A Privacy Preserving System for Friend Locator Applications

Speaker: Bin Zan
WINLAB, Rutgers

Authors: Bin Zan, Tingting Sun, Marco Gruteser, Fei Hu, Yanyong Zhang
Online Social Networks

- Facebook
- MySpace
- Twitter
- LinkedIn
- Google+
- ...more
- ...and more
- ...

Anne Helmond, May 2009
Friend Locator Applications

* Iphone application: latitude. Image originally from Apple Store Website
Problem Statement

Privacy:

1) Eve wants to find friends in the same city, town, campus, building.

Accuracy:

1) You can know my location at city level, county level, town level, block level.

Flexibility:

1) I want to find friends in the: Same city? town? campus? building?
2) You can know my location at city level, county level, town level, block level?

Overhead:

location & location trace
Dual Resolution System

- **Phase One:**
  - Accuracy: coarse location information
  - Privacy: semi privacy protection
  - Overhead: individually small
  - Flexibility: user choice

- **Phase Two:**
  - Accuracy: fine location Information
  - Privacy: strong privacy protection
  - Overhead: system wide small
  - Flexibility: user choice
Phase One: Quadtree Based Multi-Level Splitting and Variable-Length Bit Seqs

Loc bit seq:

...011000...
Phase One: Differential Permutation

0010  \rightarrow  0000

0101 = 1011

Server

Alice
Bob

Eve
Phase Two: Polygon Decomposition

Rutgers School of Law | Newark

\[ P_1 = \{a_{11}x_1 + a_{12}x_2 \geq b_1; \]
\[ a_{21}x_1 + a_{22}x_2 \geq b_2; \]
\[ a_{31}x_1 + a_{32}x_3 \geq b_3; \]
\[ a_{41}x_1 + a_{42}x_4 \geq b_4; \]
\[ a_{51}x_1 + a_{52}x_5 \geq b_5 \} \]

\[ P_2 = \{(m_{11}x'_1 + m_{12}x'_2 \geq n_1; \]
\[ m_{21}x'_1 + m_{22}x'_2 \geq n_2; \]
\[ m_{31}x'_1 + m_{32}x'_2 \geq n_3; \]
\[ m_{41}x'_1 + m_{42}x'_2 \geq n_4; \}
\[ U(m_{51}x'_1 + m_{52}x'_2 \geq n_5; \]
\[ m_{61}x'_1 + m_{62}x'_2 \geq n_6; \]
\[ m_{71}x'_1 + m_{72}x'_2 \geq n_7; \]
\[ m_{41}x'_1 + m_{42}x'_2 \geq -n_4; \} \]
Phase Two: Strong Privacy Achievement

Linear Operation & Information Exchanging

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ \vdots & \vdots \\ a_{m1} & a_{m2} \end{bmatrix}$$

$$U^i = \tilde{A}_{*2} \tilde{x}_2$$

$$\begin{pmatrix} h_{11}a_{11} + h_{21}a_{12} \\ h_{11}a_{21} + h_{21}a_{22} \\ \vdots \\ h_{11}a_{m1} + h_{21}a_{m2} \end{pmatrix}$$

$$-h_{21}x_1 + h_{11}x_2$$

$$\begin{pmatrix} h_{22} & -h_{12} \\ -h_{21} & h_{11} \end{pmatrix}$$

$$V^i = \tilde{A}_{*1} \tilde{x}_1$$

$$U^i - b^i$$

$$\geq 0?$$

$$(U^i - b^i) + V^i$$
Evaluation Example: Variable-Length Bit Seqs
Entropy Enhancement

- Pure location only based splitting is suffered by population attack
- Splitting with population density in mind increases total entropy
Conclusions

● We have proposed a dual-resolution system for friend locator applications to preserve individual privacy, provide application accuracy, user flexibility and result in small overhead.

● Some techniques used in the system:
  ○ multi-level grid
  ○ variable-length bit sequences
  ○ differential permutation method
  ○ entropy enhancement splitting
  ○ convex polygon decomposition
  ○ linear operation
Questions?

... Thank You!