Mobile Security
14-829 – Fall 2013

Patrick Tague

Class #22 – Location Privacy

Carnegie Mellon University
Silicon Valley

Exam

In-class Nov 18

- Q: What's on the exam?
- A: I don't know. I haven't made it yet.

- Q: What will the exam be like?
- A: Conceptual questions that test your understanding of the main ideas covered in class
  - Sample exam on Blackboard
  - Coverage may include anything through Nov 13 other than project presentations

- Q: What resources can I use during the exam?
- A: Open notes, open book. No electronics.

- Q: Will notes and books help me?
- A: Probably not.

Questions about the exam?

We previously discussed location and privacy practices, but now let's talk about location privacy specifically

Location Privacy

- Outline of location privacy topics covered:
  - Values of location disclosure (location-based services)
  - Risks of location disclosure
  - Location inference

Location-Based Services

- Delivery of a service (or information) at the point of need based on requester's location
- Provide personalized services based on customer requirements or requests
- Significantly increase quality of service

Example LBS

- Location-based traffic reports:
  - What are the traffic conditions on the highway?
  - What is the estimated travel time to reach home?
- Location-based retail locator:
  - What restaurants are within five miles of me?
  - Where is the nearest pizza place?
- Location-based advertisement:
  - Send e-coupons to my customers within a mile

Location-Based Social Nets

- Social recommendations using location
  - Several location-based recommendation systems can be built using your social circles
- Local businesses
  - Mobile devices can inform users of businesses within a specified distance
- Location-based reminders
  - Leave reminders for friends of interesting locations
- Friend locator
  - Alert user when their friends are nearby or at a point of interest

What are the risks of LBS?

PLEASE ROB ME

Raising awareness about over-sharing

Check out our guest blog post on the CDT website.

Why

Hey, do you have a Twitter account? Have you ever noticed those messages in which people tell you where they are? Pretty annoying, eh. Well, they're actually also potentially pretty dangerous. We're about to tell you why.

More Info

Home

Why

Made Possible By

Privacy Concerns

- Expose user locations
  - Trivial algorithms can expose sensitive location using anonymized GPS traces collected by LBS
  - Identify visits to clubs, hospitals, or embarrassing locations
- Re-identification
  - Device location often → user identity
    - Reverse white page lookups + anonymized GPS traces
    - Additional, often available information such as birthday, gender, or other traits further support identification
- Even sporadic location information is enough due to low entropy in human mobility

Further Impacts

- Lost / stolen / compromised phone:
  - Can leak location privacy of user and social contacts
  - Informing friends that your device is lost?

- Compromised storage server:
  - Data leakage – encrypted database?
  - Attacker can monitor incoming data / connections

How to protect location data?

Ways to Preserve Loc. Privacy

- Many mobile applications available to protect location information
  - AnonySense, SmokeScreen, MockDroid, etc.
- Decentralized social networks
  - Musubi: users own their content and and context info choose who to share it with
- Stronger trust models, data secrecy, etc.
- Social sharing policies
  - Strict access control policies, data sharing, visualization tools, etc.

Leakage Protection/Detection

Methodology	Advantage	Disadvantage
Permissions / policies	Light-weight	Fine-grained vs. scalable
Static analysis tools	Easy to scale up	Miss runtime behaviors
Dynamic analysis tools	Detection accuracy	Computational load and complexity
Privacy mode	Flexible	User dependence, often low usability

Permission & Policy Mgmt.

- Kirin
  - Allows definition of sensitive information permissions and policies
- XManDroid
  - Tracks communication and information flow between components in different applications
  - Can create and enforce policies like:
    - “An application that can obtain location information must not communicate [directly or indirectly] with an application that has network access.”

Static Analysis Tools

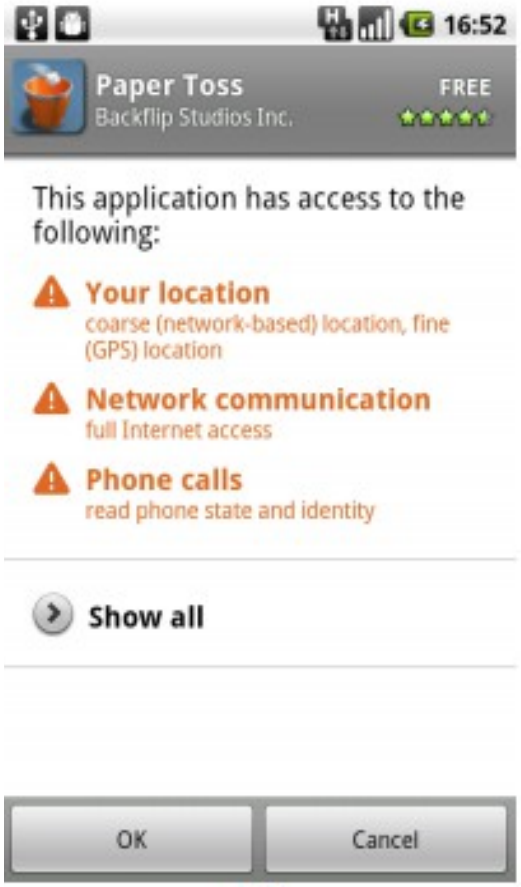
- Static analysis can be used to (partially) understand what an application is doing with collected information
  - ComDroid
  - APKInspector
- How to understand if a leak is acceptable / reasonable vs. malicious / unacceptable?

