CS525: Who's Your Best Friend? Targeted Privacy Attacks In Location-sharing Social Networks

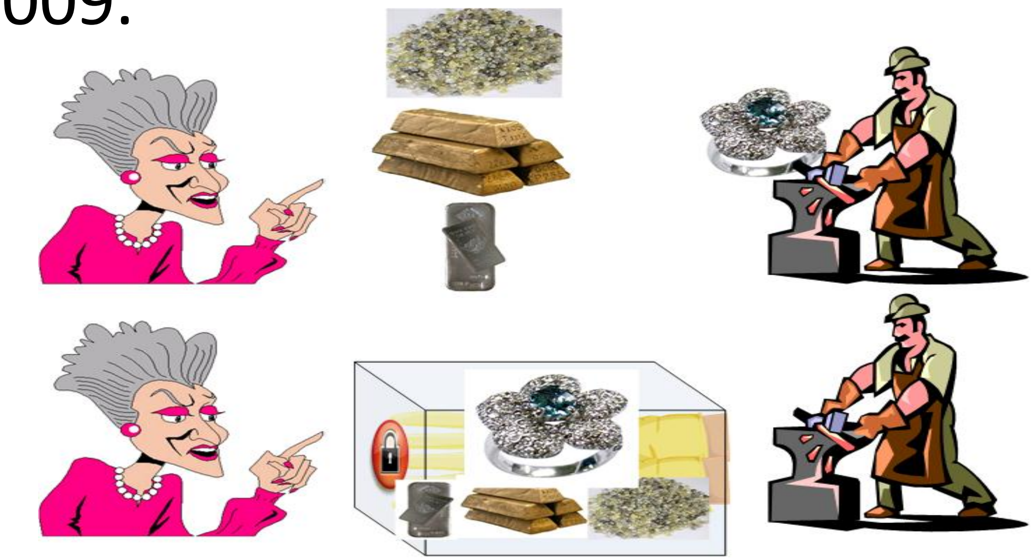
Wei Wang

ECE Dept.

Worcester Polytechnic Institute (WPI)

Security and Privacy Problems in the mobile and cloud computing

- Security and Privacy problem
  - Our private information could be accessed by the others when we outsourcing some computations by cloud
- One of the promising solution: Fully homomorphic Encryption, first plausible FHE was proposed by Gentry in 2009.



Fully Homomorphic Encryption

- Shortcoming: The algorithm has a vary large latency for the use of the million-bits multiplications and additions.
- Possible solutions:
  - New FHE schemes are coming out.
  - Design the specific chips for FHE (ASIC Design).
  - History tells:
  - Communication: GSM → 3G → 4G → …, drived by IC/SOC design technology
  - RSA (introduced in 1978): RSA circuit layed out in MIT basketball court (Shamir & Rivest) and it failed.

Overview: Targeted Privacy Attacks In Location-sharing Social Networks

- Two questions related to targeted location-sharing privacy attacks.
  - Given a group of users and their social graph, is it possible to predict which among them is likely to reveal most about their whereabouts
  - Given a user, is it possible to predict which among her friends knows most about her whereabouts.

- The authors analyze the privacy policies of users by using a realtime location sharing application, in which users actively shared their location with their contacts.

- Results and Discussion.

Related Work

- Location-sharing privacy
  - In the stressful situation involving unfamiliar environments or in crisis and safety scenarios, such services is important.
  - Users are more willing to share information with friends than acquaintances or strangers.
- Identifying “weak links”
  - Recent work on sharing ephemeral information shows that rule development is a function of tie strength.
  - Results show users are more prone to share with stronger ties as opposed to weak ties.

