



University of Pittsburgh

# Threats & Vulnerabilities in Online Social Networks

**Lei Jin**

LERSAIS Lab @ School of Information  
Sciences

University of Pittsburgh

**03-26-2015**





# Topics

- Focus is the new vulnerabilities that exist in online social networks
  - Typical online social networks (OSN); E.g., Facebook & LinkedIn
  - Location-based social networks (LBSN); E.g., Foursquare & Yelp
- Not the traditional problems in online systems
  - Secure Communication
  - Web-based Attacks; E.g., SQL Injection, Cross Site Scripting



# Outline

- Identity & Authentication Problems
  - Email Address, Connections of Identities & Login
  - Social Authentication
  - Identity Validation
- Privacy Issues
  - Privacy of User Profiles
  - Privacy of Friendships
- Malicious Resources



# Purpose

- Be aware of these problems & know how to mitigate or avoid the potential attacks
- Start to know current research topics regarding security & privacy in online social networks

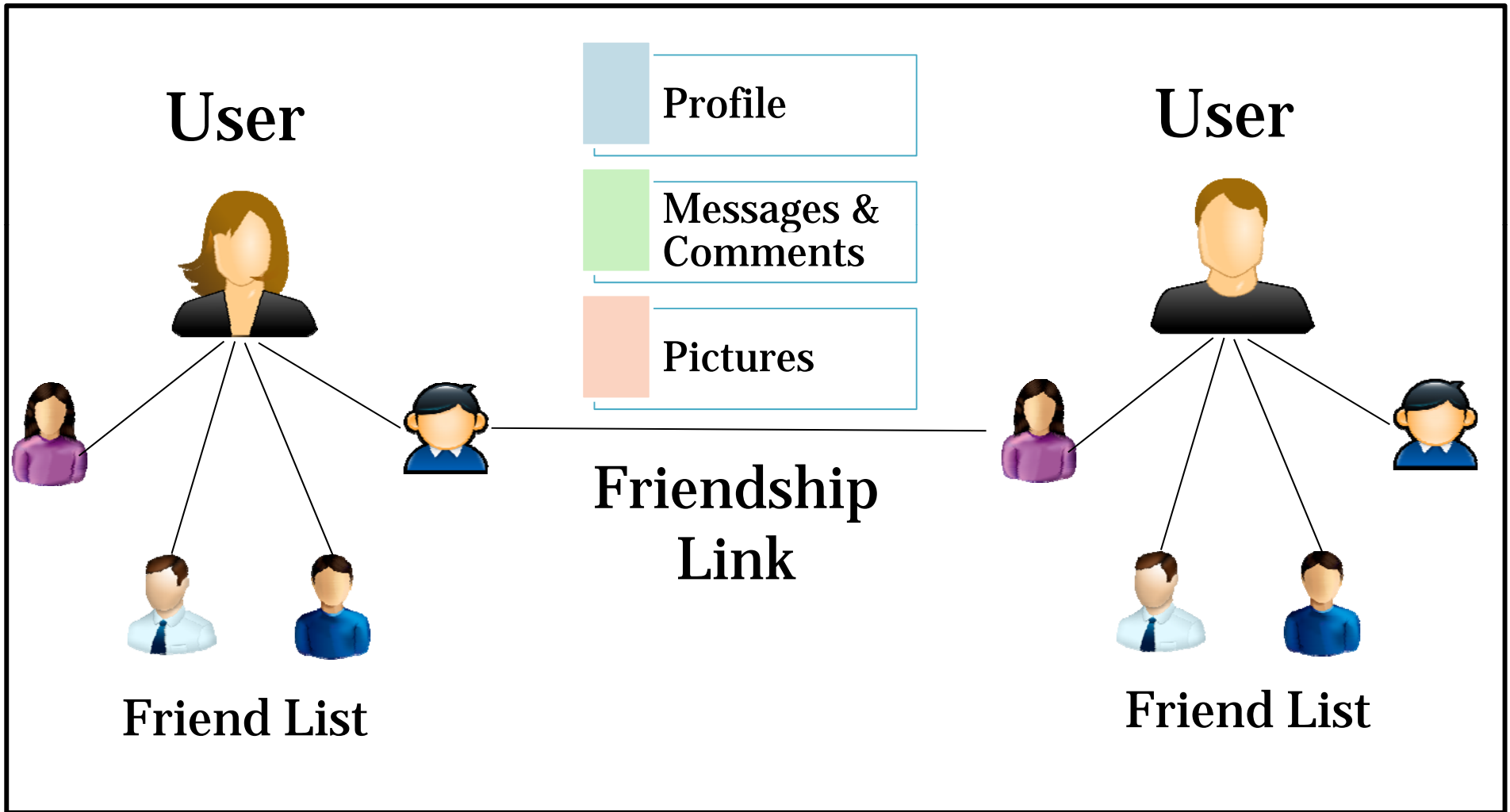


# Social Media Landscape **2013**





# Background – OSN

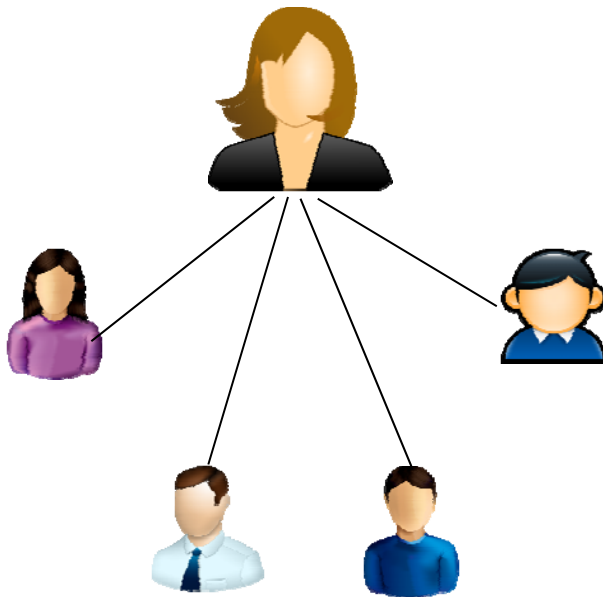






# LBSN

## User



Friendship  
Network

Create venues

Explore  
various places

Check in at  
venues



CHECK-IN

*(user, venue, time,...)*

## Venue

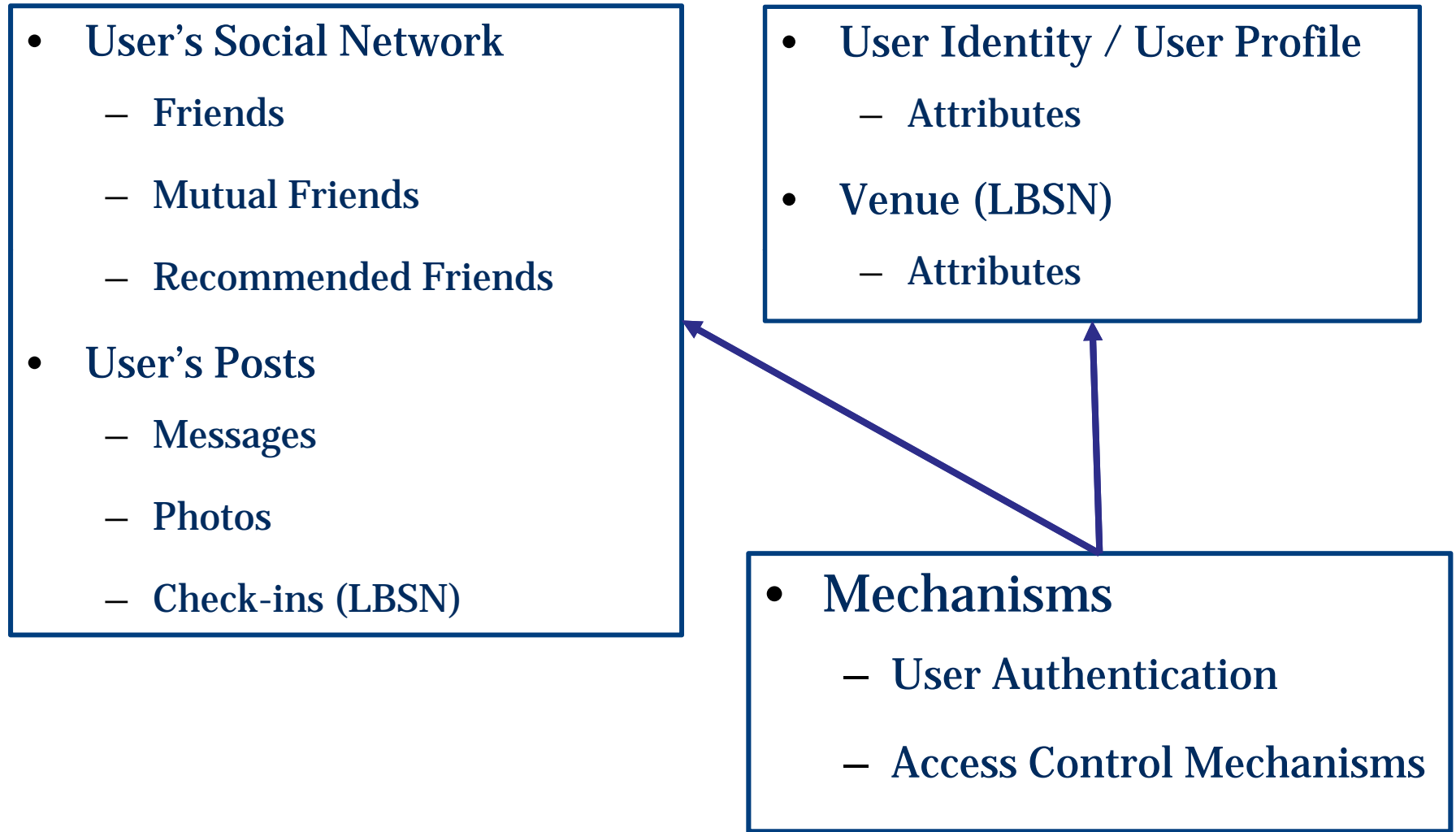


VENUE

*(name, location, category,...)*



# Entities, Elements & Mechanisms







# Outline

- Identity & Authentication Problems
  - Email Address, Connections of Identities & Login
  - Authentication
- Privacy Issues
  - Privacy of User Profiles
  - Privacy of Friendships
- Malicious Resources



# Email Address as Identity [1]

- Most online systems adopt a user's email address as the user's identity
- Caused and causing many threats
  - Used to identify various identities of a user in many online systems
  - More vulnerable regarding online password cracking
    - Share the same password
    - Avoid the limits of fail login times
  - Cracking one email address = Cracking related online accounts associated with this email address



# Email Address as Identity (cont.)

- Possible solutions
  - Different email addresses?
  - Different passwords?
  - Password management?



