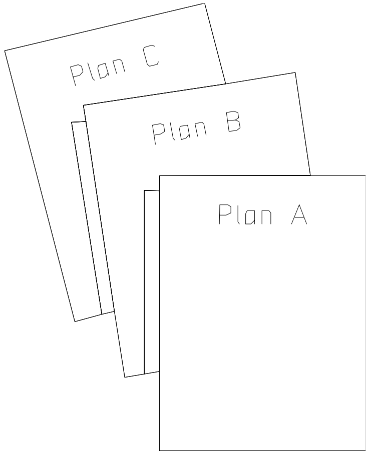
Location Privacy

Overview

- Objective
  - To understand privacy threats with the example of location data

- Content
  - Intro to location privacy
  - K-anonymity
  - CacheCloak [MobiCom 2019]



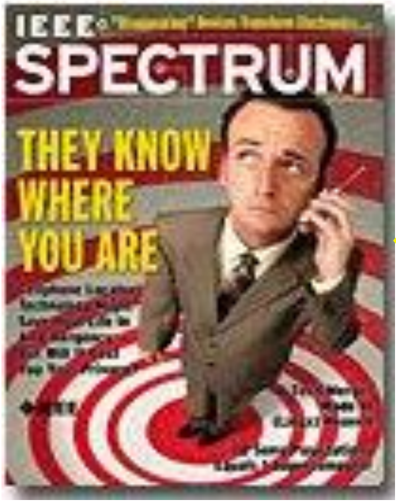
- After this module, you should be able to
  - Understand the concept of location privacy and a few techniques to protect it.

PRIVACY
●●●●●●●●●
ENTER

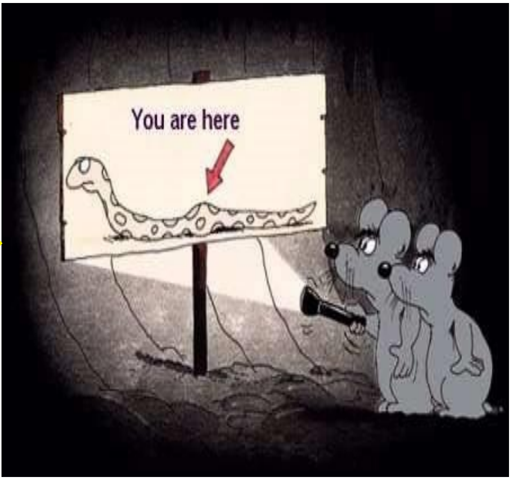
Examples of Private Data Access

- Network service providers
  - monitor incoming and outgoing calls, text messages, and emails
- Network carriers
  - keep a record of how often you access the internet
- Geo-location tools
  - sense your location and track your movements
- Geo-tagging features on cameras and SNS:
  - mark your location when you take a picture or shoot a video clip
- Websites, social media, and eCommerce platforms
  - keep a record of your personal and account data
- Browser cookies
  - note your login credentials and viewing habits
- Mobile apps
  - log email addresses, contact information, browsing activity, and other data and share with third-party advertising or marketing networks