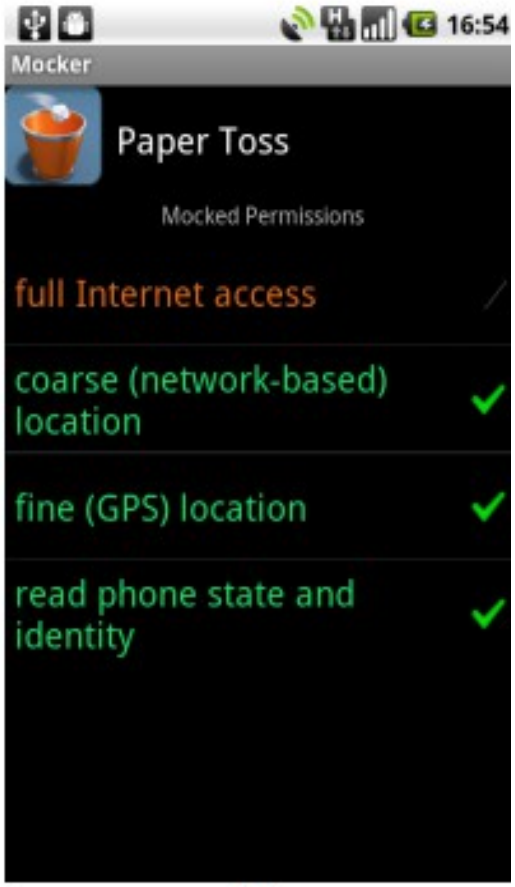
Dynamic Analysis Tools

- Dynamic analysis can capture more of the runtime behavior that static analysis misses
  - TaintDroid
  - Appfence
- How to characterize the location privacy leak?
- How to generate test input and control behavior conditions?

Privacy Mode

- MockDroid / TISSA
  - Package manager modification to mock permissions





Privacy Mode

- Locaccino
  - Uses privacy controls and explicit location UIs to provide locator services

How to understand usability concerns?

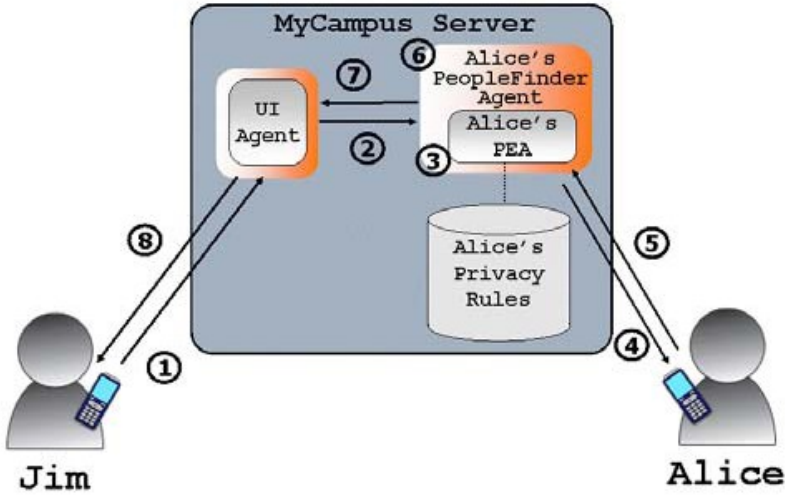
PeopleFinder Case Study

- PeopleFinder: app to allow friends/colleagues to figure out where you are, using phone/computer
- Goal of study:
  - Understand people's attitudes / behaviors around location privacy
  - Develop a usable approach to managing privacy prefs.
- Methodology:
  - Built around observations from various user studies, both for design and testing

Challenges

- People have diverse privacy preferences
  - Are there a small number of profiles that cover?
- Can we expect people to specify privacy prefs?
- Do people understand their privacy prefs?
- Can we learn people's preferences by observing their behavior?