Study

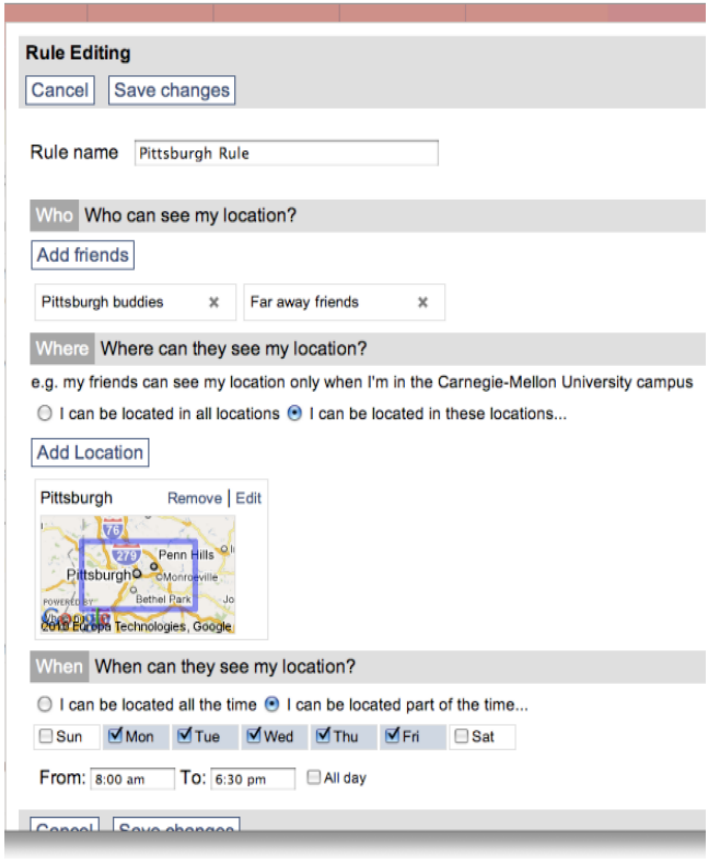
- Social Graph: a set of individual and the friendship ties.
- Degree Centrality: The number of direct connections that the user has.
- Openness: the percentage of simulated location requests made to A by B that were granted by A's policies.
- Trust: the average openness of user A towards all his friends.
- Trustworthiness: the average openness of A's friends towards A.
- Trust Rank: ranking A's friends in terms of how much they are trusted by A.
- Degree Rank: ranking A's friends in terms of their degree centralities.
- Mutual Rank: ranking A's friends in terms of how many mutual friends they have with A.

Hypotheses

- H1: Individuals who are more central to the social graph are likely to reveal the most about their location.
- H2: The target’s friends with the highest degree has higher probability of knowing more about the target.
- H3: The target’s friend with most common ties with the target knows most about the target.

System

- The study was conducted by deploying Locaccino.
- Two components: a Web application components and a mobile components.
- Platforms: Windows, Apple laptops and Symbian Smartphones.



Rule Editing

Rule name: Pittsburgh Rule

Who — Who can see my location?

Pittsburgh buddies × Far away friends ×

Where — Where can they see my location?

e.g. my friends can see my location only when I'm in the Carnegie-Mellon University campus

○ I can be located in all locations ● I can be located in these locations...

Pittsburgh Remove | Edit

When — When can they see my location?

○ I can be located all the time ● I can be located part of the time...

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

From: 8:00 am To: 6:30 pm □ All day

Figure 1. Screenshot of Locaccino's functionality that allows users to construct their location sharing policy rules.

System

- Social graph: An undirected unweighted graph describing the friendship between all the participants.
- Policy graph: A directed weighted graph describing the privacy policies between the users. The weight of the edge from users A to users B is a value between 0 and 1 based on the “openness” of user A towards user B.
- The openness value of (A,B) was calculated as the percentage of B’s possible requests that were granted by A’s policies. For each pair of users (A,B) in the dataset, a simulation was ran, which user B repeatedly requested the location of A. These requests were processed by the policies of user A.

Results

- The study ran for a month with 340 users in Facebook.
- The derived policy graph contained 1778 policy rules, two for each of the 889 friendship ties within the user population.

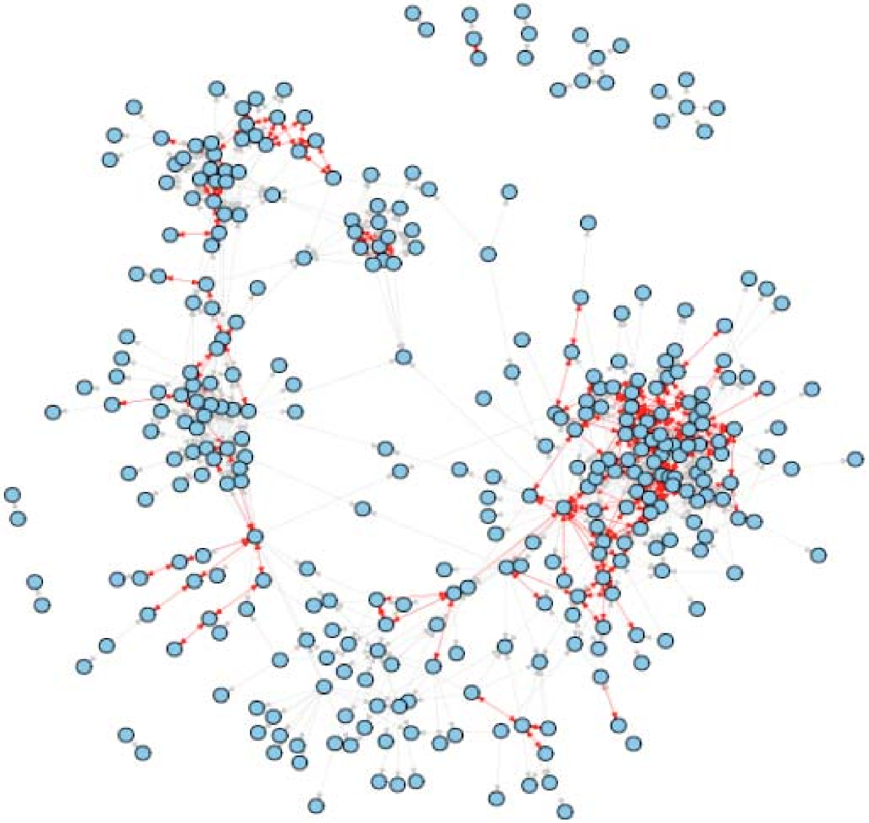


Figure 2. The graph representing the participants (nodes) and their trust relationships as directed edges. Mutually open relationships are highlighted in red.