Location: A Major Privacy Threat



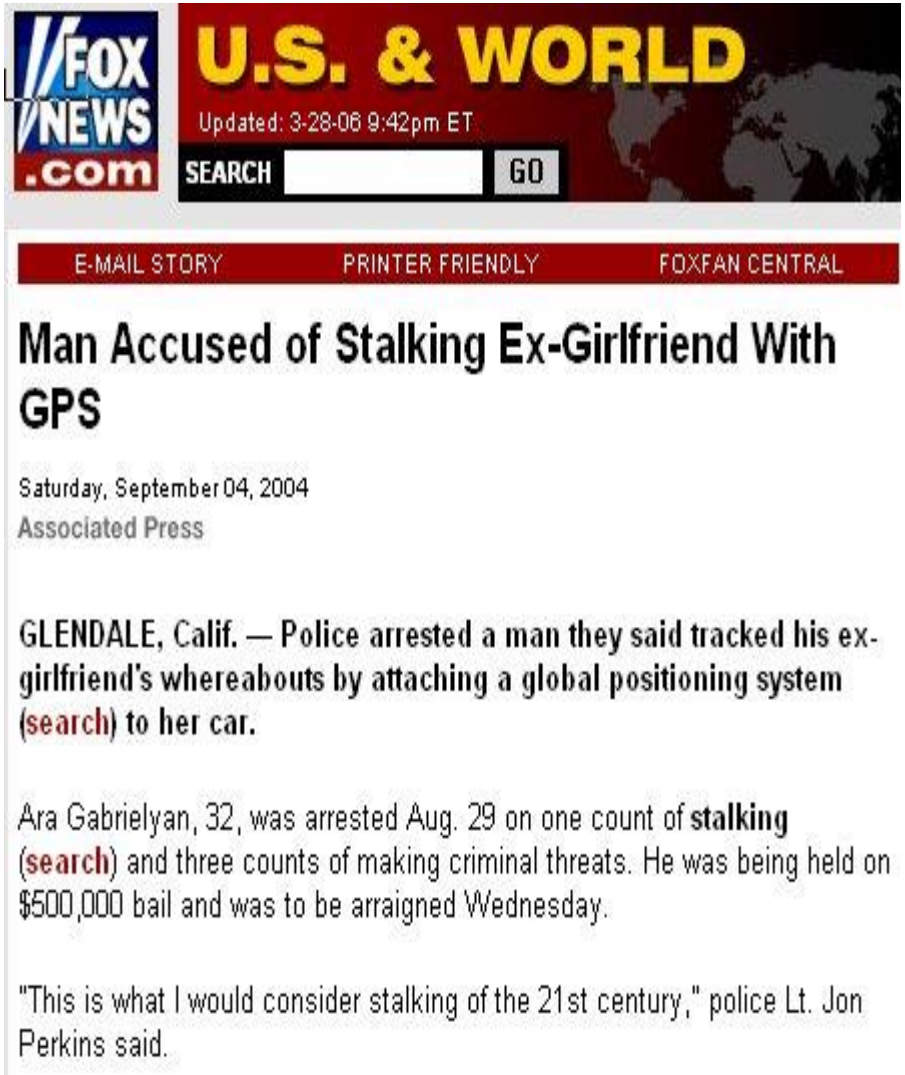
YOU ARE TRACKED…!!!!



"Technologies can pinpoint your location at any time and place. They promise safety and convenience but threaten privacy and security"