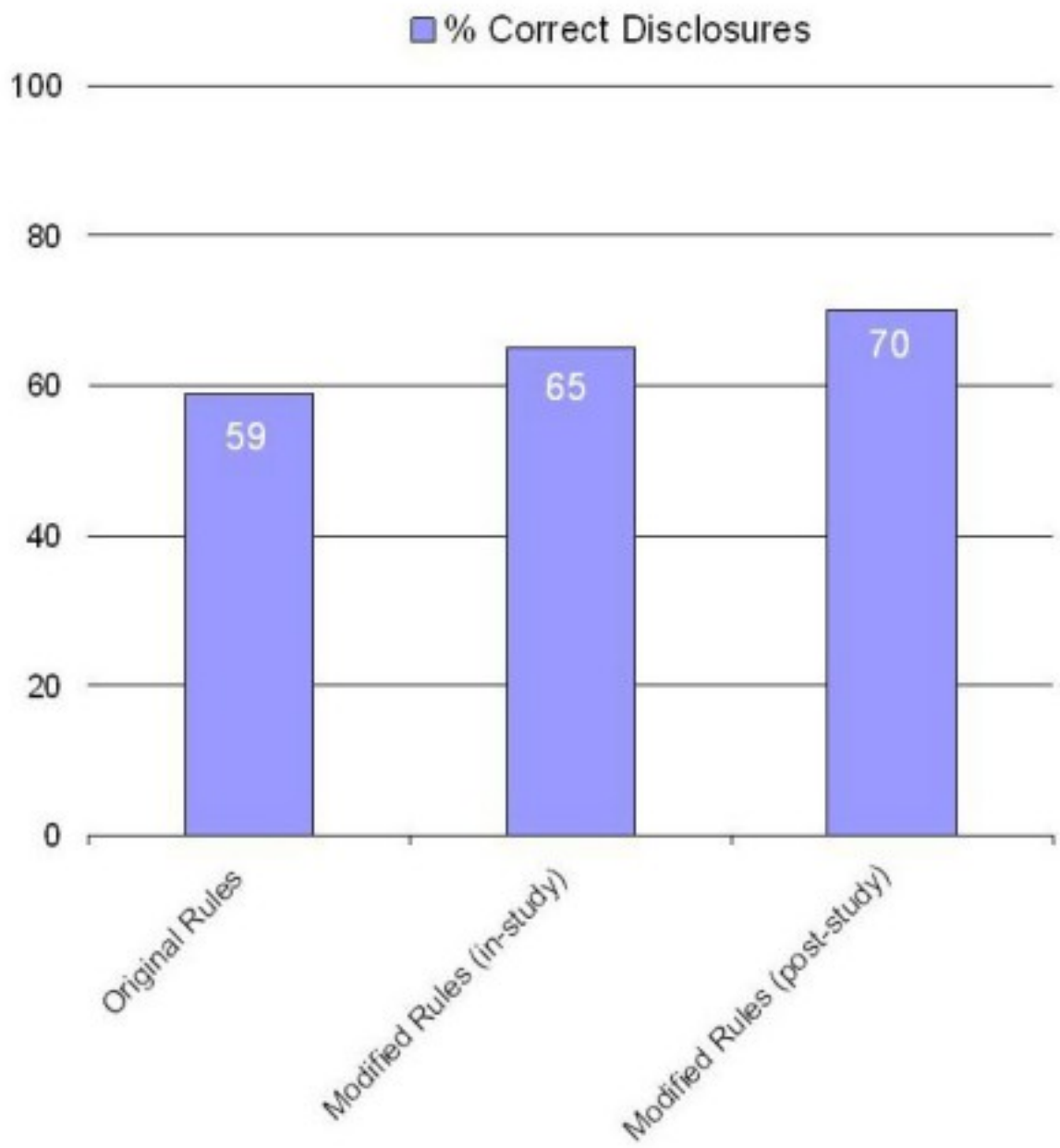
PeopleFinder



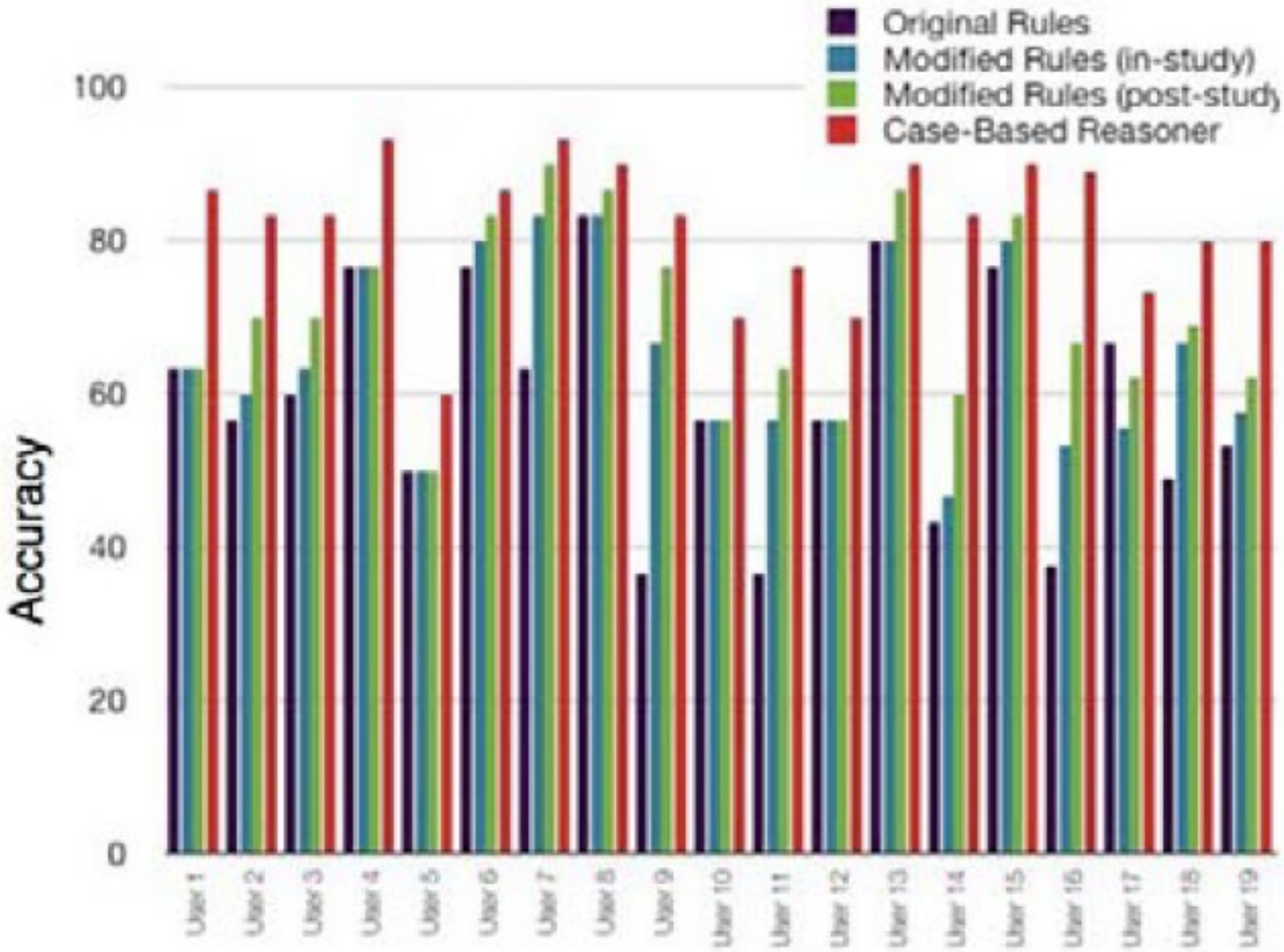
Requesting user

Target user

- Initial … d:
  - Use … y prefs
  - Aud … user incr … ining
  - Use … olicies
  - Mac … le evolve poli …



Improvement using ML



Conclusions of the Study

- PeopleFinder studies found:
  - People will only adopt location-based mobile apps if they feel they have adequate control over their location privacy
  - People have complex privacy preferences
    - They are not good at specifying their policies
    - Their preferences / policies change over time
    - Not easy to identify good default policy sets other than a default “deny all” policy
  - Auditing is critical
    - Learning and explaining disclosure decisions are helpful in guiding people to the policy that fits their preferences

