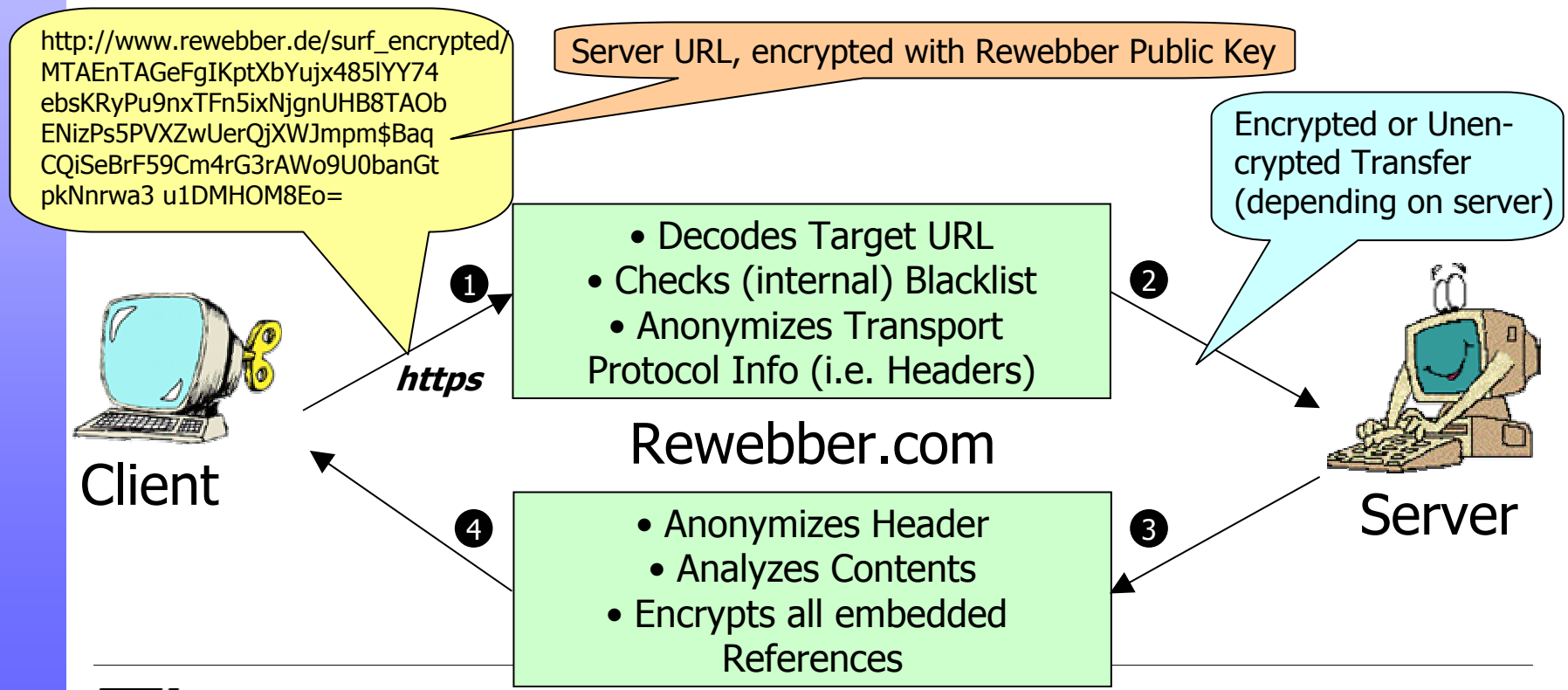
- Acts as a proxy for users
- Hides information from end servers



