Implementing Privacy as Symmetry in Location-aware Systems

Anders Kofod-Petersen Espen Klæbo Jørgen Jervidalo
Kjetil Aaltvedt Magnus Romnes Trond Martin Nyhus

Second International Workshop on Combining Context
with Trust, Security, and Privacy
(CAT 2008)

June 16th, 2008

NTNU

Overview

Motivation

- Privacy is argued to be a main concern in (social) location-aware systems
- To construct truly *context-aware* systems, privacy issues must be overcome
- (Lack of) privacy can affect users' behaviour
- Many concepts are regarded as important, such as:
  - Anonymising or pseudonymising
  - Plausible deniability
  - Reciprocity
- Our main interest is developing a tool that allows us to investigating privacy and behaviour
- We have chosen to implement a location-aware system, using the *principle of minimal asymmetry*

Similar Projects

- Find My Friends
  - Two week project in co-operation with Accenture
  - Ultrasound positioning in *Samfundet* (63 microphones)
  - Privacy was handled *by invitation*
- FriendRadar
  - Location-aware friend system using WLAN
  - Implemented in Wireless Trondheim
  - Privacy was implemented as *minimal asymmetry*
- @School
  - Mobile collaborative learning system
  - Implemented using the WLAN system in Wireless Trondheim
  - Privacy was not explicitly addressed

Similar Projects

- Find My Friends
  - Two week project in co-operation with Accenture
  - Ultrasound positioning in *Samfundet* (63 microphones)
  - Privacy was handled *by invitation*
- FriendRadar
  - Location-aware friend system using WLAN
  - Implemented in Wireless Trondheim
  - Privacy was implemented as *minimal asymmetry*
- @School
  - Mobile collaborative learning system
  - Implemented using the WLAN system in Wireless Trondheim
  - Privacy was not explicitly addressed

Similar Projects

- Find My Friends
  - Two week project in co-operation with Accenture
  - Ultrasound positioning in *Samfundet* (63 microphones)
  - Privacy was handled *by invitation*
- FriendRadar
  - Location-aware friend system using WLAN
  - Implemented in Wireless Trondheim
  - Privacy was implemented as *minimal asymmetry*
- @School
  - Mobile collaborative learning system
  - Implemented using the WLAN system in Wireless Trondheim
  - Privacy was not explicitly addressed

Find My Friends

- Finding our friends at *Samfundet* during *UKA 2007*
- 1661 people with ultrasound positioning devices
- 207 users who answered the questionnaire
- 82% used the sender once or more
- 75% used terminals
- 55% would use a similar larger scale system
- Main finding: *If it's cool, privacy is not important*!

Find My Friends

- Finding our friends at *Samfundet* during *UKA 2007*
- 1661 people with ultrasound positioning devices
- 207 users who answered the questionnaire
- 82% used the sender once or more
- 75% used terminals
- 55% would use a similar larger scale system
- Main finding: *If it's cool, privacy is not important*!

FriendRadar

- WLAN based location-aware positioning service in Wireless Trondheim
- Similar to *Find my Friends*
- Implemented *minimal asymmetry*
- 24 pupils used it for 3 weeks
- Research data is gathered through:
  - Data-log analysis
  - Questionnaire
- Main result: *QoS of the WLAN technology not sufficient*

FriendRadar

- WLAN based location-aware positioning service in Wireless Trondheim
- Similar to *Find my Friends*
- Implemented *minimal asymmetry*
- 24 pupils used it for 3 weeks
- Research data is gathered through:
  - Data-log analysis
  - Questionnaire
- Main result: *QoS of the WLAN technology not sufficient*

@School

- Models pupils and tasks by employing:
  - Dreyfus' levels of competence
  - Gardner's multiple intelligences
  - Hofstede's cultural dimensions
- Model constructed as stereotypes in the tradition of Rich
- Tested on 24 pupils in upper secondary school
- Research data is gathered through:
  - Data-log analysis
  - Questionnaire
- Main result is similar to *FriendRadar*: :
  QoS of the WLAN technology not sufficient

@School

- Models pupils and tasks by employing:
  - Dreyfus' levels of competence
  - Gardner's multiple intelligences
  - Hofstede's cultural dimensions
- Model constructed as stereotypes in the tradition of Rich
- Tested on 24 pupils in upper secondary school
- Research data is gathered through:
  - Data-log analysis
  - Questionnaire
- Main result is similar to *FriendRadar*: :
  QoS of the WLAN technology not sufficient

Minimal Asymmetry

- The principle of minimal asymmetry attempts to tackle issues such as:
  - Mutual awareness
  - Disembodiment
  - Dissociation
- The main idea is to minimise the asymmetry of information flowing between *data owners* and *data users* by:
  - *Decreasing* the flow of information from data owners to collectors and users
  - *Increasing* the flow of information from data collectors and users back to data owners

