Privacy in GeoSIM System

-- Ling Hu

lingh@usc.edu

What can a mobile phone do?

- Phone, texting
- Email, Web surfing, media player, camera
- Mobile sensors with GPS
  - Monitor traffic
  - Weather, temperature, humidity
  - Detecting chemical/hazardous materials, pollution
 - ......

Background: GeoSim

- Every user has some Geo locations with a viewpoint to take pictures;
- Users capture pictures and upload to server;
- Server maps pictures to a 3D model to provide service;

Problem: Privacy Breach

- User location is sensitive and the user may not willing to share;
- Pictures may reveal the trajectory of a user;
- Some pictures may be sensitive and the user want to be an anonymous contributor;

- How to solve these problems in GeoSIM?

User Social Network

- Every user is connected to their "Friends";
- Users form a big "social" network and exchange pictures with each other;
- A connected graph achieves max privacy protection;
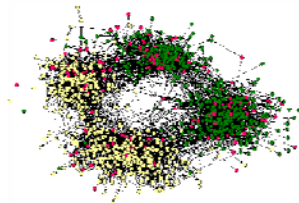
3-phase of Photo Sharing

- Picture acquiring phase:
  - Pictures are taken on spot with geo tags;
  - A random number t is assigned to each picture;
- Picture exchanging phase:
  - P2P communications;
  - User sends pictures to friends only;
  - t decrease by 1 on every exchange;
  - Exchange phase finishes when t is zero;
- Picture uploading phase:
 - When t is 0, picture is sent to the server by the current user;

Development

- Develop a client to maintain a friend list per user;
- Photo exchange protocols
  - Exchange photos between friends;
  - One can move photos between two of his friends;
- Upload photos to the server;

Physical channels of communication

- Friend-2-Friend
  - WIFI
  - Internet
  - Bluetooth
  - Message
  - etc……
- User-2-Server
  - Cellular network
  - Internet

Scenario
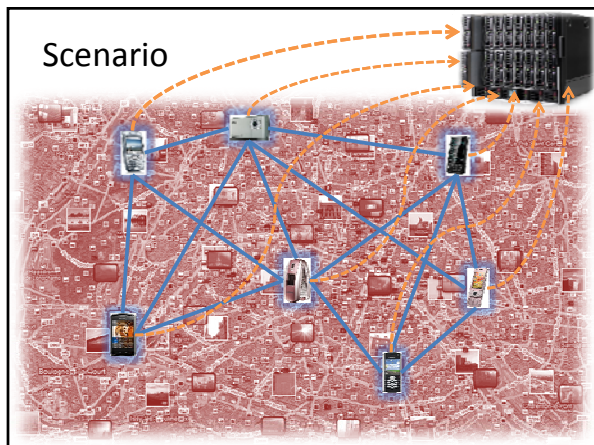
Analysis

- Photo exchange can be done in various ways, no server involved;
- Every photo goes through multi-users before it reaches the server;
- The chance that the server knows who is the original owner of a picture is no better than a random guess;
- None of the users know who was the original owner of a picture unless all the users are compromised and gives out their photo exchange history;

Attack Model

- Server is compromised;
- Users are compromised;
- Adversaries join the network and sniff P2P communications;

Requirements

- 3-4 players;
- Love programming, good in Java;
- With mobile phone programming Exp.
- Eager
  - to learn new technology;
  - **to change the world**;

Yes, We can!!!

Related work

- Tor Project: Online anonymity
  http://www.torproject.org/index.html.en
- Participatory Privacy Regulation (PPR)

  http://urban.cens.ucla.edu/technologies/selectivesharing/
- Selective Sharing
  http://urban.cens.ucla.edu/technologies/ppr/
- "They know all about you"
  http://www.guardian.co.uk/world/2006/aug/28/usa.searchengines