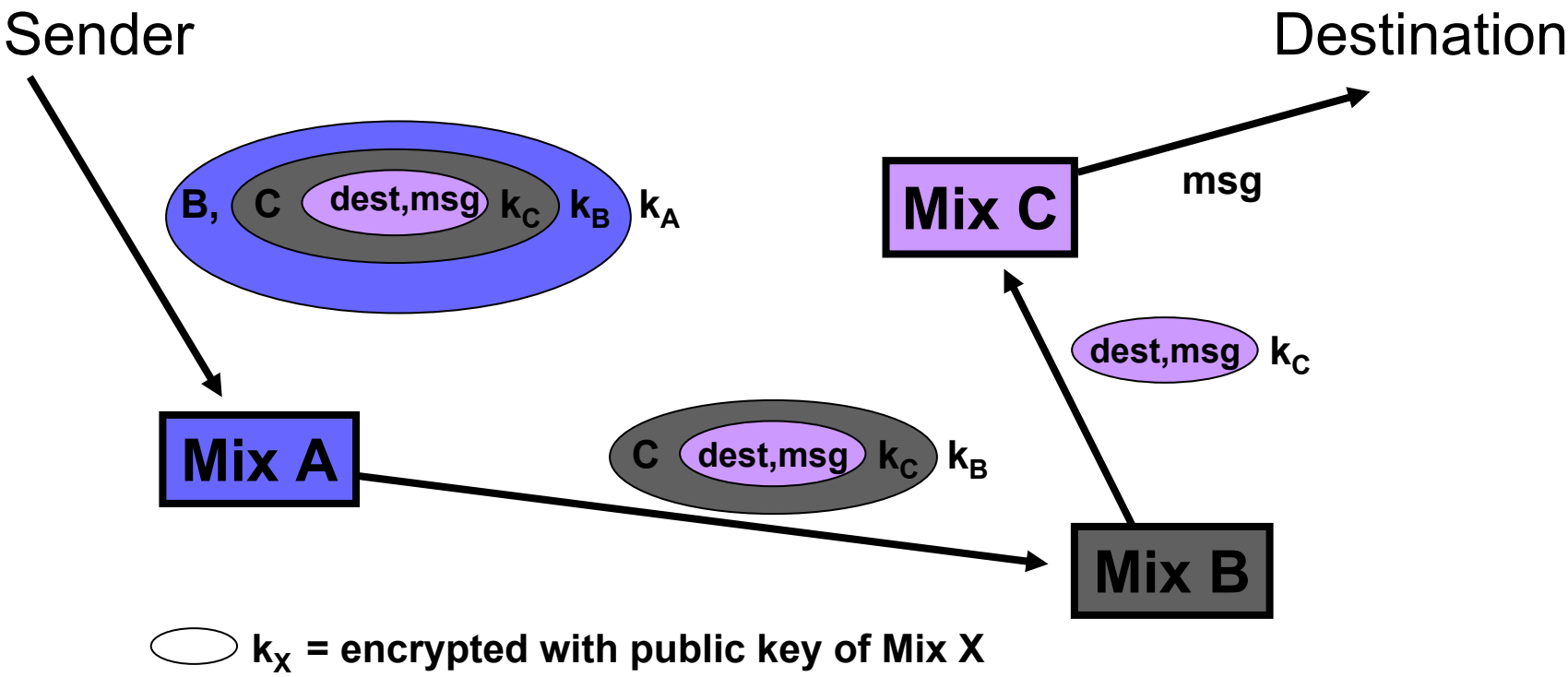
- Proxy Sees all traffic
- User Identity Easily Compromisable
- Note: Server Identity Protectable (Rewebber)

Rewebber.com

- Created at Hagen University, Germany
- Provides both Client- and Server-Anonymity
- Only as subscription service ($5-$15 per month)



Mixes [Chaum81]



Sender routes message randomly through network of "Mixes", using layered public-key encryption.

Realization of Mixes

- Onion Routing (Office of Naval Research)
  - http://www.onion-router.net
  - service ended 01/2000

- Freedom (Zero-Knowledge Systems, Canada)

zerøknowledge

  - http://www.zeroknowledge.com
- Java Anon Proxy (TU Dresden)

  - http://anon.inf.tu-dresden.de

Further Issues

- Mobile IPv4/IPv6 Node Mobility
  - Binding Updates Can be Tracked
  - Unencrypted Home Network Address
  - Integration into Mix Networks necessary
- IPv6 Stateless Address Configuration
  - Address Based on Fixed Interface Identifier
  - Better: Fake Identifiers (Random/Statistical)
- Bluetooth BD_ADDR Problem

IPv6 Privacy See also: Alberto Escudero Pascale, KHT Sweden. http://www.it.kth.se/~aep/

Transparency Tools

RESEARCH GROUP FOR

Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Example: Web Privacy Policies

- Let consumers know about collector's privacy practices
- Consumers can then decide
  - whether or not practices are acceptable
  - when to opt-in or opt-out
  - who to do business with
- Increase consumer trust

Privacy Policy Drawbacks

- BUT policies are often
  - difficult to understand
  - hard to find
  - take a long time to read
    - usually 3-4 pages!
  - changed without notice