Minimal Asymmetry

- The principle of minimal asymmetry attempts to tackle issues such as:
  - Mutual awareness
  - Disembodiment
  - Dissociation
- The main idea is to minimise the asymmetry of information flowing between *data owners* and *data users* by:
  - *Decreasing* the flow of information from data owners to collectors and users
  - *Increasing* the flow of information from data collectors and users back to data owners

Choice of Technology

- There are currently three protocols and models readily available:

  XFN XHTML Friends Network

  - Friendship is a *directional* relationship, thus asymmetric

  FOAF Friend of a Friend

  - Does not *explicitly* cover control of data issues

  XMPP Extensible Messaging and Presence Protocol (Jabber)

  - Is easily extensible and offers core functionality

Choice of Technology

- There are currently three protocols and models readily available:

  XFN XHTML Friends Network

  - Friendship is a *directional* relationship, thus asymmetric

  FOAF Friend of a Friend

  - Does not *explicitly* cover control of data issues

  XMPP Extensible Messaging and Presence Protocol (Jabber)

  - Is easily extensible and offers core functionality

Choice of Technology

- There are currently three protocols and models readily available:

  XFN XHTML Friends Network
  - Friendship is a *directional* relationship, thus asymmetric

  FOAF Friend of a Friend
  - Does not *explicitly* cover control of data issues

  XMPP Extensible Messaging and Presence Protocol (Jabber)
  - Is easily extensible and offers core functionality

Design

- A simple application that allows you to maintain a list of friends (and groups) and see their position on a map
- The system is designed as a server-client architecture, with a thin-client
- Communication is done through the GSM or UMTS networks
- Position is gathered from network operators' services
- All transmissions are uses the XMPP protocol
- It only supports a subset of XMPP's subscription states (*none* and *both*)

Implementation

- The system is implemented in Java and Python, using a relational database (PostgreSQL)
- Subscriptions are in both directions, that is both participants must agree to share *presence* and *location* information
- A user can (temporarily) make himself invisible, thus appearing *offline*
  - This will disable his ability to see others as well (preserving minimal asymmetry)
- Cancelling a subscription will make a user appear *offline* to others
  - Preserving minimal asymmetry and plausible deniability

Summary

- Functionality (and *coolness*) outweighs privacy
- Implementing minimal asymmetry might “hide” privacy from the user (in a good way)
- This implementation achieves minimal asymmetry by:
  - Enforcing bi-directional “invisibility”
  - Supporting directional cancelling of subscriptions
- The system uses (a subset of) standardised protocols
- The protocol is further extended to include contextual information

Summary

- Functionality (and *coolness*) outweighs privacy
- Implementing minimal asymmetry might “hide” privacy from the user (in a good way)
- This implementation achieves minimal asymmetry by:
  - Enforcing bi-directional “invisibility”
  - Supporting directional cancelling of subscriptions
- The system uses (a subset of) standardised protocols
- The protocol is further extended to include contextual information

Summary

- Functionality (and *coolness*) outweighs privacy
- Implementing minimal asymmetry might “hide” privacy from the user (in a good way)
- This implementation achieves minimal asymmetry by:
  - Enforcing bi-directional “invisibility”
  - Supporting directional cancelling of subscriptions
- The system uses (a subset of) standardised protocols
- The protocol is further extended to include contextual information

Summary

- Functionality (and *coolness*) outweighs privacy
- Implementing minimal asymmetry might “hide” privacy from the user (in a good way)
- This implementation achieves minimal asymmetry by:
  - Enforcing bi-directional “invisibility”
  - Supporting directional cancelling of subscriptions
- The system uses (a subset of) standardised protocols
- The protocol is further extended to include contextual information

Future Work

- In addition to the privacy implemented, some contextual information for the messages is also supported
- Messages between users can be tagged with *performatives* from *speech-act* as described by FIPA
- The server allows for a very high amount of logging
- This system should allow us to investigating user behaviour when using location-aware social system by tracing:
  - Physical connections
  - Social connections
  - Messaging patters

Future Work

- In addition to the privacy implemented, some contextual information for the messages is also supported
- Messages between users can be tagged with *performatives* from *speech-act* as described by FIPA
- The server allows for a very high amount of logging
- This system should allow us to investigating user behaviour when using location-aware social system by tracing:
  - Physical connections
  - Social connections
  - Messaging patters

Future Work

- In addition to the privacy implemented, some contextual information for the messages is also supported
- Messages between users can be tagged with *performatives* from *speech-act* as described by FIPA
- The server allows for a very high amount of logging
- This system should allow us to investigating user behaviour when using location-aware social system by tracing:
  - Physical connections
  - Social connections
  - Messaging patters