## Email Address as Identity (cont.)

- Email address is private & sensitive
- **Anonymous Email Service**
  - Like Craigslist email system
  - [leijin@anonymous.com](mailto:leijin@anonymous.com) <-> [leijin@gmail.com](mailto:leijin@gmail.com)
  - Anonymous.com
    - ✓ Accept, extract messages and construct the new email, send
    - ✓ No any record
    - ✓ Not record [leijin@gmail.com](mailto:leijin@gmail.com) as a plaintext
  - Gmail
    - ✓ Not disclose [leijin@anonymous.com](mailto:leijin@anonymous.com)



# Outline

- Identity & Authentication Problems
  - Email Address, Connections of Identities & Login
  - Authentication
- Privacy Issues
  - Privacy of User Profiles
  - Privacy of Friendships
- Malicious Resources



# Authentication problems in OSNs

- Authentication between a user and a social network system: facilitating login attempts (Login)
- Authentication between users: validating a user's identity (Identity Validation)



# Login

- Motivations
  - Difficult to remember text-based passwords
  - Tend to use one simple password for multiple systems
- Social Authentication: adopting users' knowledge in OSNs to authenticate users in order to facilitate their login attempts





# Photo-Based Authentication

- Proposed by Yardi *et al.* [2]
- Basic idea: authenticate a user's login using the tagged photos in Facebook based on the assumption that a user can identify their friends from various photos



## Photo-Based Authentication (cont.)

- Facebook Implementation
- It is triggered when the system detects a suspicious login attempt, according to a set of heuristics
  - the user logs in from a different geographical location
  - uses a new device (e.g., computer or smartphone) for the first time to access his account



## Photo-Based Authentication (cont.)

- A sequence of 7 pages featuring authentication challenges after the password-based authentication



This appears to be:

- |                                      |   |   |
|--------------------------------------|---|---|
| <input type="radio"/> Jason Polakis  | <input type="radio"/> Marco Lancini     | <input type="radio"/> Georgios Kontaxis |
| <input type="radio"/> Federico Maggi | <input type="radio"/> Sotiris Ioannidis | <input type="radio"/> Angelos Keromytis |

them, but must correctly identify the people in at least 5 to pass the social authentication test



# Issues in Photo-based Social Authentication

- Kim *et al.* [3]
  - Friend information is not private enough
  - People in the photos can be automatic recognized using face recognition tools
  - Such a social authentication is vulnerable to statistical guessing attack for the names
- Polakis *et al.* [4] conducted the real attacks for the photo-based social authentication in Facebook
  - Access to 42% of friends -> solve 22% of Facebook social authentication tests
  - Access to 120 faces of friends - > solve 100%



# Improvements

- Polakis *et al.* [5]
  - photo selection by using photos that fail software-based face recognition

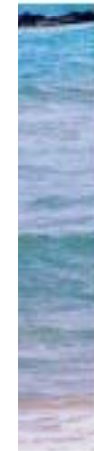
– photo  
mat



• F



nder image



ted

with




## Improvements (cont.)

- Jain *et al.* [6]: asks users to verify information about private their social contacts and their interactions
- Results: not as what they expected, since many users tend to private their

**Message Test**

One of the following five pictures is of a friend with whom you exchanged a message with recently. Type in the complete name of that friend (Please wait for the images to load)



Name



## Conclusions - Login

- Social authentication (*e.g.*, photo-based authentication) still needs many improvements
  - Not each user has enough friends who are tagged in the photos
  - No enough appropriate photos for authentications
  - Theatrical analysis: How secure is it?





# Identity Validation

- Motivations
- Difficult to identify the authenticity of a user's identity in an OSN
  - Identity Clone Attacks [7] -> Various Security & Privacy Attacks



# Cloned Identity



**Lei Jin**

PHD at University of Pittsburgh  
Greater Pittsburgh Area | Computer & Network Security  
Education University of Pittsburgh, Tsinghua University, Tsinghua University

[View Full Profile](#)



**Lei Jin**

PHD at University of Pittsburgh  
Greater Pittsburgh Area | Computer & Network Security

[View Full Profile](#)



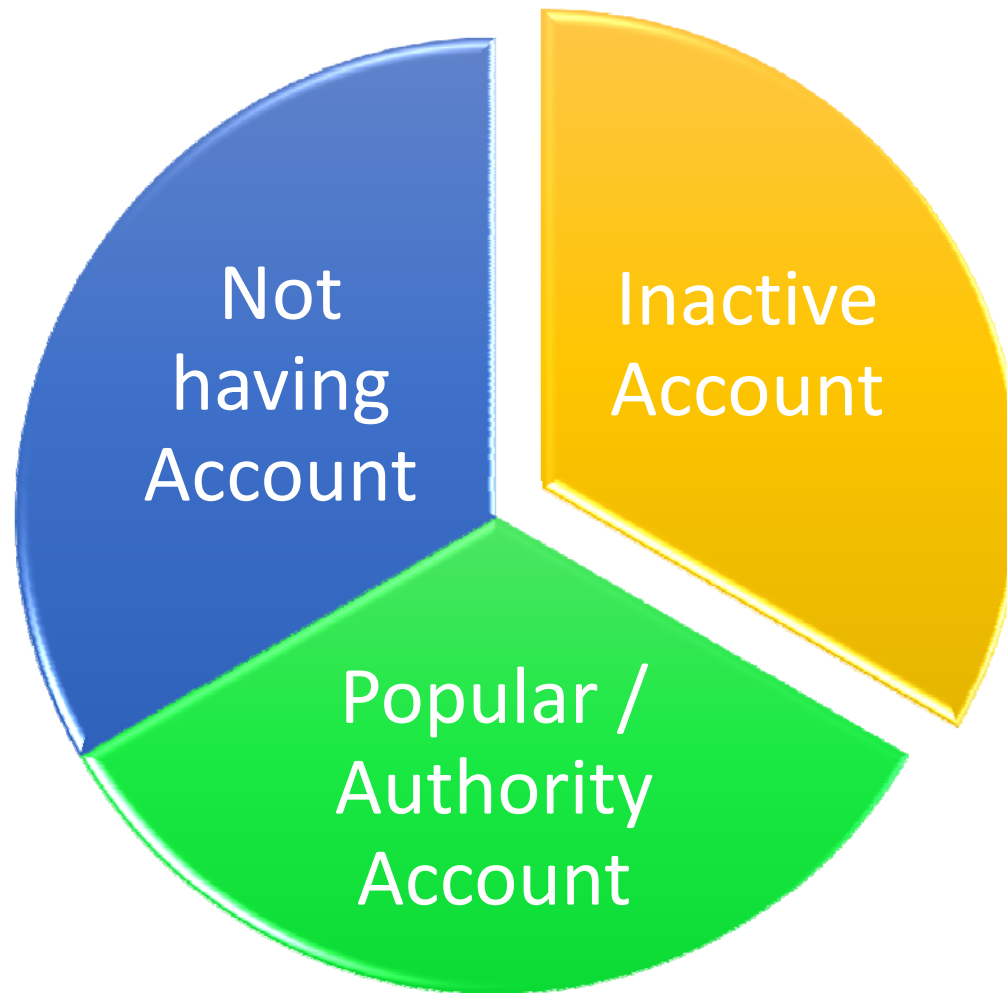


# Identity Clone Attack [7] - Design

- **Attributes:** name, education, birthday...
- **Friend network**
  - **Friend List (FL):** Connected friends of an ID
  - **Recommended Friend List (RFL):**
    - ✓ Generated by OSN systems (function of “*People You May Know*” on Facebook)
    - ✓ Share same RFs
  - **Excluded Friend List (EFL):**
    - ✓ Social embarrassments
    - ✓ Attackers - try to connect these individuals