Seal Programs

- TRUSTe – http://www.truste.org
- BBBOnline – http://www.bbbonline.org
- CPA WebTrust – http://www.cpawebtrust.org/
- Japanese Privacy Mark http://www.jipdec.or.jp/security/privacy/

Seal Program Problems

- Basic Principle:
  - Publish a policy (*any* policy) and follow it
- Only few require base-level standard
  - BBBOnline requires client in good standing with Better Business Bureau
- Effect:
  - Good notices of bad practices

P3P

- Platform for Privacy Preference Project
  - Chartered by World Wide Web Consortium (W3C)
  - 1997-2001 (Recommendation December 2001)
- A framework for automated privacy discussions
  - Web sites disclose their privacy practices in standard machine-readable formats
  - Web browsers automatically retrieve P3P privacy policies and compare them to users' privacy preferences
  - ~~Sites and browsers can then~~ negotiate ~~about privacy terms~~

P3P1.0 defines

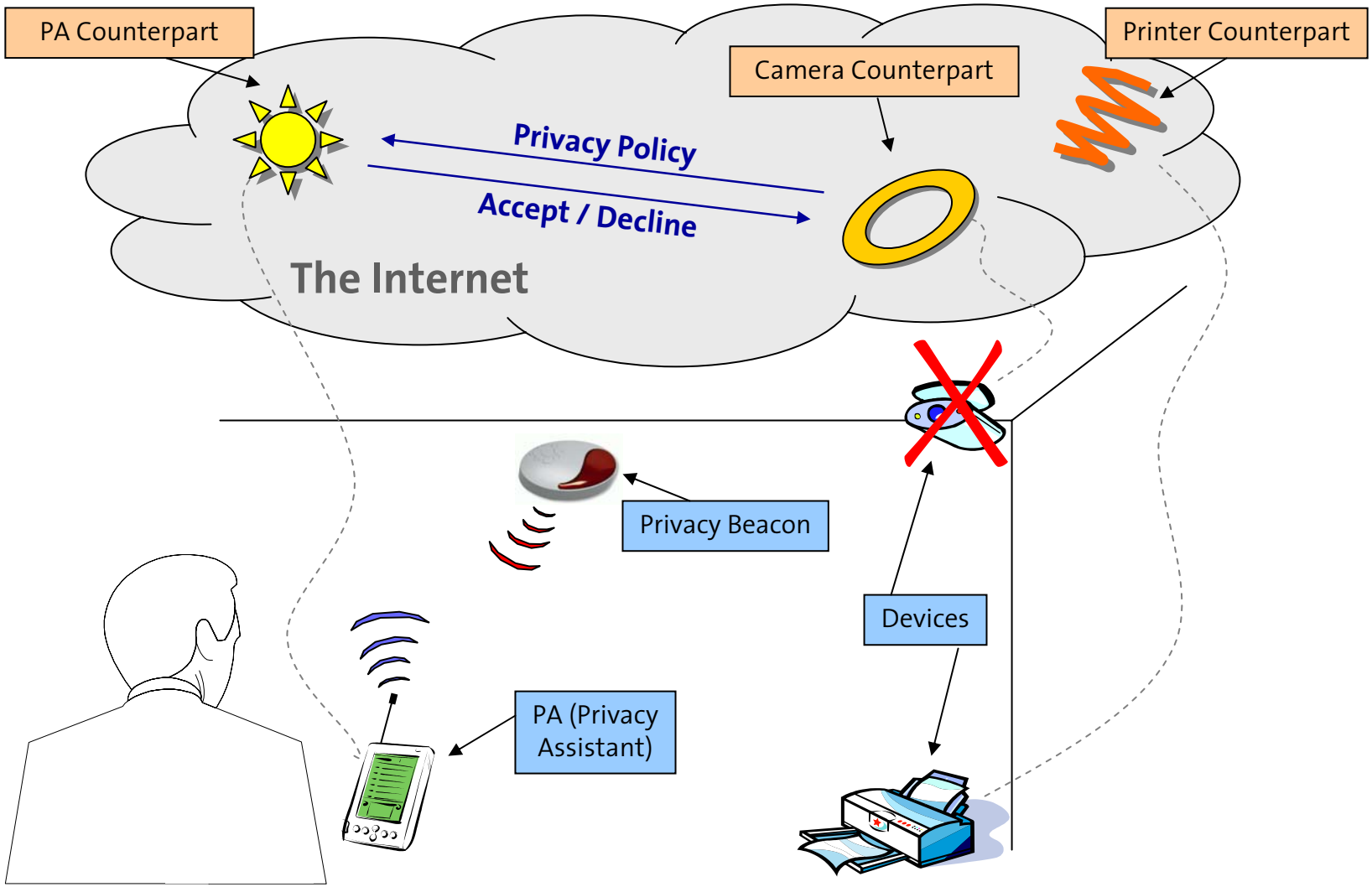
- Data
  - Us
  - All
- Voca
  Colle
  - Pu
- XML
- Meth
- Trans
  - No