Cover story, IEEE Spectrum, July 2003

Example Cases



Man Accused of Stalking Ex-Girlfriend With GPS

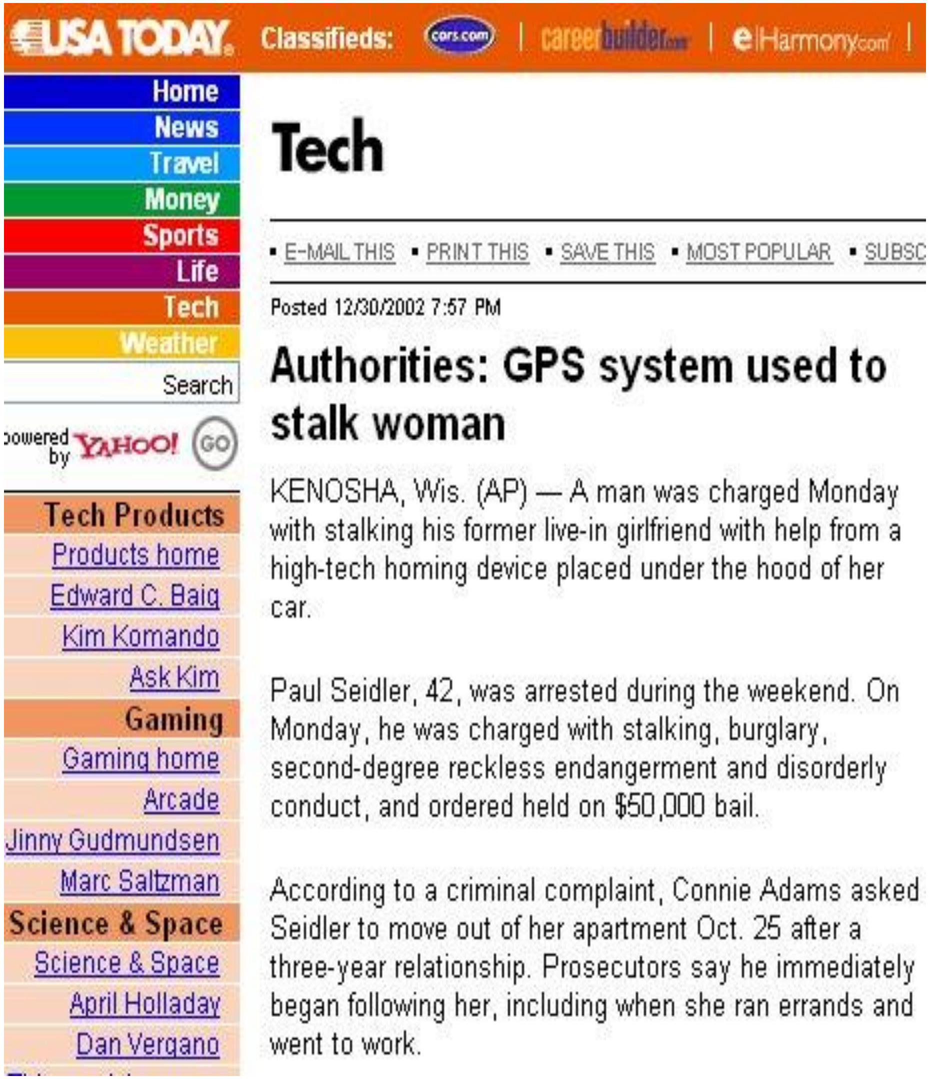
Saturday, September 04, 2004

Associated Press

GLENDALE, Calif. — Police arrested a man they said tracked his ex-girlfriend's whereabouts by attaching a global positioning system (search) to her car.

Ara Gabrielyan, 32, was arrested Aug. 29 on one count of **stalking** (**search**) and three counts of making criminal threats. He was being held on $500,000 bail and was to be arraigned Wednesday.

"This is what I would consider stalking of the 21st century," police Lt. Jon Perkins said.



