Research Challenges in Privacy

Florian Kerschbaum / SAP Research
October 2012

What is a success of privacy research ?

Anonymous communication

It adds anonymity (privacy) as an additional function to network communication

It implements a technical approach to verifiable data minimization

It is a system that combines systems and cryptography

It is almost oblivious to existing protocols, algorithms and infrastructures

It was implemented and is run by a group of mostly academic volunteers

What is a challenge of privacy research ?

More and more is collected and processed in central data stores

The challenge is no longer at the network layer, but at the application layer

There is no rational reason to entrust your private data to service providers

Let‘s build on the success

Technically implement the data minimization principle

Combine systems and modern cryptography

The challenge is to implement applications that technically implement the data minimization principle

How would I address this challenge ?

Building privacy-preserving application one-by-one does not scale

Every privacy-preserving protocol one PhD student

What is an application ? Code

What is the best (oblivious) interface for a privacy-preserving tool for applications ? Code

In order to scale we need to build a compiler that translates the code into a privacy-preserving, data-minimizing application

The compiler needs volunteers (public funding)

A first application could be the privacy architecture for the Internet-of-Things/cyber-physical systems

Privacy-preserving smart metering, toll collecting, RFID

How to avoid big brother ?

Massive data collection (in the cloud) is a serious concern

The challenge is not protecting the sensor, but the database

The only principle that can help protect users is data minimization

Data should be controllable not collectable

Deletion cannot be reliably implemented

This is a technical challenge

The consequence of economics is that you can be cheated out of your privacy

- Although the only reasonable choice is to reveal nothing to data collectors

But it can be done ! (Although it‘s not obvious)

The data collectors will object !

The opposite needs to be proven by researchers

How can it be done ?

Modern cryptography has to offer many technologies

It is hard to understand (opposite from the economics)

- Education is necessary

The technological burden needs to be lowered

Cost of

- Running the system
- Developing the system
- Using the system

This requires public funding / research

Data collectors will not foster this development

It is in the public interest

Once feasibility has been proven, uptake needs to be regulated

Encrypted private data should no longer be private data (but the key should be)

Some proposals

Compiler for secure functions

An encrypted cloud database

A multi-user, privacy-preserving data exchange platform

Privacy in the Internet of Things

Encrypted computation on smartphones

Thank You!

Contact information:

Dr. Florian Kerschbaum
Research Expert
SAP Research
florian.kerschbaum@sap.com

© 2011 SAP AG. All rights reserved

© 2011 SAP AG. Alle Rechte vorbehalten.