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
     <CONSEQUENCE-GROUP>
        <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
      </CONSEQUENCE-GROUP>
     <RECIPIENT><ours/></RECIPIENT>
      <RETENTION><indefinitely/></RETENTION>
     <PURPOSE><custom/><develop/></PURPOSE>
     <DATA-GROUP>
       <DATA name="dynamic.cookies" category="state"/>
       <DATA name="dynamic.miscdata" category="preference"/>
       <DATA name="user.gender"/>
       <DATA name="user.home." optional="yes"/>
     </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
     <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

The P3P Vocabulary

- Who is collecting data?
- What data is collected?
- For what purpose will data be used?
- Is there an ability to change preferences about (opt-in or opt-out) of some data uses?
- Who are the data recipients (anyone beyond the data collector)?
- To what information does the data collector provide access?
- What is the data retention policy?
- How will disputes about the policy be resolved?
- Where is the human-readable privacy policy?

Privacy Infrastructures

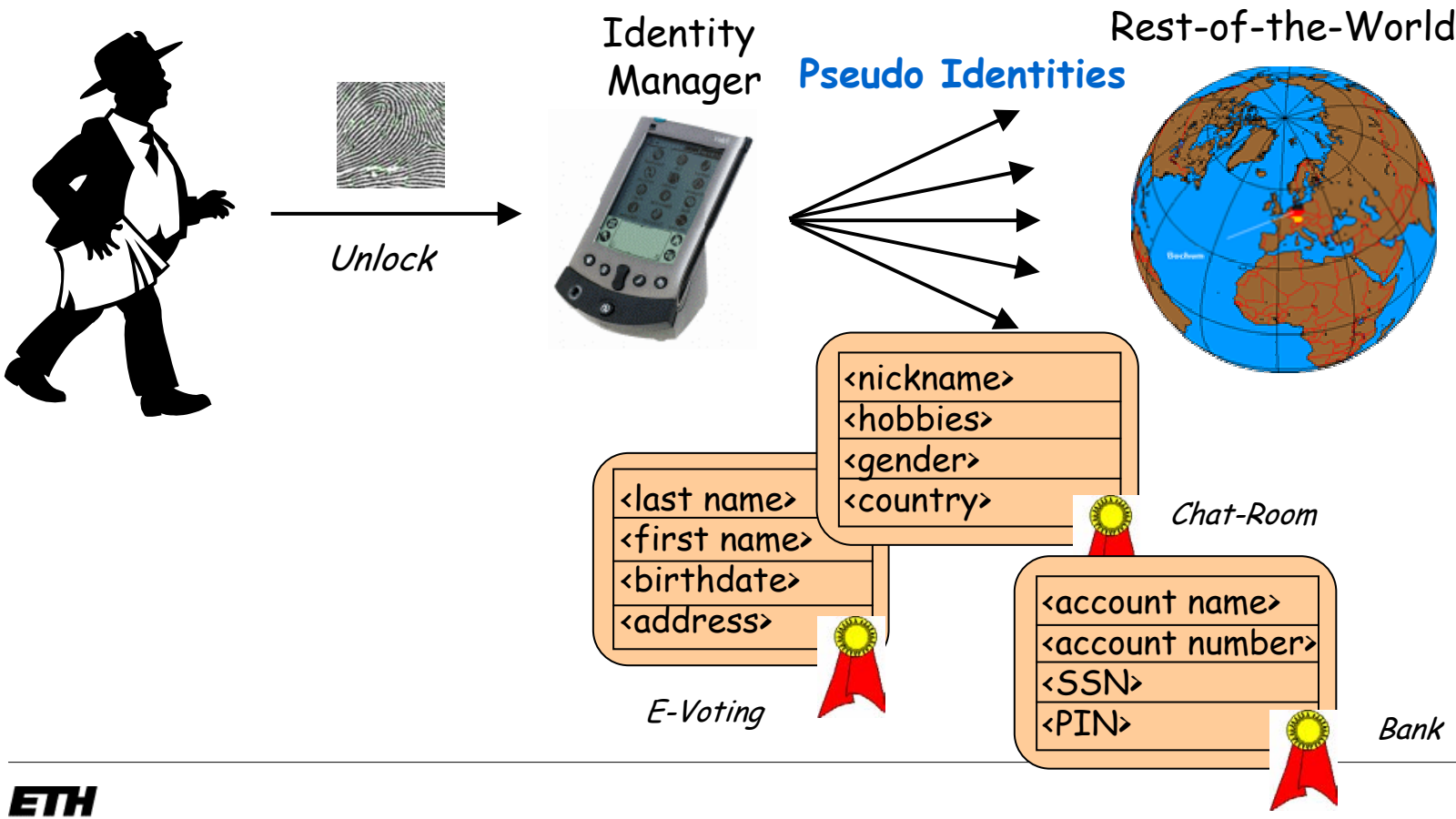


P3P Issues

- Legal Applicability of XML-Policies?
  - Lawyers Do Not Like Binary Stuff
- Expressability of Personal Preferences?
  - Not All Situations Foreseeable and Definable
- User Proficiency?
  - Can the Layman Configure Sufficiently?
- Who Sets the Defaults?
  - Most Users Will Not Bother to Change Prefs
- Promises, Promises, Promises
  - Who Says That Policies Will Be Followed?
- Negotiations?

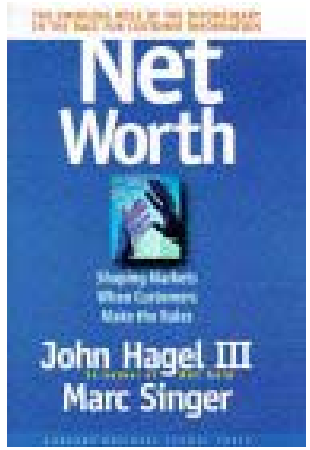