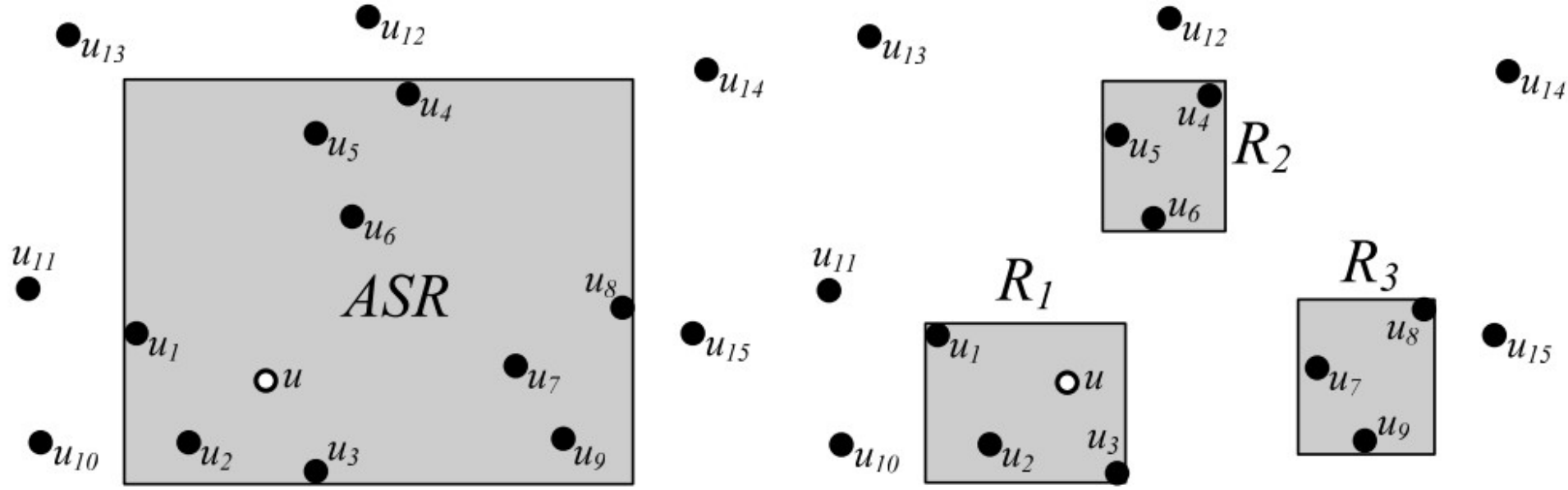
What if users just want to provide access to partial location information?

Location Anonymity

- Spatial cloaking
- Temporal cloaking
- Spatiotemporal cloaking

Spatial Cloaking

- Spatial cloaking is an attempt to reduce the location granularity and mix users into indistinguishable groups



(a) Single ASR (k=10) (b) Multiple ASRs (k=10)

[Tan, Lin, and Mouratidis, 2009]