Results

- The average openness that they show towards their friends was calculated and the average openness that a user was shown by his friends (their trustworthiness) was calculated.

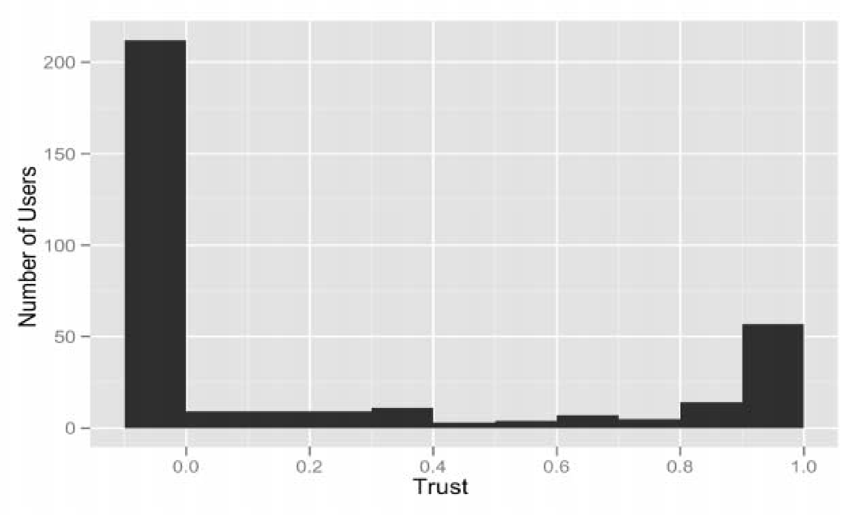


Figure 3. Histogram of distribution of nodes' average openness (i.e. the average of all outgoing ties for each node)

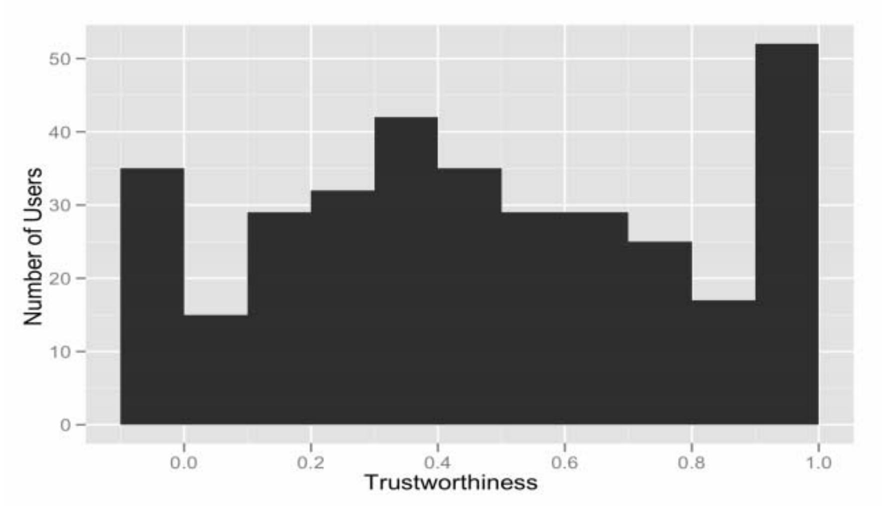


Figure 4. Histogram of nodes' average trustworthiness (i.e. the average of all incoming ties for each node).

Hypothesis testing

- H2: The target's friends with the highest degree has higher probability of knowing more about the target.
- All of A's friends were ranked in terms of how much they are trusted by A (Trust Rank), and in terms of how many friends they have (Degree Rank).