The Identity Protector

- John Borking, 1996 (Dutch Data Protection Comm.)



Infomediaries

- Hagel/Singer: „Net Worth“ 1997



- Services and tools that help people manage their online identities
  - **Digitalme** - http://www.digitalme.com
  - **Lumeria** - http://www.lumeria.com
  - **Privaseek** – http://www.privaseek.com

digitalme

Lumeria Inc.

Persona℠

Identity Managers

- History: Open Profiling Standard (Netscape, 97)
  - Inspired P3P, Local Storage, Soon Abandoned
- XNS.ORG (Open Source by *OneName Inc.*)
  - Implements Subset of P3P + Identity Services
- Microsoft Passport ("My Services")
  - Mounting Criticism Led to Number of Alterations
- Liberty Alliance (Sun, 2001)
  - AmEx, HP, IBM, Nokia, GM, NTT, Philips, Visa, SAP, ...
- IDSec (Open Source, IETF-Draft, 05/2002)

See also: http://weblog.digital-identity.info/

More Identity Managers

- PISA – Privacy Incorporating Software Agent (EU 5th Framework Project)
  - Uses Software Agent Technology
  - Partners: ZeroKnowledge, NRCC, TU Delft, …
  - http://www.tno.nl/instit/fel/pisa/
- Freiburg University Identity Manager
  - Mobile Applications
  - Incorporate with Location Privacy System
  - http://www.iig.uni-freiburg.de/telematik/atus/

Encryption and Authentication

RESEARCH GROUP FOR

Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Confidentiality

- Plenty of Options
  - IPSec, SSH, SSL, SET, PGP, WEP (Flawed)…
- Bulk Traffic Encryption Possible
  - But Power Consumption a Factor
- Most Important Question: Who You Are Talking To?
  - Authentication Primary Concern
  - Difficult Due to Lack of Infrastructure!