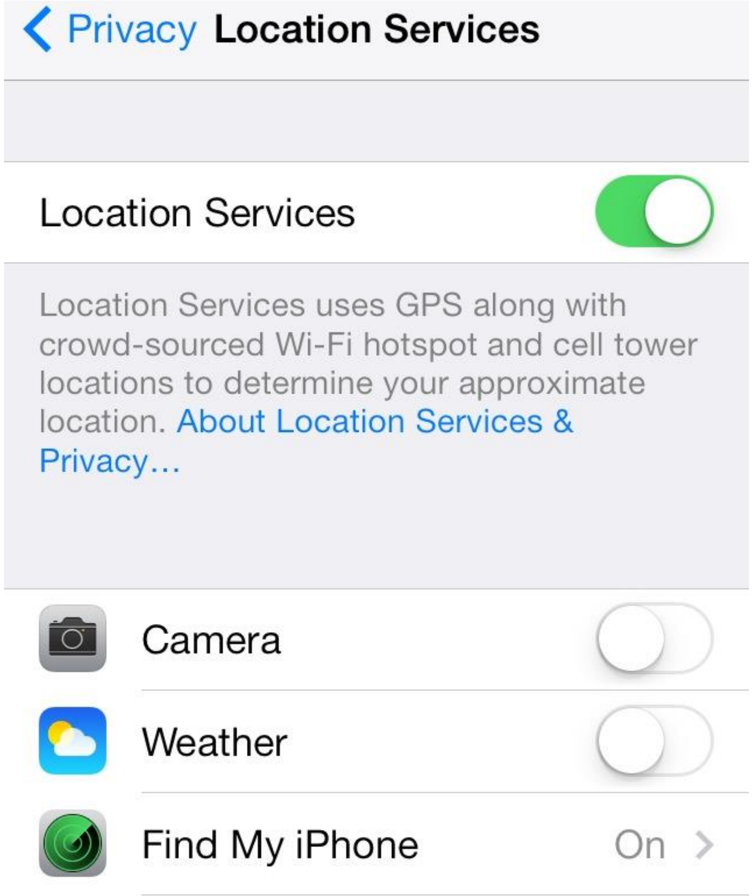
Posted 12/30/2002 7:57 PM

Authorities: GPS system used to stalk woman

KENOSHA, Wis. (AP) — A man was charged Monday with stalking his former live-in girlfriend with help from a high-tech homing device placed under the hood of her car.

Paul Seidler, 42, was arrested during the weekend. On Monday, he was charged with stalking, burglary, second-degree reckless endangerment and disorderly conduct, and ordered held on $50,000 bail.

According to a criminal complaint, Connie Adams asked Seidler to move out of her apartment Oct. 25 after a three-year relationship. Prosecutors say he immediately began following her, including when she ran errands and went to work.


Privacy Location Services

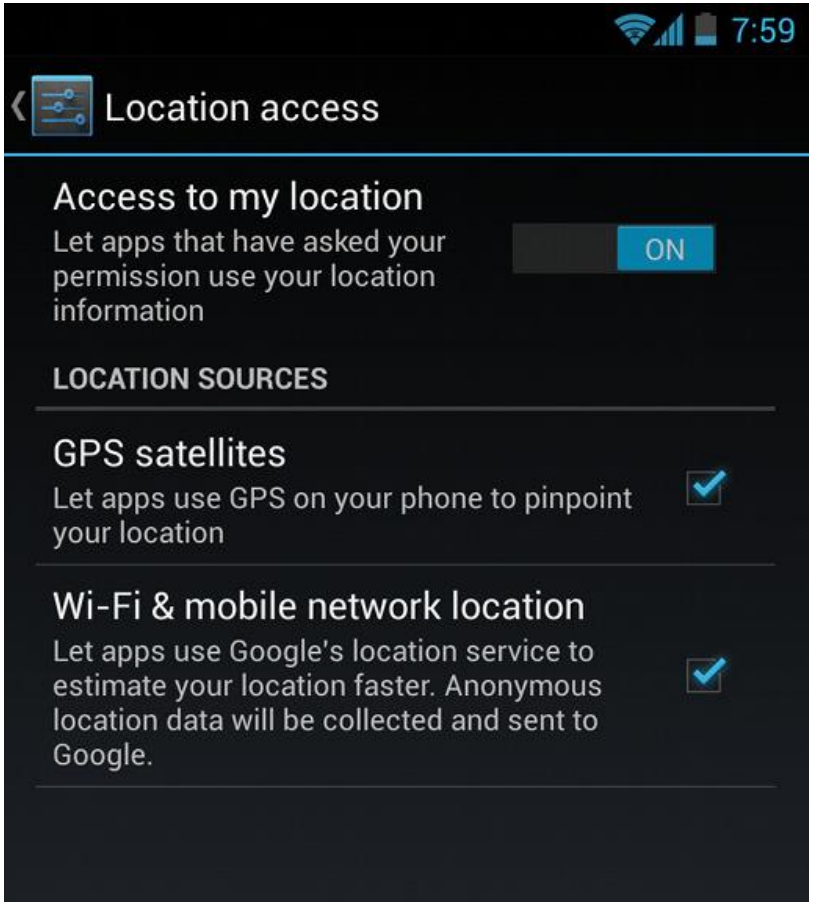
Location Services

Location Services uses GPS along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy…