# What are the best targets

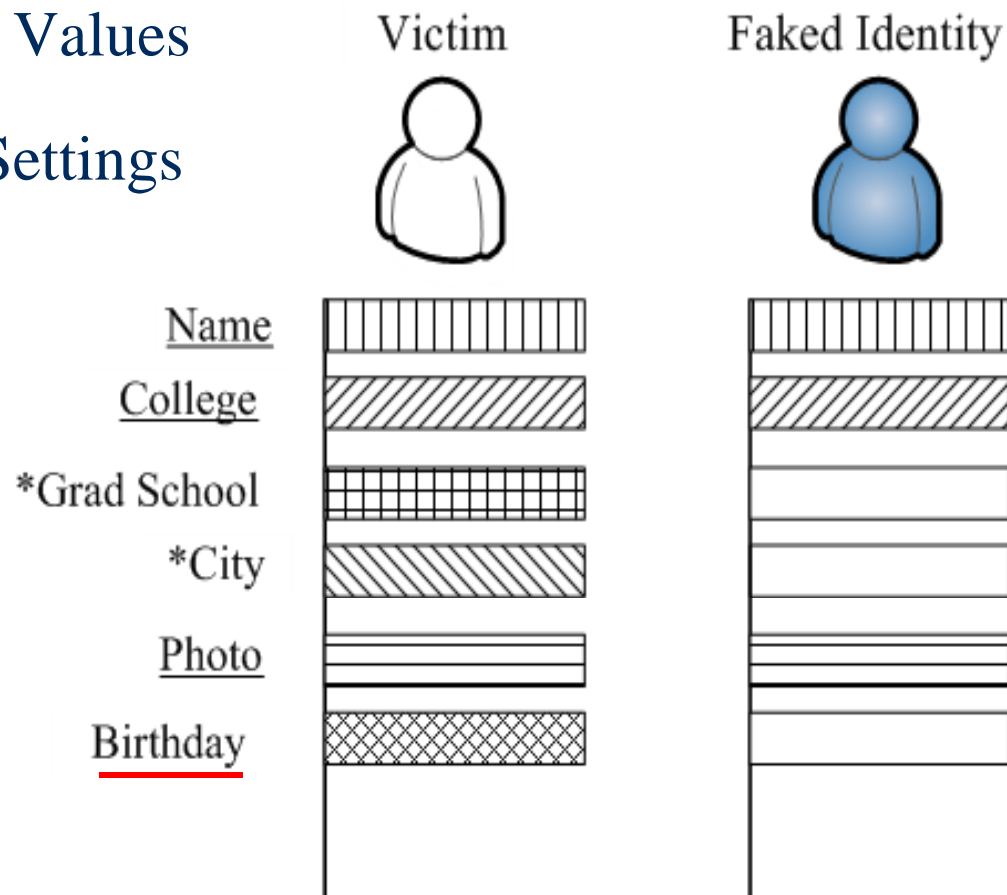




# Attribute As Target

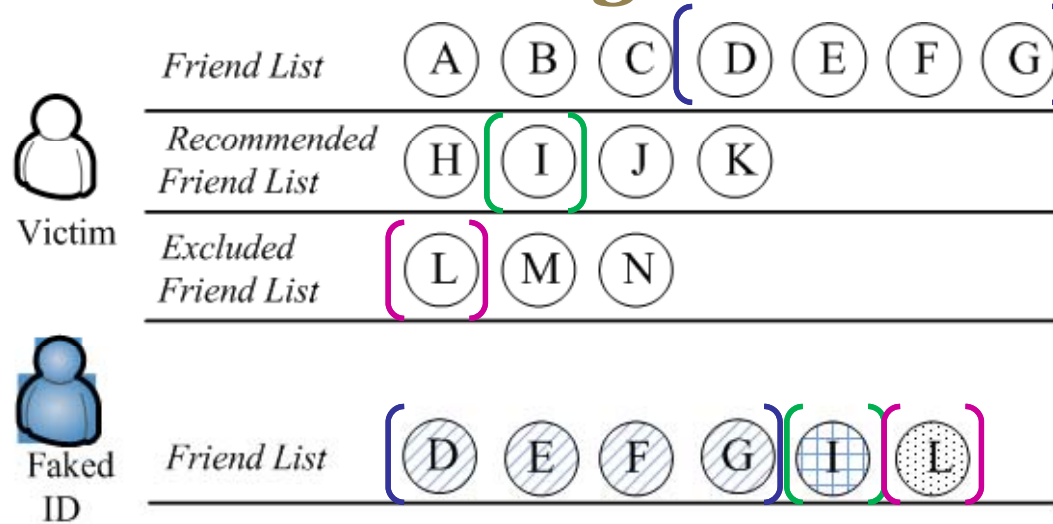
## Sub Targets:

1. Attribute Values
2. Privacy Settings

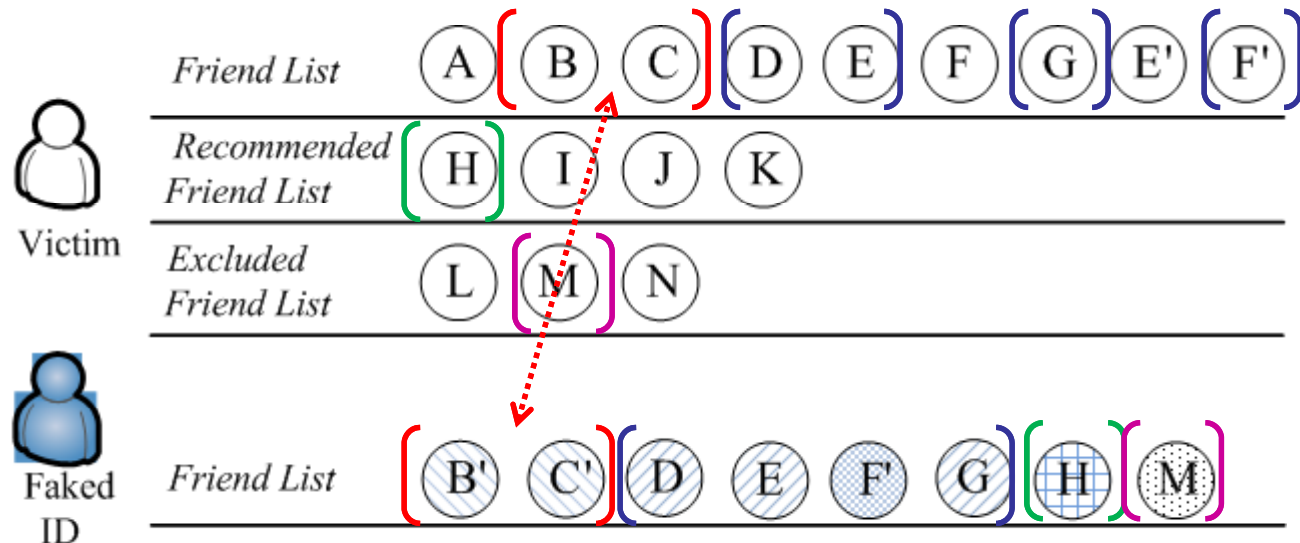


## Friend Networks As Target

FL  
RFL  
EFL

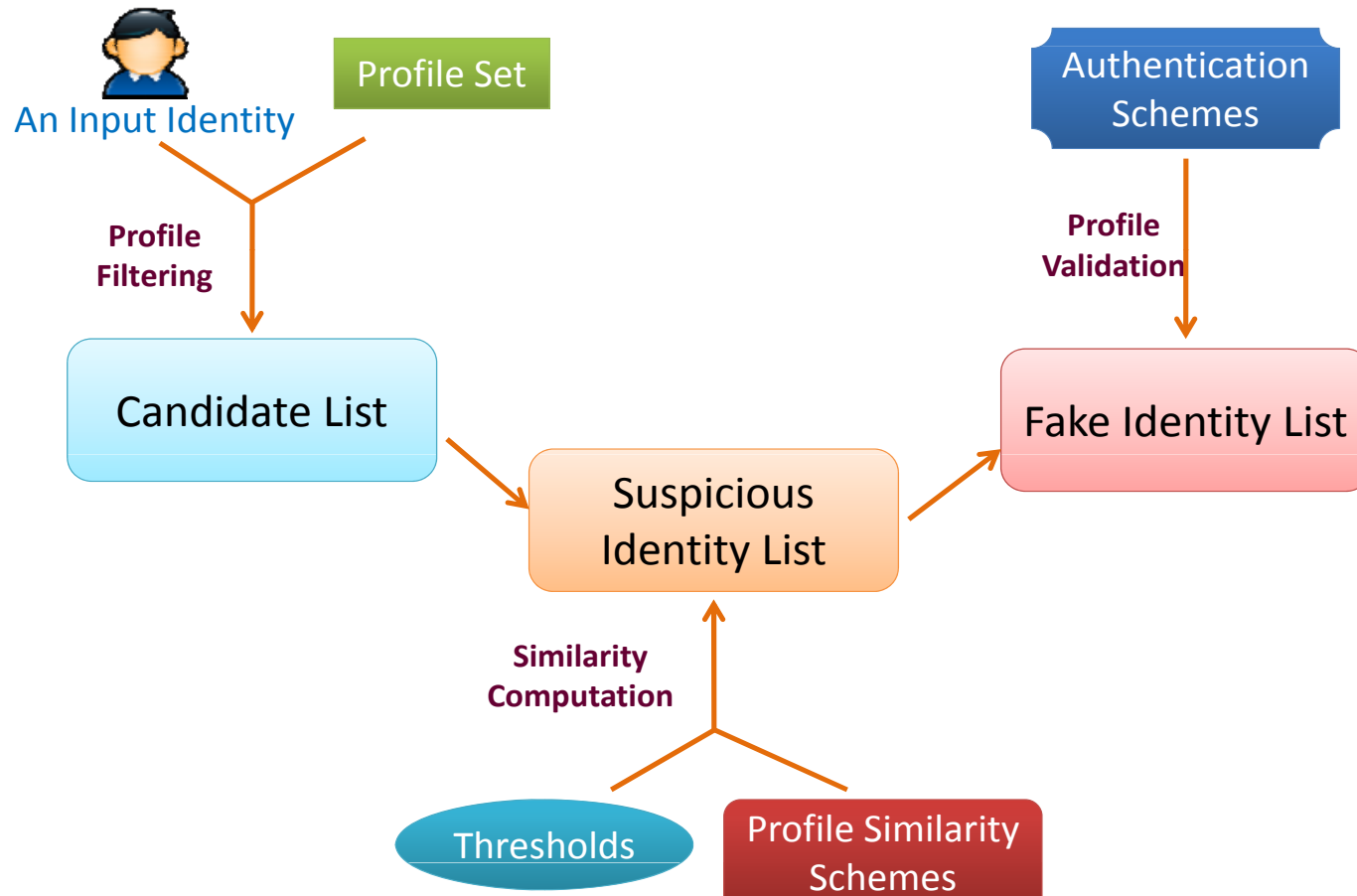


FL  
RFL  
EFL  
Faked ID





# Cloned Identity Detection [7]







# Profile Similarity

## Attribute Similarity

$$S_{att}(P_c, P_v) = \frac{SA_{cv}}{\sqrt{|A_c| \times |A_v|}}$$

Basic Principle: Similar Attributes in Two Profiles

## Friend Network Similarity

For Basic Profile Similarity (BPS)

$$S_{bfn}(P_c, P_v) = (\alpha S_{ff} + \beta S_{frf} + \gamma S_{fef})$$

Basic Principle:  
Mutual Friends in Friend Networks

For Multiple-faked Identities Profile Similarity (MFIPS)