Making ”Friends”

- Resurrecting Duckling Model (Stajano)
  - Security Principal Imprinted on “Blank” Unit
  - ”Secure Transient Association:” Deassociation Possible After Imprinting
- Interface Challenge
  - Example: Smart-Its

Image: TecO

Making "Friends"

- The shaking motion establishes a shared context (i.e., acceleration pattern) that no other devices will have

Image: TecO

Access & Control

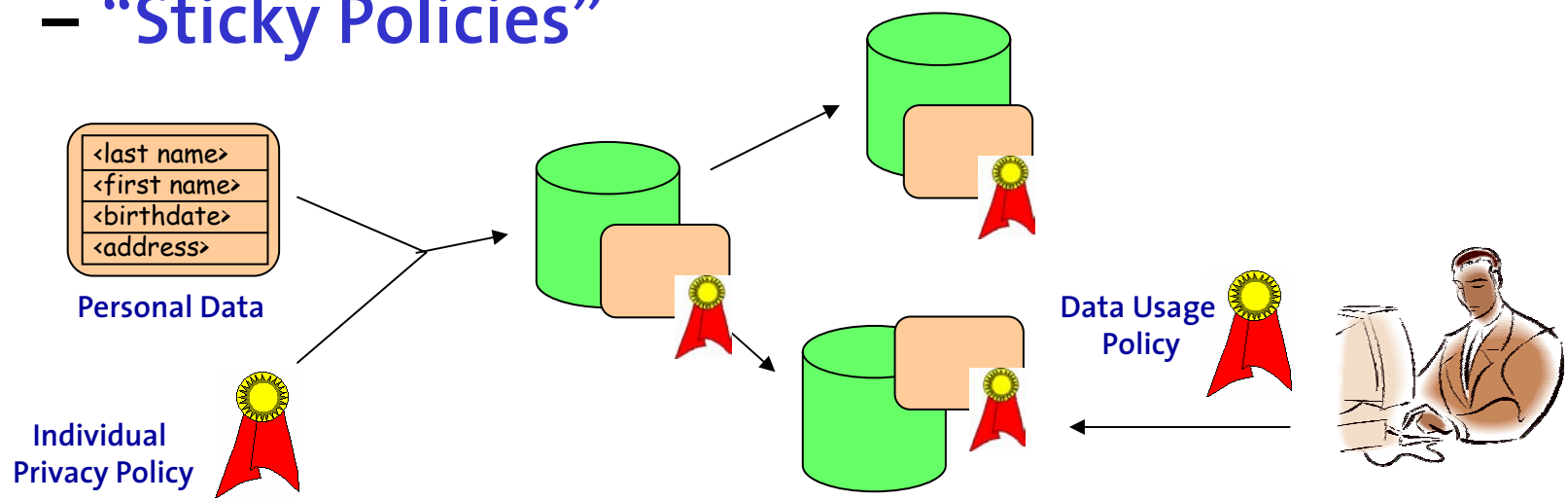
RESEARCH GROUP FOR

Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Keeping Your Promises

- Goal: Data Processing in Synch with Data Collection Policies
  - Enterprise-wide PETs
  - Metadata Controls Back-End Processing
  - "Sticky Policies"



Enterprise PETs

- Advantages
  - Allows Individual Policies
  - Simplifies Data Management (Metadata)
  - Provides Accountability (Privacy Audits)
- Players
  - IBM (e.g., pASL, Zurich Research Labs)
  - PricewaterhouseCoopers (Consulting)
  - NCR Teradata (Warehousing Software)

More PET Issues

- Digital Watermarking
  - Protecting Personal Information with Digital Copyright Protection?
- Individual Access
  - Authenticating Users to Edit Personal Data
  - Costs?
- Negotiation
  - How Much Do We Need?
- …

Solution Space Revisited

- Notice and Disclosure
  - Transparency Tools
- Choice and Consent
  - Anonymity and Pseudonymity Tools
- Security
  - Encryption and Authentication Tools
- Access and Control
  - PETs in the Enterprise
- Recourse
  - Laws and Regulations

Laws & Regulations

RESEARCH GROUP FOR

Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Laws and Regulations

- Privacy laws and regulations vary widely throughout the world
- US has mostly sector-specific laws, with relatively minimal protections
  - Self-Regulation favored over comprehensive Privacy Laws
  - Fear that regulation hinders e-commerce
- Europe has long favoured strong privacy laws
  - First data protection law in the world: State of Hesse, Germany (1970)
  - Privacy commissions in each country (some countries have national and state commissions)

Privacy Laws In the US

- Basis
  - 4th Amendment
- Historical Development (Surveillance)
  - Olmstead vs. US
  - Katz vs. US
  - Kyllo vs US
- Modern Privacy Laws (Informational)

4th Amendment

- Basis for many privacy issues in US
  - "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Olmstead vs. US, 1928

- Police caught bootlegger by placing wiretaps to phone lines outside his house
- Defendant claimed 4th Amendment
- Supreme Court claimed no physical trespassing occurred
  - Judge Brandeis disagreed: Phone Tapping a Search, Recording Conversation a Seizure
- Privacy as By-Product vs. Privacy as Limit of Power!