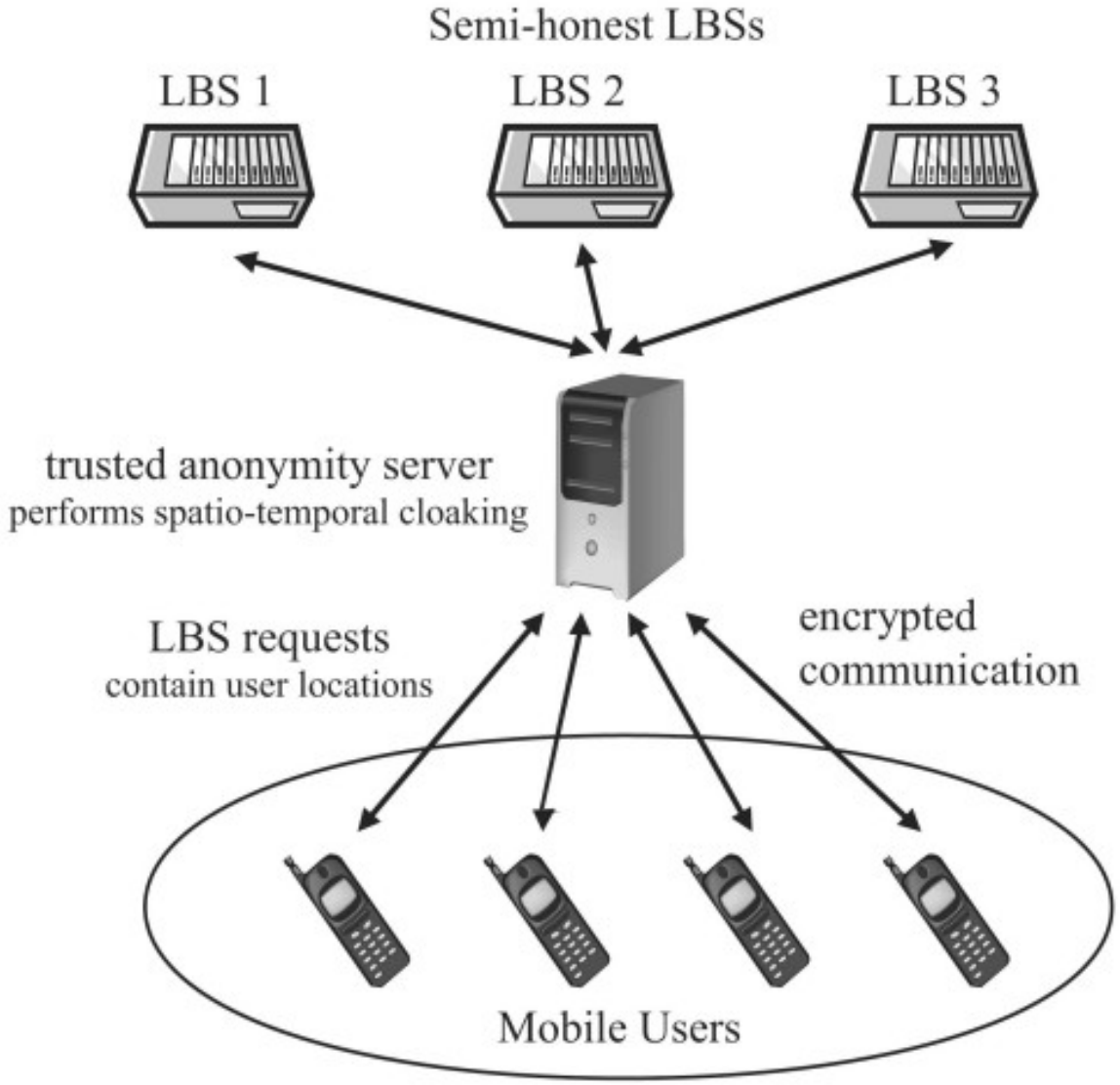
(Spatio)Temporal Cloaking

- Temporal cloaking takes a similar approach, only reducing the temporal resolution
  - Effectively replacing a time-stamp with an interval
  - Larger interval → lower temporal resolution → higher location anonymity → better location privacy