Camera

Weather

Find My iPhone On


7:59

Location access

Access to my location

Let apps that have asked your permission use your location information

ON

LOCATION SOURCES

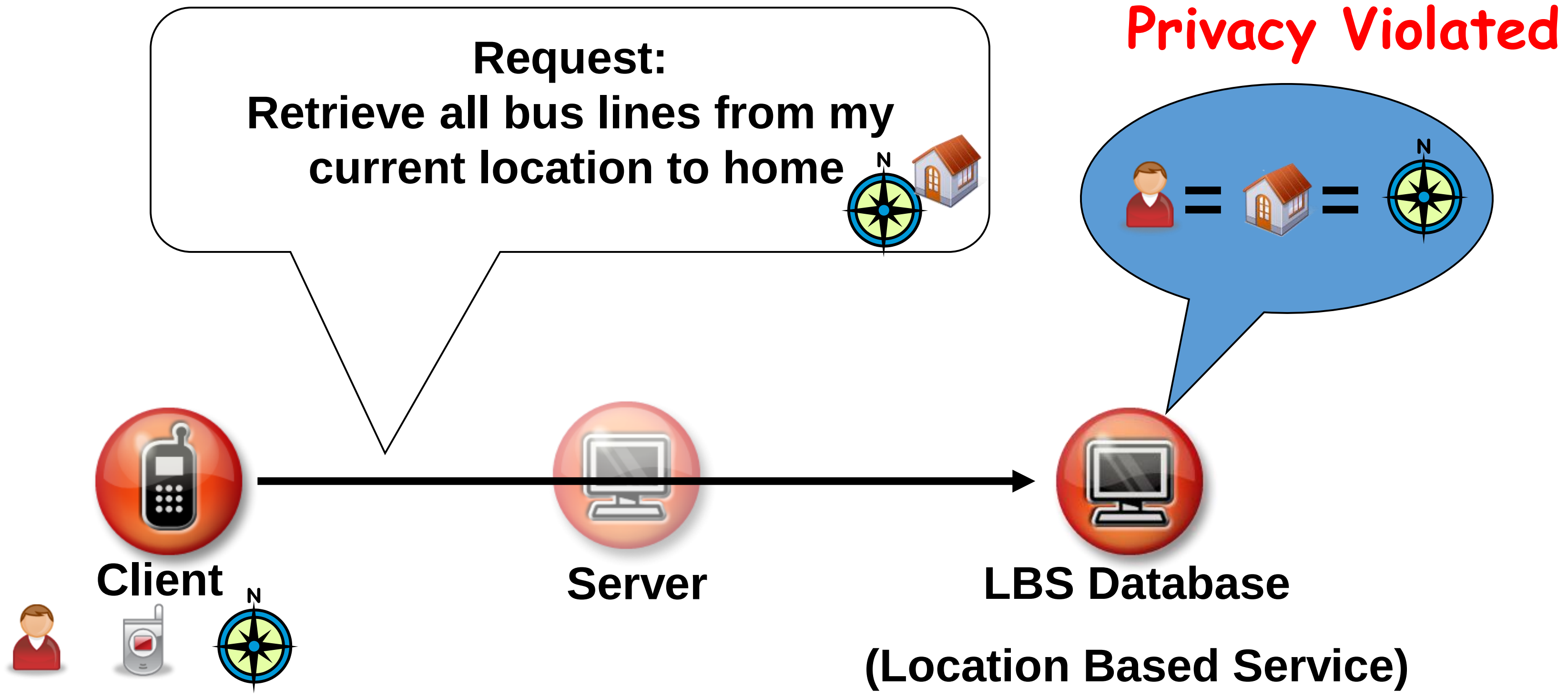
GPS satellites ☑

Let apps use GPS on your phone to pinpoint your location

Wi-Fi & mobile network location ☑

Let apps use Google's location service to estimate your location faster. Anonymous location data will be collected and sent to Google.