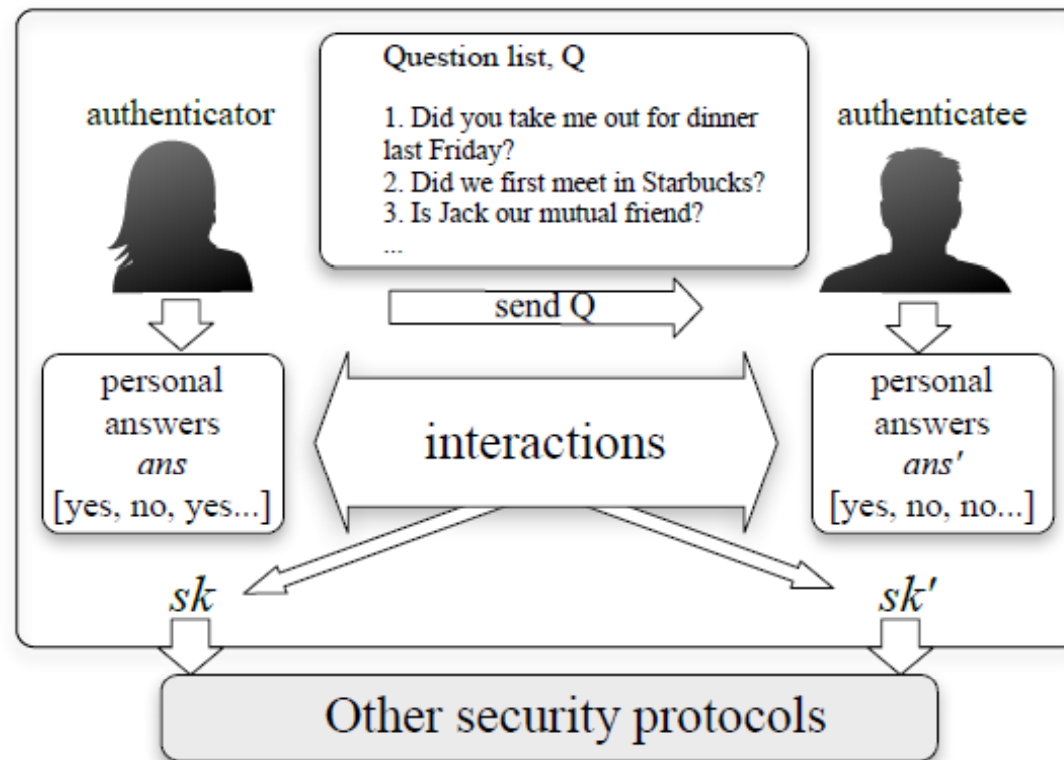
$$S_{mfn}(P_c, P_v) = \alpha(S_{s-ff} + S_{s-cf}) + \beta(S_{s-frf} + S_{s-cfrf}) + \gamma S_{s-fef}$$

Basic Principle:  
Similar Friends in Friend Networks

# Identity Validation

- Li *et al.* [8] propose a key exchange protocol that utilizes the secret questions, which work like a

"natural" interaction between two parties





## Identity Validation (cont.)

- Proposed by Zhao *et al.* [9]
- Basic Idea:
  - A user trusts their friends and the trust in a social network system is transitive. A user could find a trusted path, indicating the transmission of the trust, to another in a social graph
  - When two strangers meet in a social network, if they can find a trusted path, then they can rely on this common trusted persons in the path to authenticate each other



# Conclusions - Identity Validation

- Many limitations
- *Li et al*:
  - Friends in the physical world
  - Not enough secrets
  - How to select secrets
- *Zhao et al*:
  - trust may not be transitive



## Conclusions - Identity Validation (cont.)

- A practical approach [7]:
  - To ask users to provide their IDs in the real world
  - Education



# Outline

- Identity & Authentication Problems
  - Email Address, Connections of Identities & Login
  - Authentication
- Privacy Issues
  - Privacy of User Profiles & Shared Resources
  - Privacy of Friendships
- Malicious Resources



# Infer User's Profile Information

- Assumptions: Friends tend to share the same interests
- Inferring a targeted user's private attribute based on his/her friends' public attributes
- Example [10]:
  - A user hides his education and occupation from the public
  - Many of a user's friends are current students at the University of Pittsburgh
  - Inference: University of Pittsburgh, Student





## Issues related to Shared Resources

- Photos
  - A photo includes multiple individuals
  - One of them posts it in his/her wall
  - Privacy: others in the photos may be upset
- Check-ins (LBSNs) [11]
  - A user exposes where and when he is
  - A user exposes where he lives
  - A user's friend or other people expose the user's location related information
- Existing Access Control mechanisms cannot address all of these problems [12]



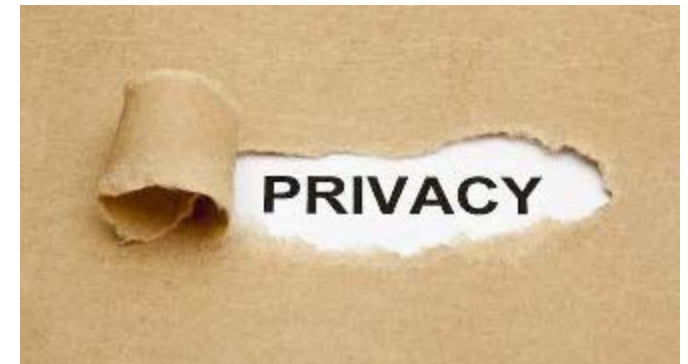
# Outline

- Identity & Authentication Problems
  - Email Address, Connections of Identities & Login
  - Authentication
- Privacy Issues
  - Privacy of User Profiles & Shared Resources
  - Privacy of Friendships
- Malicious Resources



## Issues Related to Users' Friend Lists

- Importance of the friend list
- What a user's friends reveals
  - Family, Work, Income, Reputation, Religion...
  - Used for Identity Clone Attacks
  - Used for Inferring Private Attributes





# Attacks - Expose a User's Social Network

- Mutual-friend based Attack [13]
- Friendship Identification and Inference Attack [14]