Katz vs. US, 1967

- Police Placed Microphone outside Public Phone in Front of Defendants House
  - Federal Communications Act, 1934, Forbid Wire Tapping (Exceptions Possible)
- Overruled Olmstead case: Reasonable Expectation of Privacy
- Law "protects people, not places."
  - Microphone was Unreasonable Search, Recording was Unreasonable Seizure

Kyllo vs. US, 2001

- Police used Thermal Image Scanner to Detect Heat Lamps Growing Marijuana Plants
- Supreme Court: Unreasonable Search Barred By 4th Amendment
  - Device Not In General Use By Public, Gives Expectation of Privacy
  - But: Visual Search Still Allowed

US Privacy Law (Tort)

- Allows Recovery of Damages (Prosser, 1960)
  - Intrusion
  - Disclosure of Private Facts
  - False Light
  - Appropriation ("Identity Theft")
- Other Torts
  - Intentional Infliction of Emotional Distress
  - Assault
  - Trespass
- But: No Privacy Protection in Public Places
  - Unless "Reasonable Expectation of Privacy"

Source: **Ronald B. Sandler, „Privacy Law in the USA"** (http://www.rbs2.com/privacy.htm)

US Public Sector Privacy Laws

- Federal Communications Act, 1934, 1997 (Wireless)
- Omnibus Crime Control and Safe Street Act, 1968
- Bank Secrecy Act, 1970
- Privacy Act, 1974
- Right to Financial Privacy Act, 1978
- Privacy Protection Act, 1980
- Computer Security Act, 1987
- Family Educational Right to Privacy Act, 1993
- Electronic Communications Privacy Act, 1994
- Freedom of Information Act, 1966, 1991, 1996
- Driver's Privacy Protection Act, 1994, 2000

US Private Sector Laws

- Fair Credit Reporting Act, 1971, 1997
- Cable TV Privacy Act, 1984
- Video Privacy Protection Act, 1988
- Health Insurance Portability and Accountability Act, 1996
- Children‘s Online Privacy Protection Act, 1998
- Gramm-Leach-Bliley-Act (Financial Institutions), 1999

Laws and Regulations

- Privacy laws and regulations vary widely throughout the world
- US has mostly sector-specific laws, with relatively minimal protections
  - Self-Regulation favored over comprehensive Privacy Laws
  - Fear that regulation hinders e-commerce
- Europe has long favoured strong privacy laws
  - First data protection law in the world: State of Hesse, Germany (1970)
  - Privacy commissions in each country (some countries have national and state commissions)

EU Data Directive

- 1995 Data Protection Directive 95/46/EC
  - Sets a Benchmark For National Law For Processing Personal Information In Electronic And Manual Files
  - Follows OECD Fair Information Practices
    - Collection Limitation, Openness, Purpose Specification, Use Limitation, Access, Security, Participation, Accountability
  - Facilitates Data-flow Between Member States And Restricts Export Of Personal Data To „Unsafe“ Non-EU Countries

Safe Harbor

- Membership
  - US companies self-certify adherance to requirements
  - Dept. of Commerce maintains list (222 as of 08/02)
    `http://www.export.gov/safeharbor/SafeHarborInfo.htm`
- Signatories must provide
  - **notice** of data collected, purposes, and recipients
  - **choice** of opt-out of 3rd-party transfers, opt-in for sensitive data
  - **access** rights to delete or edit inaccurate information
  - **security** for storage of collected data
  - **enforcement** mechanisms for individual complaints
- Approved July 26, 2000 by EU
  - reserves right to renegotiate if remedies for EU citizens prove to be inadequate

Privacy around the World

- Australia*
  - Proposed: Privacy Amendment (Private Sector) Bill in 2000
  - In talks with EU officials
- Brazil
  - Proposed: Bill No. 61 in 1996 (pending)
- Canada*
  - Passed: Bill C-6 in 4/2000
  - Under review by EU
- Hong Kong*
  - Passed: Personal Data (Privacy) Ordinance in 1995
- Japan
  - Currently: self-regulation & prefectural laws
  - In talks with EU officials
- Russia
  - Law on Information, Informatization, and Inform. Protect. 1995
  - In Progress: updated to comply with EU directive
- South Africa
  - Planned: Privacy and Data Protection Bill
- Switzerland*
  - EU-certified safe third country for data transfers

http://www.privacyinternational.org/survey/

* Has National Privacy Commissioner

EU Directive (cont.)