- Spatiotemporal combines both:
  - <x,y,t> → <[x1,x2],[y1,y2],[t1,t2]>

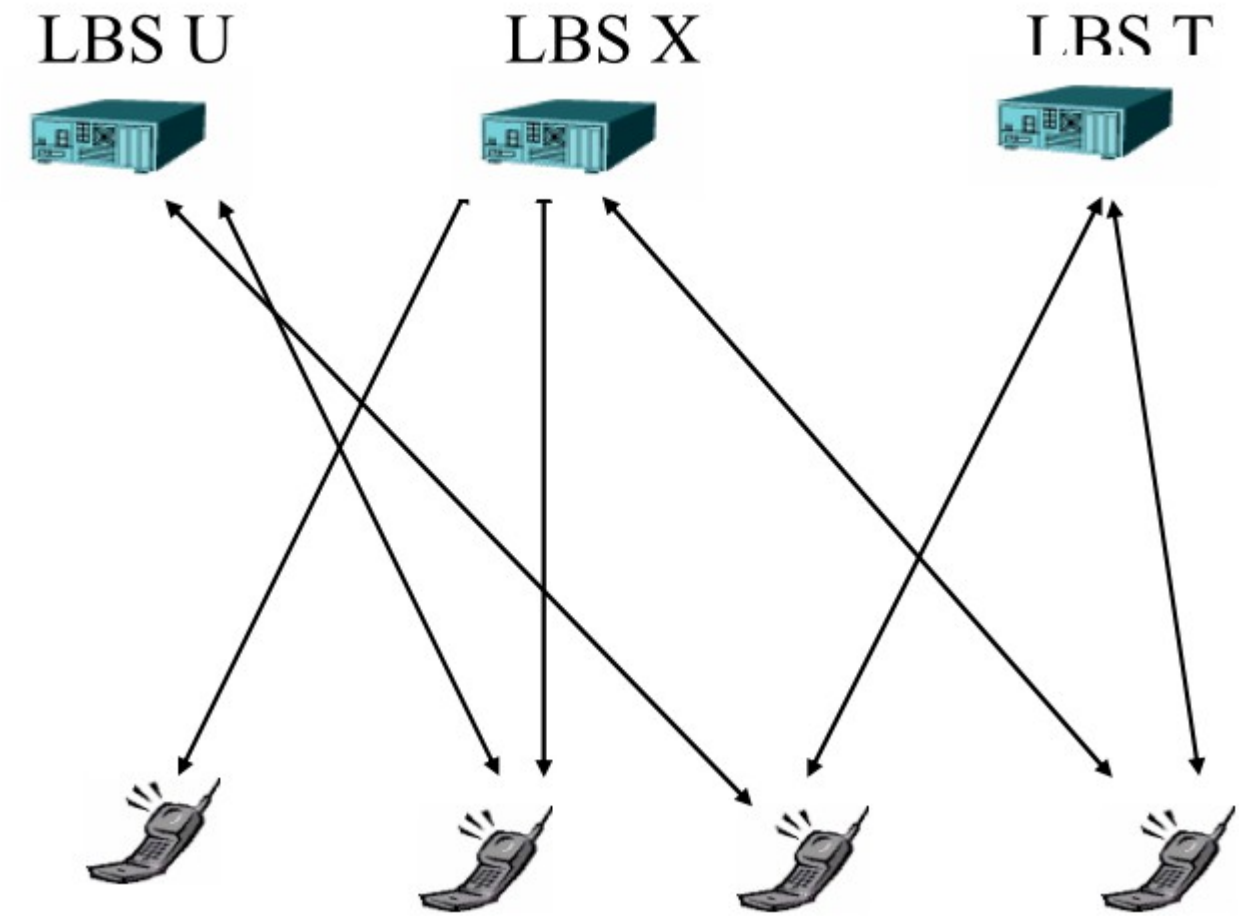
Location Anonymization

[Gedik and Liu, TMC 2008]



Client-side Anonymization

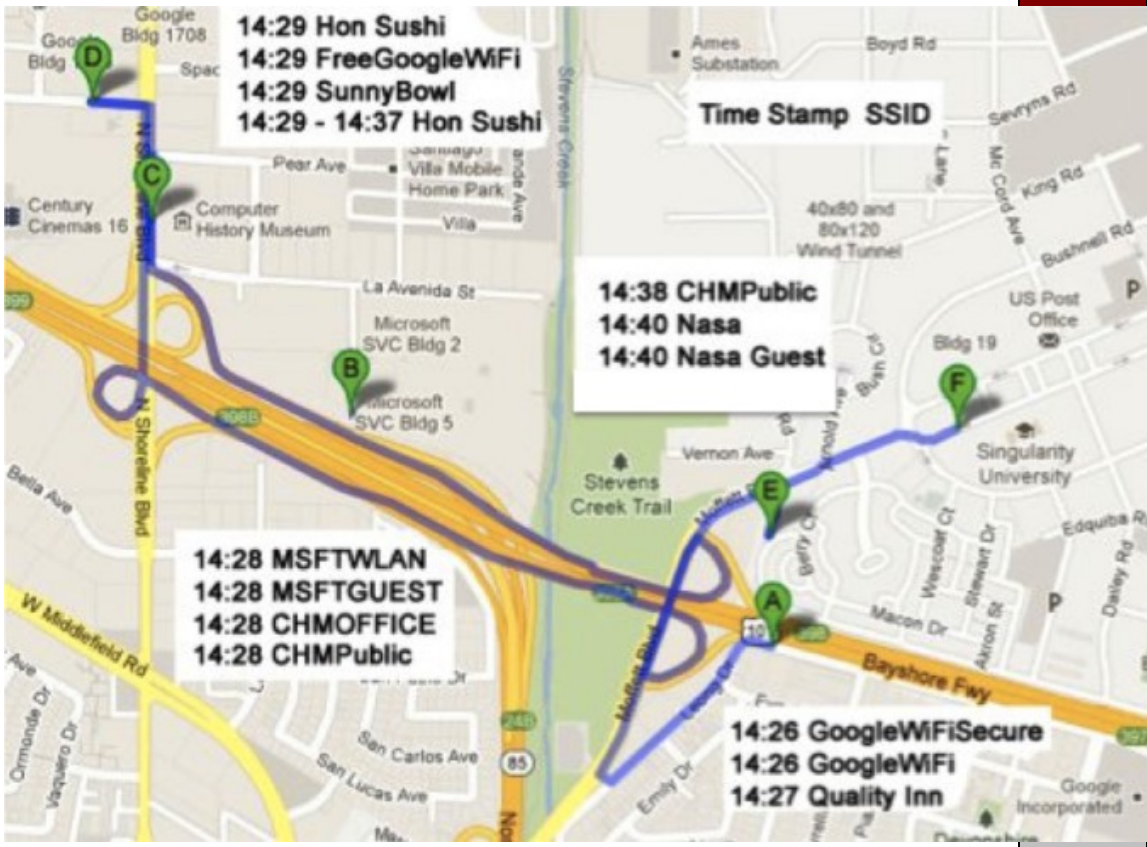
[Liu, VLDB 2007]



What about apps that learn location information without permission?