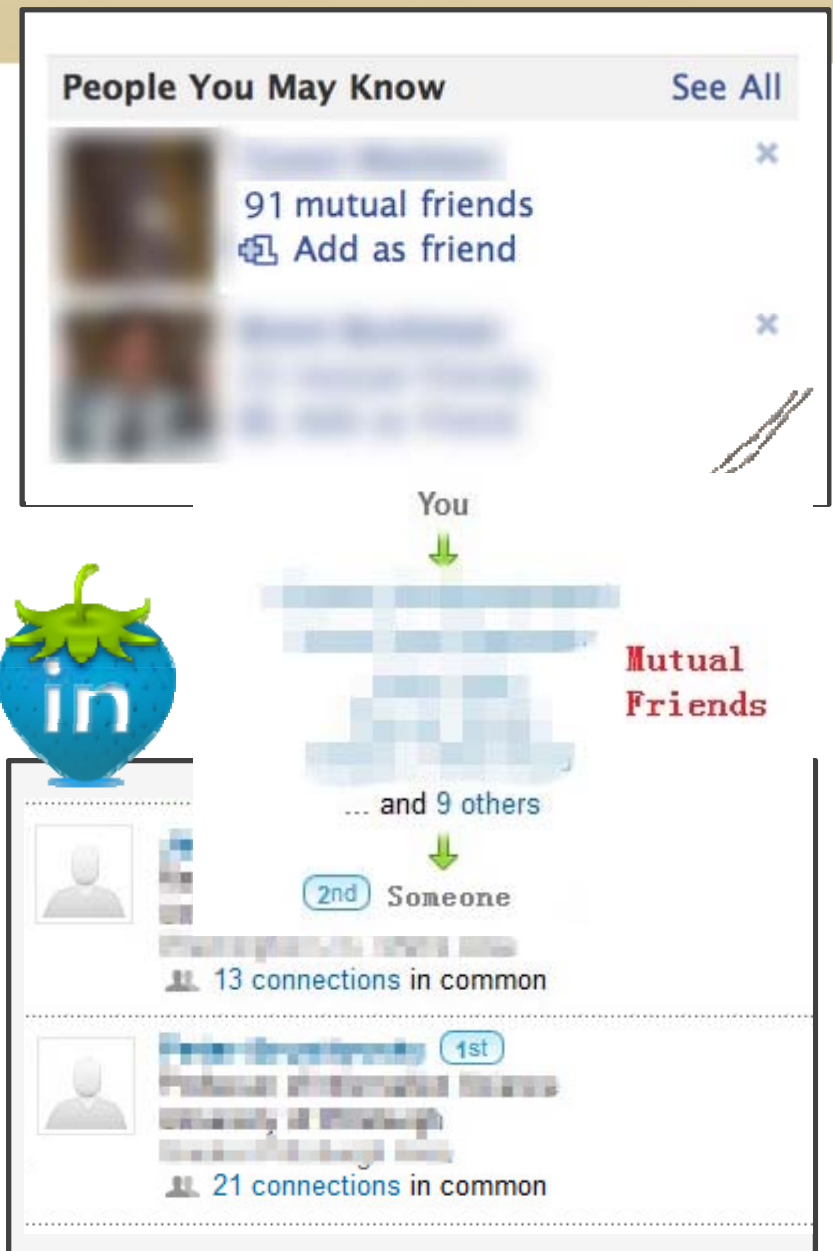




## Mutual Friend Feature

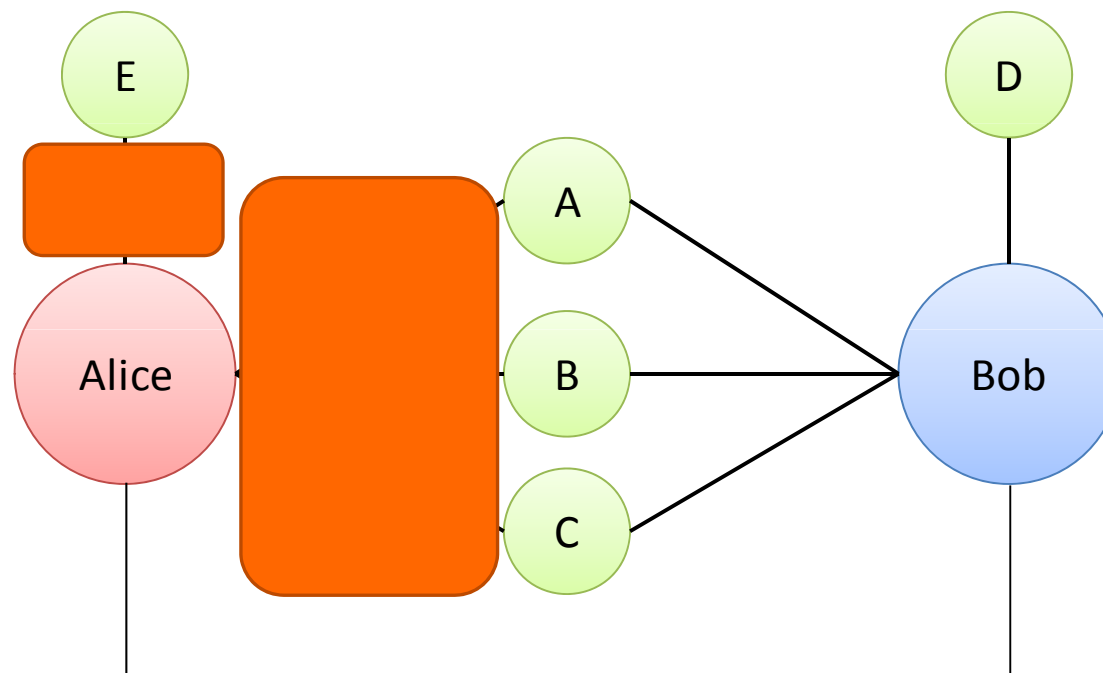
- Show mutual friends between two users
- Useful feature, *e.g.* Friend Recommendation, Friend Introduction

Lack of the Access Control Mechanism !





# Attack Example





# Defense Approaches

- Reason
  - ❖ **no restriction** for querying mutual friends
- Defense approaches
  - ❖ Hide user profile
  - ❖ Access control to query mutual friends

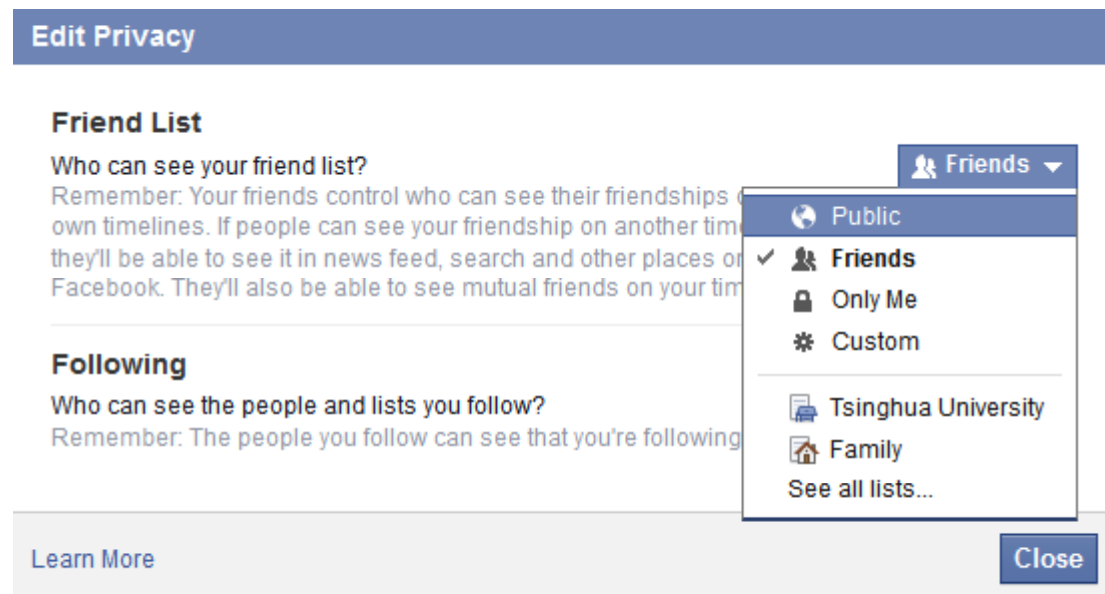




# Friendship Identification & Inference Attack

- Users' Privacy Settings for Friend Lists
  - Private
  - Friends w/o an excluding list
  - Public