Architectural View of Privacy Violation



Request:
Retrieve all bus lines from my current location to home

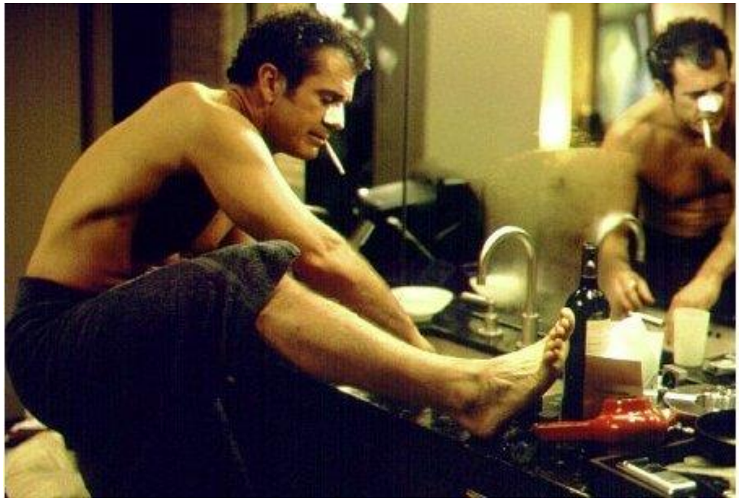
Privacy Violated

Client

Server

LBS Database

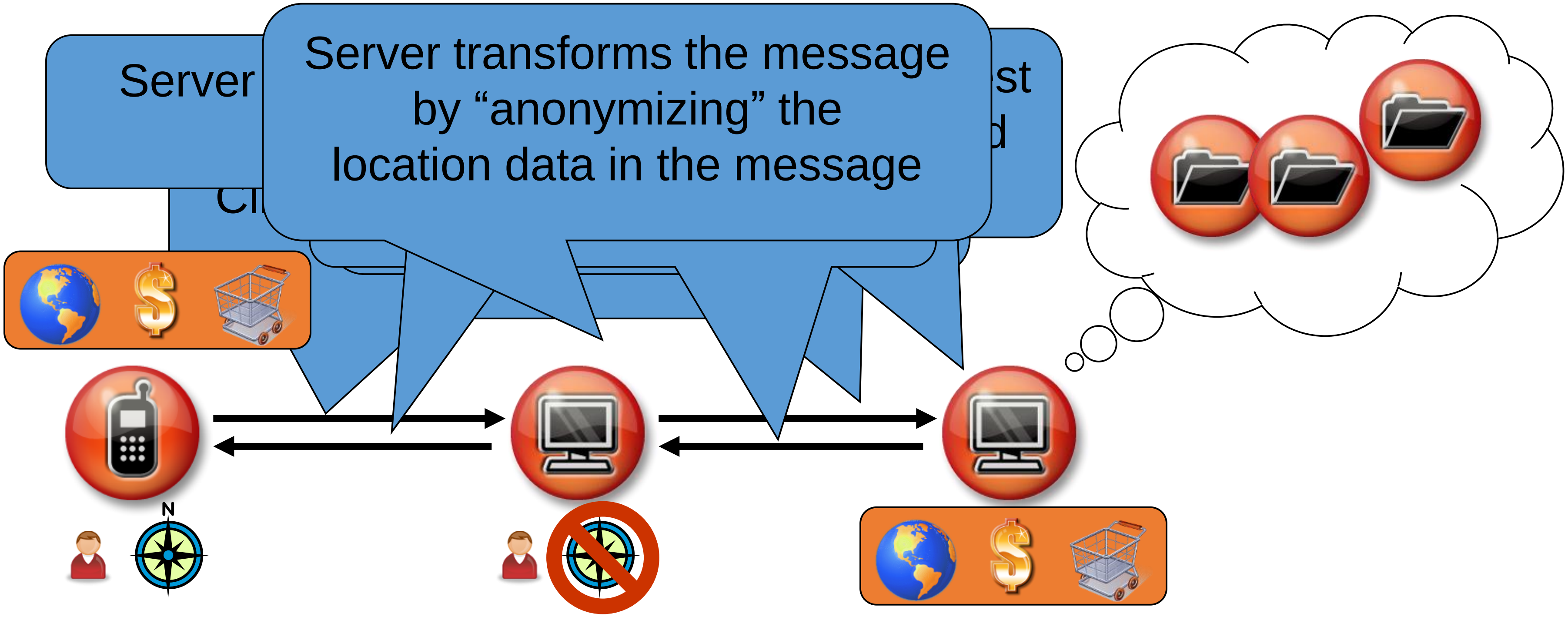
(Location Based Service)