- 1997 Telecommunications Directive 97/66/EC
  - establishes specific protections covering telecommunications systems
  - July 2000 proposal to strengthen and extend directive to cover „electronic communications“
- Member states responsible for passing relevant national laws by 10/1998
  - 13 out of 15 member states have passed legislation, 2 are still pending (as of 08/2002)

Data Protection Agencies

- Australia: http://www.privacy.gov.au/
- Canada: http://www.privcom.gc.ca/
- France: http://www.cnil.fr/
- Germany: http://www.bfd.bund.de/
- Hong Kong: http://www.pco.org.hk/
- Italy: http://www.privacy.it/
- Spain: http://www.ag-protecciondatos.es/
- Switzerland: http://www.edsb.ch/
- UK: http://www.dataprotection.gov.uk/

... And many more

Post 9-11 Issues (US)

- Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001
  - online activities, surveillance, money laundering, immigration
- Operation TIPS (Terrorist Information and Prevention System)
  - Begin Scheduled August 2002
  - One Million Volunteers in 10 US Cities to Report "Suspicious Activity" (Goal: 4% of Population)
  - Targets: Letter Carriers, Utility Technicians, ...

Post 9-11 Issues (EU)

- Directive on Privacy and Electronic Communications 2002/58/EC
  - Members States Have Until 11/03 to Implement National Law Allowing Traffic Data Retention
  - Retention Period: 12 Months – 7 Years (Proposal)
- Data to be Retained (Planned Requirement):
  - Email: IP address, message ID, sender, receiver, user ID
  - Web/FTP: IP address, User ID, Password, Full Request
  - Phone: numbers called (whether connected or not), date, time, length, geographical location for mobile subscribers

See also: http://www.epic.org/privacy/intl/data_retention.html

Example UK

- UK Terrorism Act, 2001
  - Telcos, ISPs Retain Traffic Data Longer Than for Billing Purposes
  - Purpose: National Security Investigations
- Regulation of Investigatory Powers Act, 2000
  - Allows Law Enforcement Access To Retained Data
  - Planned: Extend Access to Health and Transport, Local Authorities, ... (Halted 06/02)
- Other EU Countries With Existing Laws for Data Retention:
  - Belgium, France, Spain

EU Private Video Surveillance

- Usually Governed By General Data Protection Principles (EU Directive)
  - Justified (by Agreement, Public/Private Interest, Law)
  - Proportional (Sufficient to Achieve Purpose)
    - Footage Selection
    - Storage Duration
  - Clearly Identified (Signs, maybe Contact Info)
  - Secure Storage (If Any)
  - Use Limitation (No Secondary Uses)

For Example of Swiss Law see http://www.edsb.ch/e/doku/merkblaetter/video.htm

Summary & Outlook

RESEARCH GROUP FOR

Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Summary

- Privacy Enhancing Technologies (PETs)
  - Large Body of Existing Technology (Internet)
  - Many New Challenges in Ubicomp
    - Authentication and Authorization
    - User Interfaces, Configuration for Consent
- Legal Aspects
  - Strong Differences US vs Europe
  - New Legal Developments Re. Data Retention

Privacy Web Sites

- http://www.privacyinternational.org
- http://www.privacyfoundation.org
- http://www.privacyexchange.org
- http://www.privacycouncil.com
- http://www.privacyplace.com
- http://www.junkbusters.com
- http://www.privacilla.org
- http://www.statewatch.org
- http://www.privacy.org
- http://www.pandab.org
- http://www.epic.org
- http://www.cdt.org

More Books

- Security for Ubiquitous Computing, by Frank Stajano
- The Privacy Law Sourcebook 2001: United States Law, International Law, and Recent Developments, by Marc Rotenberg
- Privacy & Human Rights, EPIC