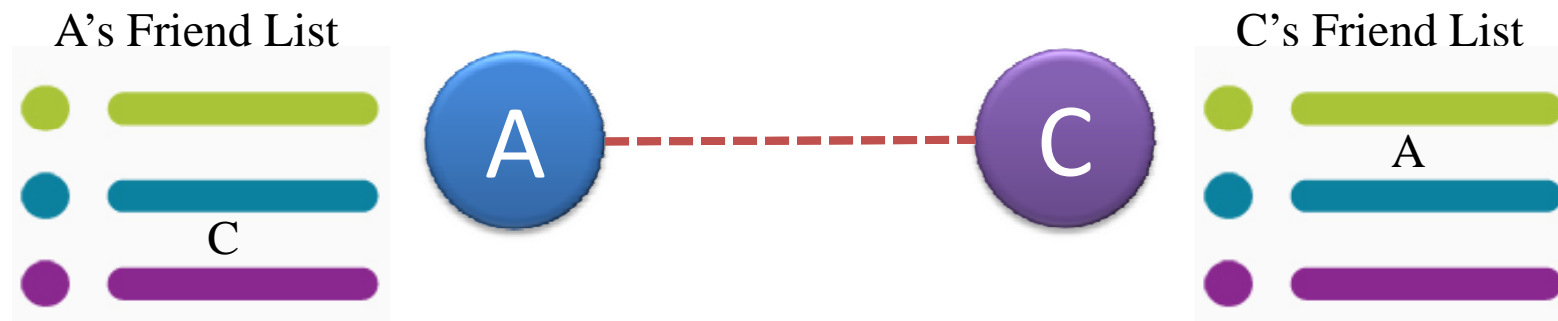
**Consistent  
Among  
Users?**





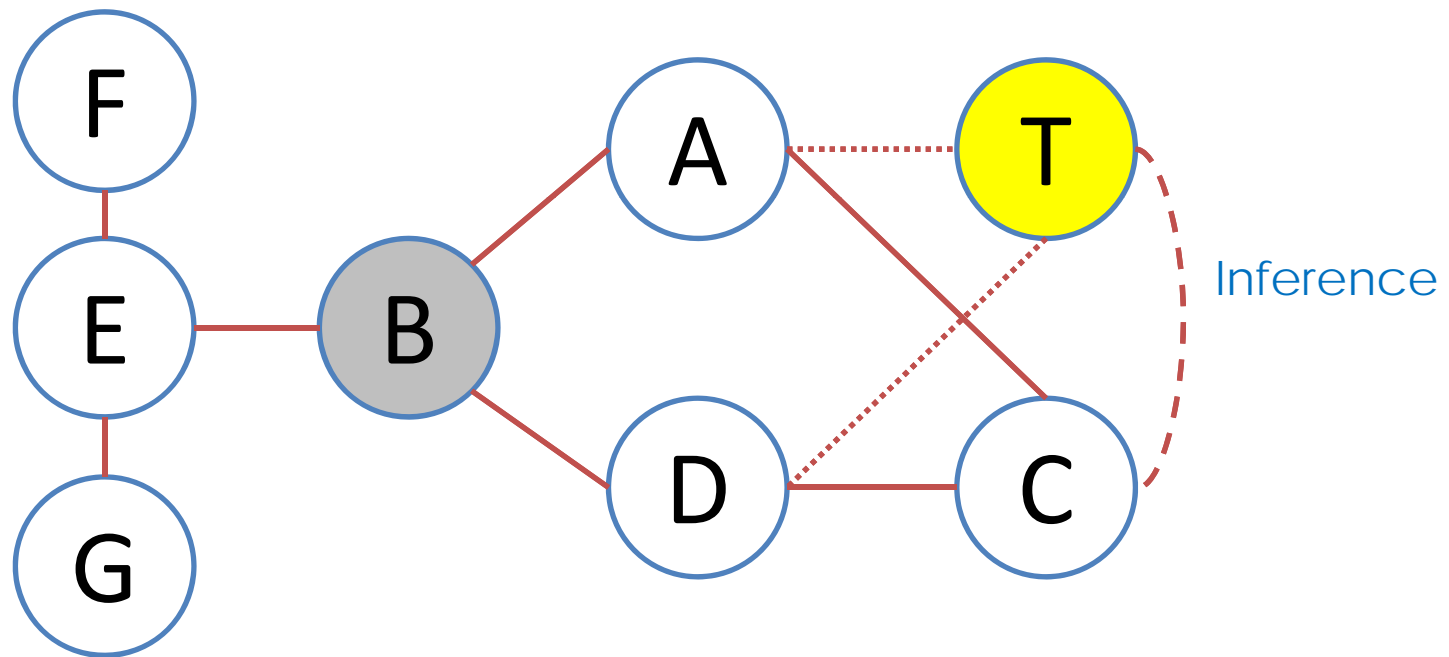


# Inconsistent Policies



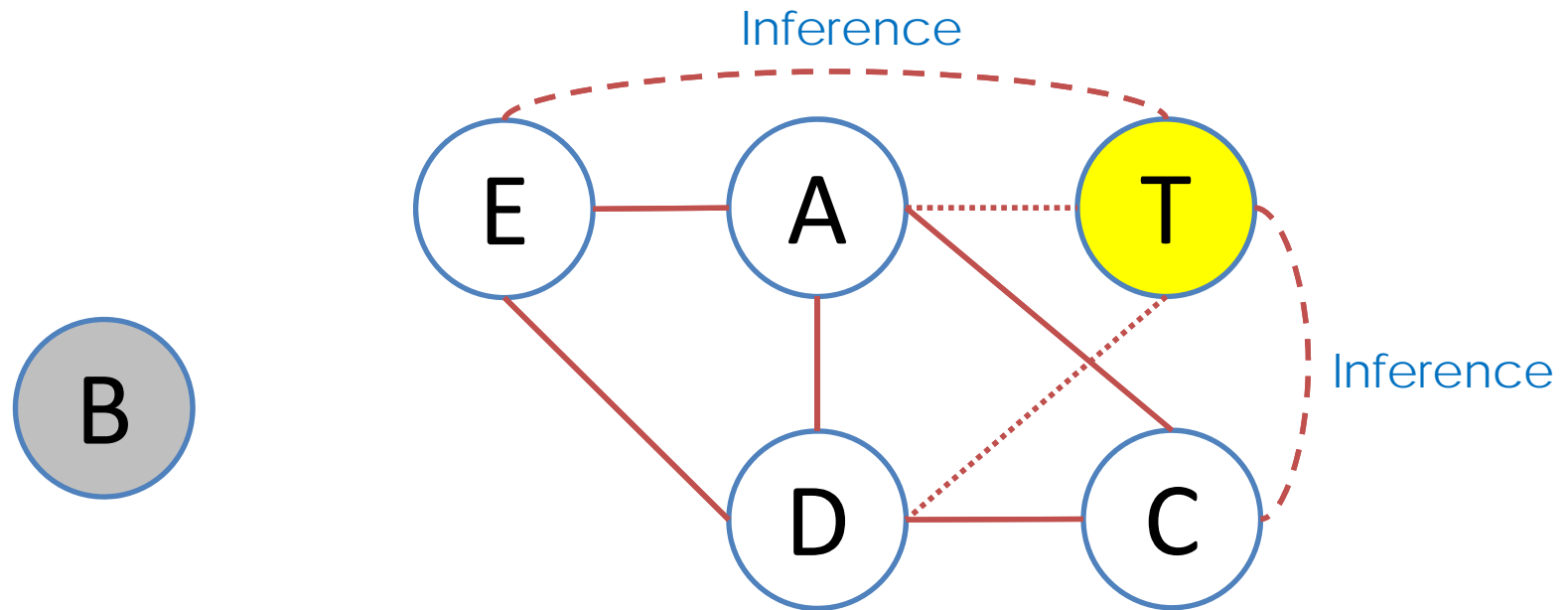


## Inconsistent Preferences Example -1





## Inconsistent Preferences Example -2





# Key Issue

- How to conduct effective inferences to identify the private friendships
  - Guess
  - Similarity-based inferences
  - Random-walk inferences





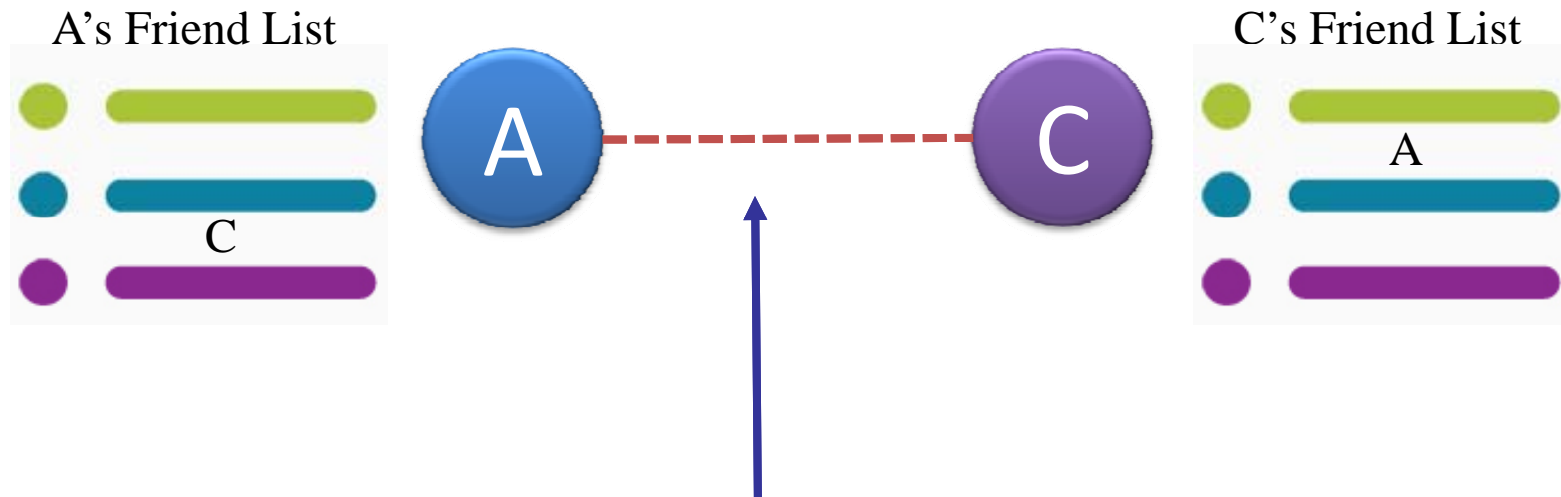
# Attack Schemes



- **One attacker node & one target**
  - ❖ Adversary chooses a number of users, who are the most likely to be friends of a target, at one time based on the calculations
- **Multiple attacker nodes & one target**
  - ❖ Combine the attack knowledge (segments of the network) from different attacker nodes to be a more completed segment of the network
- **Topology of the entire social network (multiple attacker nodes & multiple targets)**
  - ❖ Attack the most vulnerable targets first



# Defense Approaches



- Squicciarini et al. -> voting algorithm & game theory
- Hu et al. -> Label Privacy Level, minimize privacy risk & sharing loss



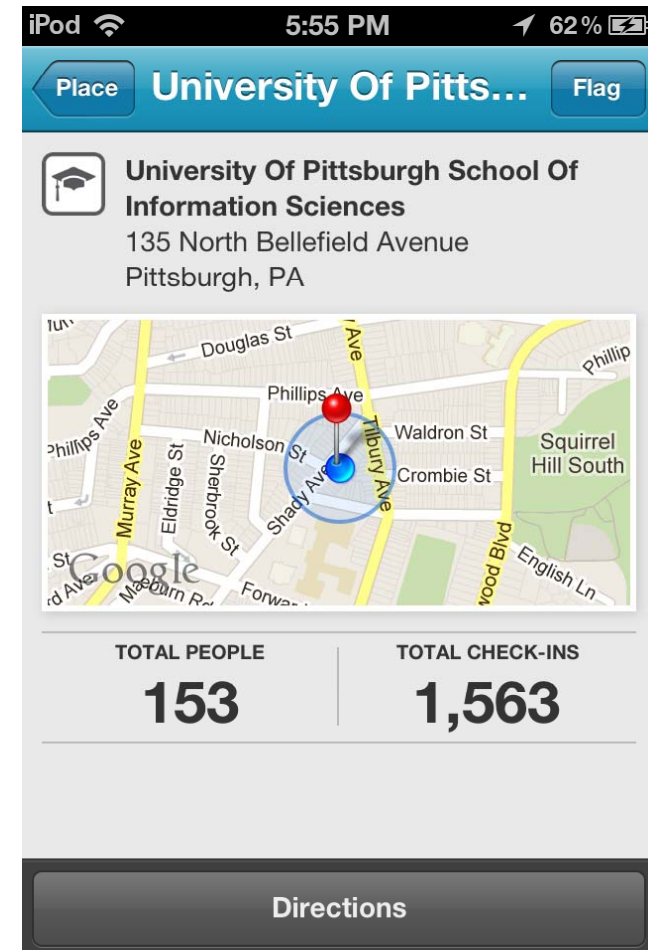
# Outline

- Identity & Authentication Problems
  - Email Address, Connections of Identities & Login
  - Authentication
- Privacy Issues
  - Privacy of User Profiles
  - Privacy of Friendships
- Malicious Resources



# Venue Attacks in LBSNs [15]

- Venue Attributes
  - Creator
  - Owner
  - Name
  - Address
  - Geo-location
  - Category
  - Statistical Information - Owner
  - Promotion/Coupon (Set by Owner)







# Malicious Venue Creation Attack

- **ANY** user can create **ANY** type of a venue without being subjected to any **AUTHENTICATION** and the **AUTHORIZATION** from the actual owner
- Venue Not Created in a LBSN
  - Does not exist in the real world: deceive and confuse users, destroy users' trust for LBSNs
  - Exists in the real world but not willing to share; e.g. home, private place
- Venue Already Created in a LBSN
  - Create a similar venue using a similar/alternative name; e.g., School of Information Sciences - iSchool



# Venue Ownership Hijacking Attack

- Bypass the owner authentication process & become the owner of the created venue
- Owner Authentication in Foursquare, Yelp and Facebook Place
  - Phone number
  - Address
- Impacts
  - Expose customers' visit information: users' privacy
  - Manipulate coupons/promotions: financial loss and/or destroy user trust on the venue
  - Change the address of the venue
  - ...