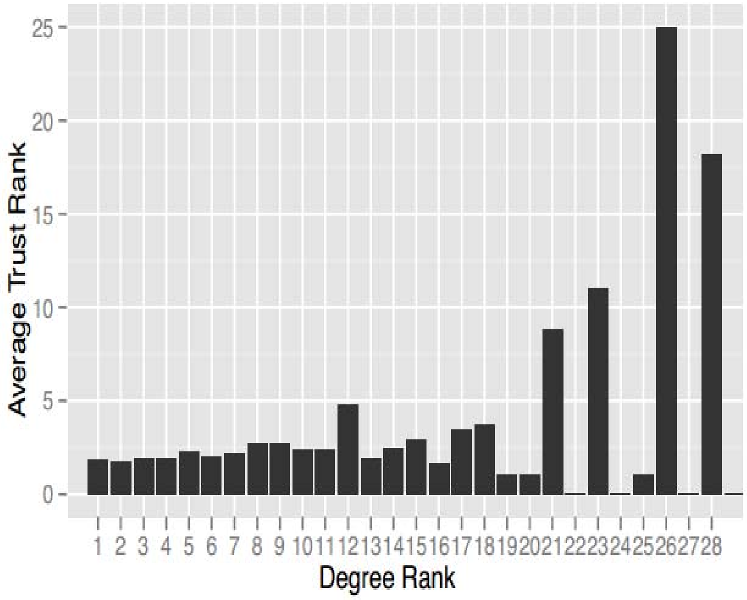


Figure 5: Degree rank of nodes (x-axis) versus the average trust rank (y-axis) for all nodes of a specific degree rank

Hypothesis testing

- H3: The target's friend with most common ties with the target knows most about the target.
- For each user A, all of A's friends were ranked in terms of how much they know about A (Trust Rank) and in terms of how many mutual friends they have with A (Mutual Rank).

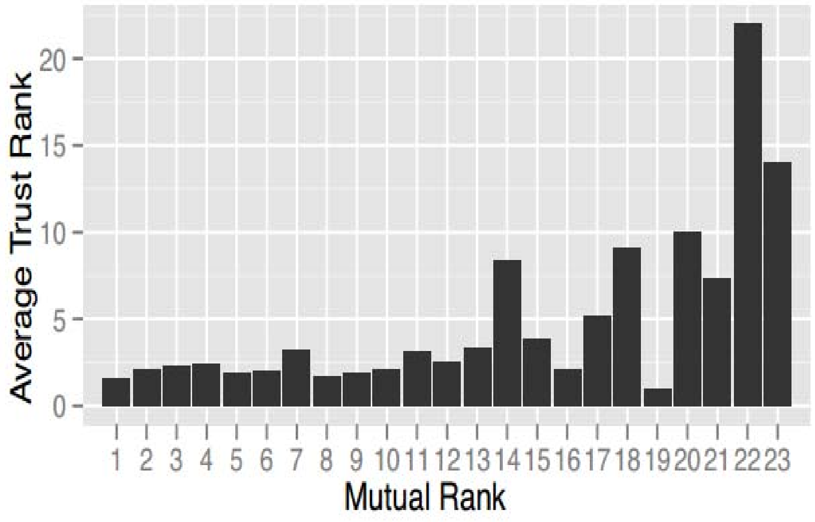


Figure 6. Histogram of Mutual rank (x-axis) vs. average trust rank (y-axis) for all nodes of a specific CommonFriends rank.

Discussion

- Targeted location-sharing privacy attacks
  - The attacker needs to identify suitable targets.
  - Then the attacker attempts to gain access to the target in order to collect data about the target location.
    - The attacker needs to figure out which one of the target’s friends are more likely to have access to the target’s location data.
    - The attacker could collect data about the target by befriending one of the target’s friends, a “weak link”.
  - Two questions proposed in the overview
  - The study captured a measure of “openness” between individuals, which reflects the probability that a request for someone’s real-time location is likely to be satisfied.
  - Trust and Trustworthiness could be applied across multiple features of online social networks.

Discussion

- Identifying a suitable target
  - The motivation for H1 was to suggest a way in which the attacker can identify users who are more likely to share their location with friends.
  - The results show that individuals who are more central to their network are more likely to be willing to share their location with others, being good target for a potential attacker.

Discussion

- How to target individuals
  - Identify a weak link
    - Based on the number of friends that a weak link may have (H2). (Reciprocity in social interactions)
    - Based on the number of common friends that the weak link may have with the target (H3). (Indicate shared membership in a community or organization)
    - H2 and H3 are directly related. Individuals have many friends are more likely to be extroverts who socialize and engage in multiple social interactions activities.

Discussion

- Protection against such privacy attacks
  - Individuals are notified if anyone is making too many location-sharing requests.
  - The users can ensure their information is visible only to their friends.
  - Limits could be imposed on how often a user can update their location.
- Making useful predictions
  - The system may be able to make automated suggestions about who to ask regarding whereabouts of interest based on a simplistic network-structure analysis.

Limitations

- In real life, there may be multiple factors affecting the share of information (battery life and group norms).
- This study presents and tests a generic strategy to do such an attack. (How the information are recorded).
- The application starts with a default privacy policy of not sharing their location information with anybody in the network. The seasoned users of the system could invest more time to articulate their location sharing preferences.

Q&A

THANKS