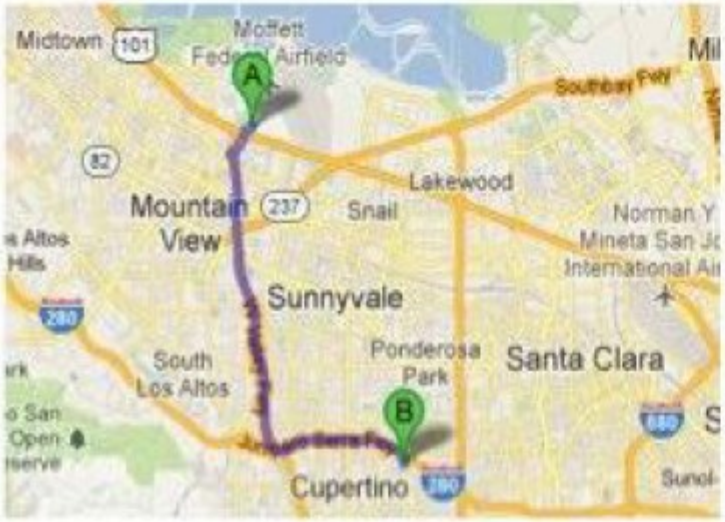
Other Location Resources

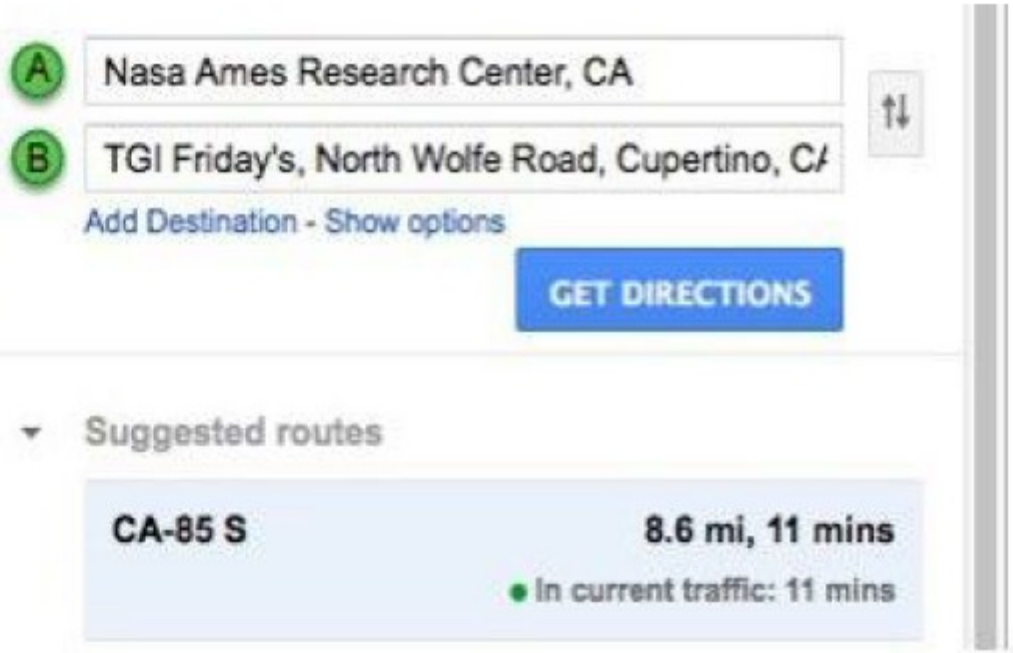
- Smartphones have a lot of resources available that can expose information related to location
  - Timestamped WiFi SSIDs
  - Contact log
  - Phonebook
  - SMS history
  - Social network data
  - Calendar



Timestamped SSIDs

```
18:19, SSID: SingularityUniversity, BSSID:
18:19, SSID: nasa-guest, BSSID: 00:24:6c:d0
18:19, SSID: nasa, BSSID: 00:24:6c:d0:c8:a2
18:20, SSID: GoogleWiFiSecure, BSSID: 00:0c
18:21, SSID: Quality Inn, BSSID: 00:26:f2:b
18:24, SSID: GoogleWiFiSecure, BSSID: 00:0c
18:30, SSID: TGI Friday's, BSSID: 58:6d:8f:
18:31, SSID: Dyansty Guest, BSSID: c0:3f:0e
```





Question to consider:

How to protect against unauthorized location inference?

Nov 13:
BYOD

Nov 18:
Exam