# Venue Location Hijacking Attack

- Venue's location is associated with its geo-location not the physical address
- Geo-location is dynamic in terms of possible inaccurate GPS signals
- Location update: the center of all the honest check-ins marked by a LBSN





Users' Honest Check-ins & Marked as Host Check-ins by System



Users' honest Check-ins & Marked as Dishonest Check-ins by System



Users' Dishonest Check-ins & Marked as Honest Check-ins by System



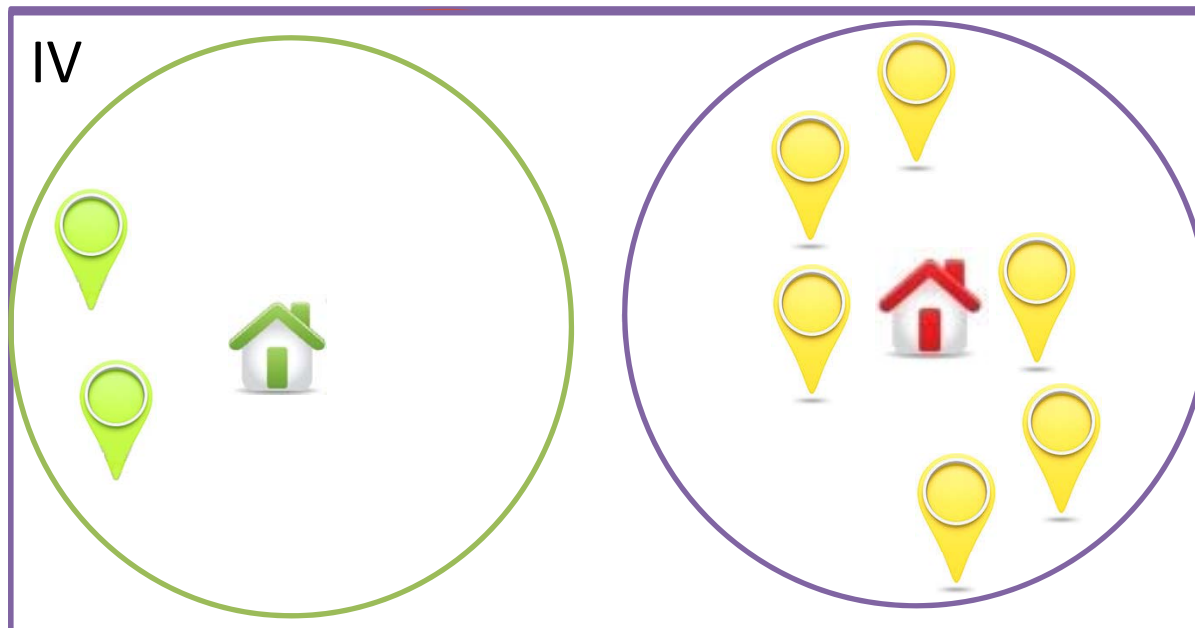
Users' Dishonest Check-ins & Marked as Dishonest Check-ins by System



