Privacy in the semantic Web
Social networks based on XMPP

Jan Torben Heuer
Institute for Geoinformatics, University of Muenster

25C3 – nothing to hide – 2008
Why do I give this talk?

- Current ideas and work are based on my diploma thesis
- Open the project for non-academic users
- Discuss the approach with interested people
Overview

1 Motivation

2 Privacy in the social semantic web

3 Friend-to-Friend architecture
What is a social network?
**What is a social network?**

**Is a social network something new? What changed?**

- Is it social because it is written for the people? Unsure.
- It is social *because of* the people who use it.
What is a social network?

How differ the users today?

- Years ago, the internet was only available to academics and used by technology-geeks
- Today, all kinds of people use the internet
- Most users are not interested in technical details
What is a social network?

Why are social networks so attractive?

- Social applications are easy to use.
  - Your data are on the web, accessible from everywhere.
- Your real life and online life get connected
  - Real-life friends can easily be contacted
  - Make connections to thousands of new virtual friends.
What is a social network?

Why are social networks so attractive?

- Social applications are easy to use.
  - Your data are on the web, accessible from everywhere.
- Your real life and online life get connected
  - Real-life friends can easily be contacted
  - Make connections to thousands of new virtual friends.

Many users do not know about security or privacy issues
WHAT DOES PRIVACY MEAN?

Privacy is about...
What does privacy mean?

Privacy is about...

- Personal data stored in social networks
  - profiles on MySpace
  - bookmarks on Delicious
- Activity in the Internet
  - Doubleclick
  - Google analytics
- What others publish about me
  - Party photos on Facebook
What does privacy mean?

Privacy is about...

- Personal data stored in social networks
  - profiles on MySpace
  - bookmarks on Delicious
- My activity in the Internet
  - Doubleclick
  - Google analytics
What does privacy mean?

Privacy is about...

- Personal data stored in social networks
  - profiles on MySpace
  - bookmarks on Delicious
- My activity in the Internet
  - Doubleclick
  - Google analytics
- What others publish about me
  - your party photos on facebook ... is not technical issue!
What is the Semantic Web?

- A vision of a machine-readable internet (T. Berners Lee)
- One (or the only) example: FOAF profiles
- Internet as one big database
- Aggregate and combine information from different sources
WHAT IS THE SEMANTIC WEB?

- A vision of a machine-readable internet (T. Berners Lee)
- One (or the only) example: FOAF profiles
- Internet as one big database
- Aggregate and combine information from different sources

Will the semantic web come? Should we be prepared?
**How can we protect our privacy today?**

- Not using social networks is rarely an option
- The issue is the architecture:
  - Central databases store user information
  - The user doesn’t know what the provider does with the information

We need another architecture
Web based social networks
People store personal data on remote servers
What do we want to change?

1. Data must not be stored at a central place
2. Data exchange must be between friends only
3. Transmissions must be encrypted
XMPP Network
**XMPP Network**

- Extensible instant messaging protocol
- Is not true peer-to-peer but needs messaging servers
- Ensures communication between two peers even if they are hided between packet filters
PGP encryption

- PGP allows for secure end-to-end encryption
- Currently, PGP isn’t widely used
- We need user-friendly PGP support!
CURRENT PROTOTYPE

- Social bookmark sharing application
- Create bookmarks and tag them
- Query your friends recursively for tagged bookmarks
CURRENT PROTOTYPE

Privacy in the Social Semantic Web

Friend-to-Friend architecture

Privacy in the Semantic Web

Jan Torben Heuer
CURRENT PROTOTYPE

- Java6 Webstart application
- Sesame RDF database
- Smack API
- prefuse.org visualization toolkit
Open Challenges

- How can a serverless network survive? What happens if too many clients are offline?
- How can PGP be implemented in a secure but user-friendly way?
INTERESTED?

- Extend the current Java approach
- Create another client
  - Web interface
  - Instant Messenger extension (Pidgin, Kopete, ...)
  - Flash application
  - Mobile
THANKS FOR YOUR ATTENTION

Questions?