Actual Location of the Venue

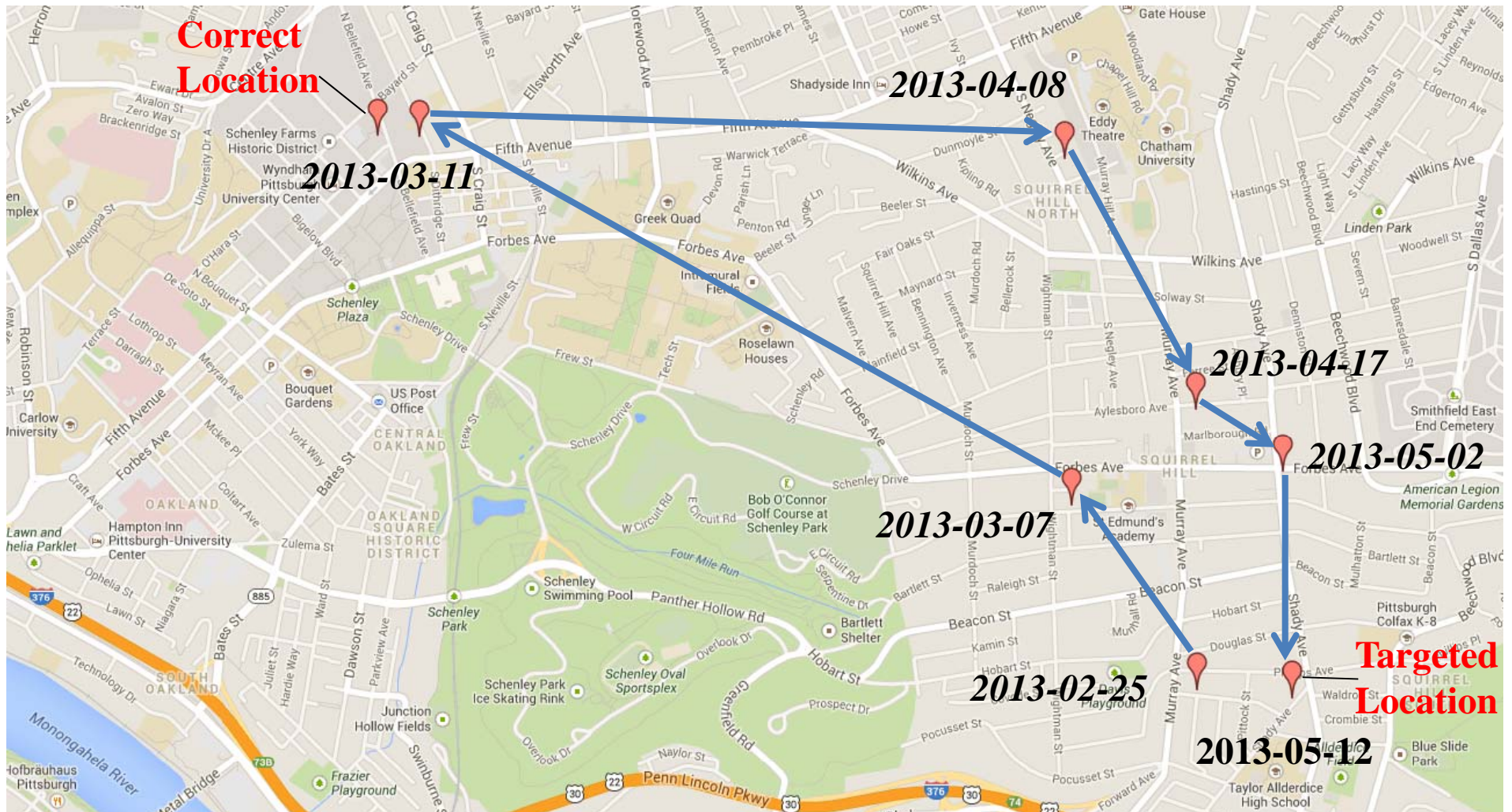


Manipulated Location of the Venue





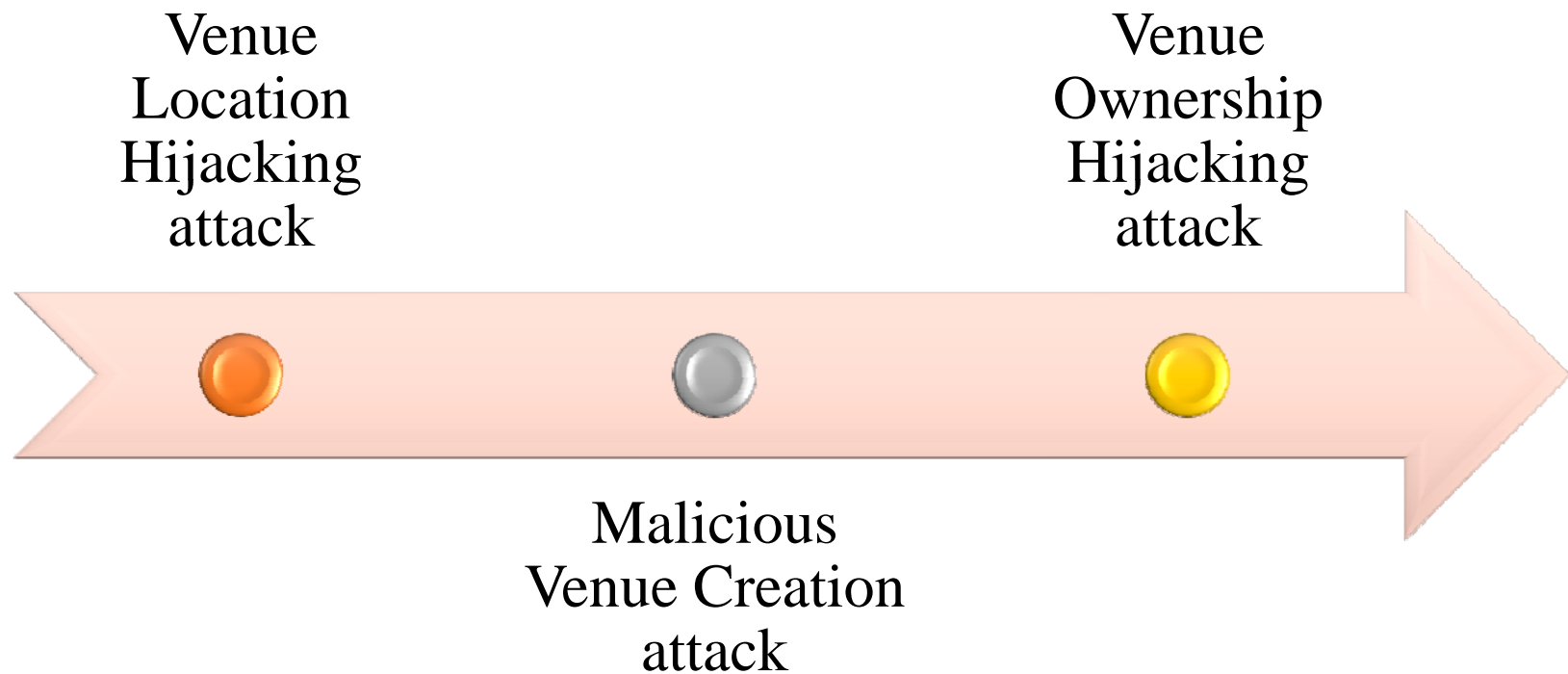
## The Movements of the Locations of the LERSAIS Lab





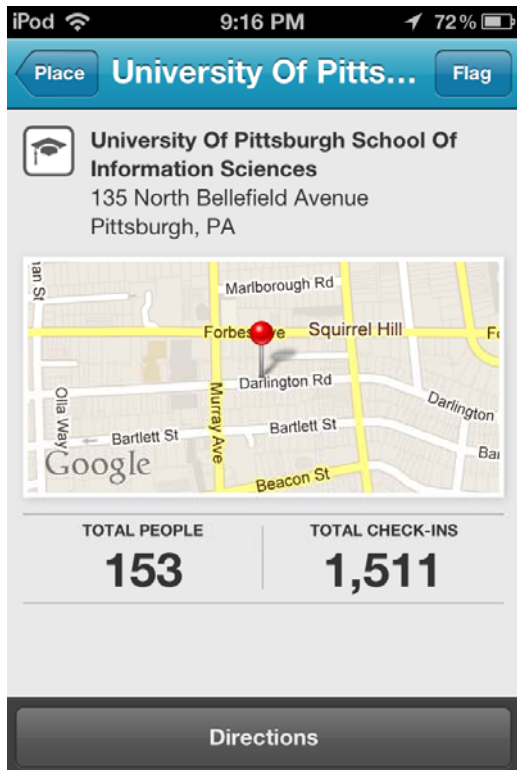


# Combined Venue Attacks

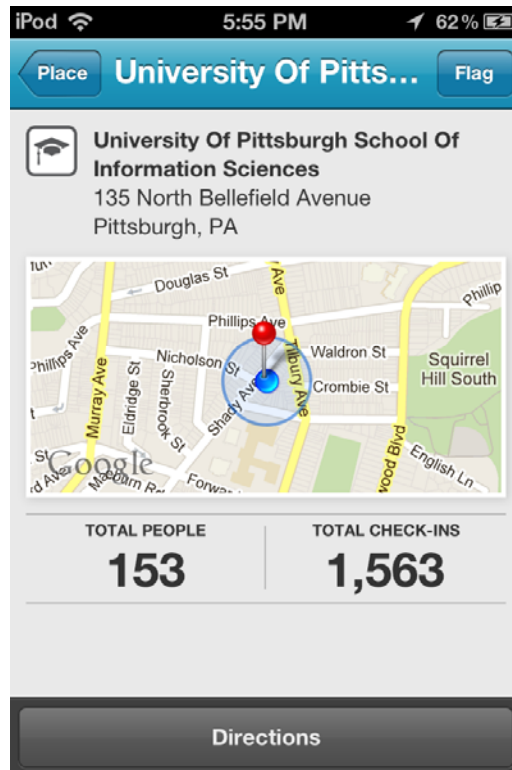




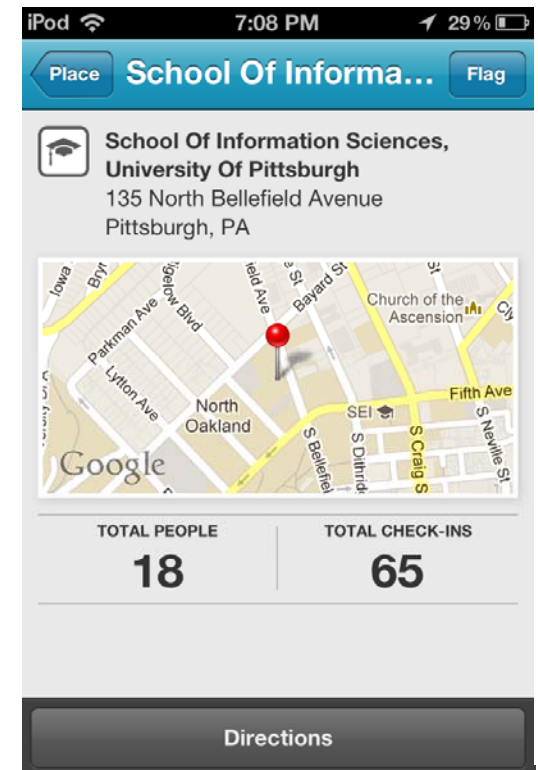
# University of Pittsburgh



**Moved 2 Miles  
away in May,  
2012**



**Moved 3 Miles  
away in July,  
2012**



**New Venue Created  
& Its Check-ins in  
August, 2012**



# References

- 1) Jin, L., Takabi, H., & Joshi, J. B. (2010, August). Security and privacy risks of using e-mail address as an identity. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on* (pp. 906-913). IEEE.
- 2) Yardi, S., Feamster, N., & Bruckman, A. (2008). Photo-based authentication using social networks. In *Proceedings of the first workshop on Online social networks* (pp. 55-60). ACM.
- 3) Kim, H., Tang, J., & Anderson, R. (2012). Social authentication: harder than it looks. In *Financial Cryptography and Data Security* (pp. 1-15). Springer Berlin Heidelberg.
- 4) Polakis, I., Lancini, M., Kontaxis, G., Maggi, F., Ioannidis, S., Keromytis, A. D., & Zanero, S. (2012). All your face are belong to us: breaking Facebook's social authentication. In *Proceedings of the 28th Annual Computer Security Applications Conference* (pp. 399-408). ACM.
- 5) Polakis, I., Ilia, P., Maggi, F., Lancini, M., Kontaxis, G., Zanero, S., ... & Keromytis, A. D. (2014, November). Faces in the distorting mirror: Revisiting photo-based social authentication. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 501-512). ACM.
- 6) Jain, S., Lang, J., Gong, N. Z., Song, D., Basuroy, S., & Mittal, P. (2015). New Directions in Social Authentication. NDSS Workshop on Usable Security.
- 7) Jin, L., Takabi, H., & Joshi, J. B. (2011, February). Towards active detection of identity clone attacks on online social networks. In *Proceedings of the first ACM conference on Data and application security and privacy* (pp. 27-38). ACM.





## References

- 8) Li, L., Zhao, X., & Xue, G. (2012, May). An identity authentication protocol in online social networks. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (pp. 28-29). ACM.
- 9) Zhao, X., Li, L., & Xue, G. (2011, December). Authenticating strangers in fast mixing online social networks. In *Global Telecommunications Conference (GLOBECOM 2011)*, 2011 IEEE (pp. 1-5). IEEE.
- 10) Mislove, A., Viswanath, B., Gummadi, K. P., & Druschel, P. (2010, February). You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining* (pp. 251-260). ACM.
- 11) Jin, L., Long, X., & Joshi, J. B. (2012, October). Towards understanding residential privacy by analyzing users' activities in foursquare. In *Proceedings of the 2012 ACM Workshop on Building analysis datasets and gathering experience returns for security* (pp. 25-32). ACM.
- 12) Jin, L., Long, X., Joshi, J. B., & Anwar, M. (2012, August). Analysis of access control mechanisms for users' check-ins in Location-Based Social Network Systems. In *Information Reuse and Integration (IRI), 2012 IEEE 13th International Conference on* (pp. 712-717). IEEE.
- 13) Jin, L., Joshi, J. B., & Anwar, M. (2013). Mutual-friend based attacks in social network systems. *Computers & security*, 37, 15-30.
- 14) Jin, L., Takabi, H., Long, X., & Joshi, J. (2014, November). Exploiting Users' Inconsistent Preferences in Online Social Networks to Discover Private Friendship Links. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (pp. 59-68). ACM.
- 15) Jin, L., & Takabi, H. (2014, November). Venue attacks in location-based social networks. In *Proceedings of the 1st ACM SIGSPATIAL International Workshop on Privacy in Geographic Information Collection and Analysis* (p. 1). ACM.



**Questions?**

**Thank You!**