What Users Want

Entertain location-based services
without
revealing their private location information

Implementation of Location Anonymity



Server transforms the message by “anonymizing” the location data in the message

Anonymization of User ID

User 1
(Samsung S4)

date	time	latitude	longitude
03/06/2019	12:00:01	41°24'12.2"N	2°10'26.5"E

User 2
(HTC One)

date	time	latitude	longitude
03/06/2019	12:00:05	41°24'13.2"N	2°10'28.5"E

User 3
(LG G2)

date	time	latitude	longitude
03/06/2019	12:00:07	41°24'17.5"N	2°10‘35.5"E

Encoding User ID

Anonymized
Location
Database

user_id	date	time	latitude	longitude
123456	21/04/2014	12:00:01	41°24'12.2"N	2°10'26.5"E
654321	22/04/2014	12:00:05	41°24'13.2"N	2°10'28.5"E
234567	23/04/2014	12:00:07	41°24'17.5"N	2°10‘35.5"E

Anonymizing ID Sufficient?

- Anonymizing personal IDs may not be sufficient.

- For some users, identity might be easily inferred (e.g., students attending a small-size class).

- Homes and works are often easily identified and can be mapped to the identity.

Service-Privacy Trade-off

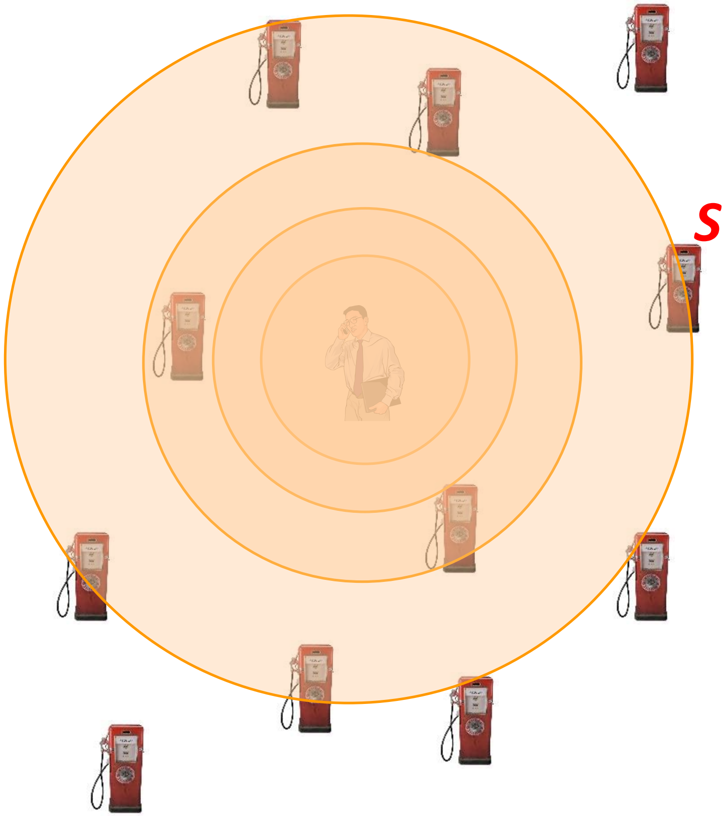
- First extreme:
  - A user reports her exact location → 100% service

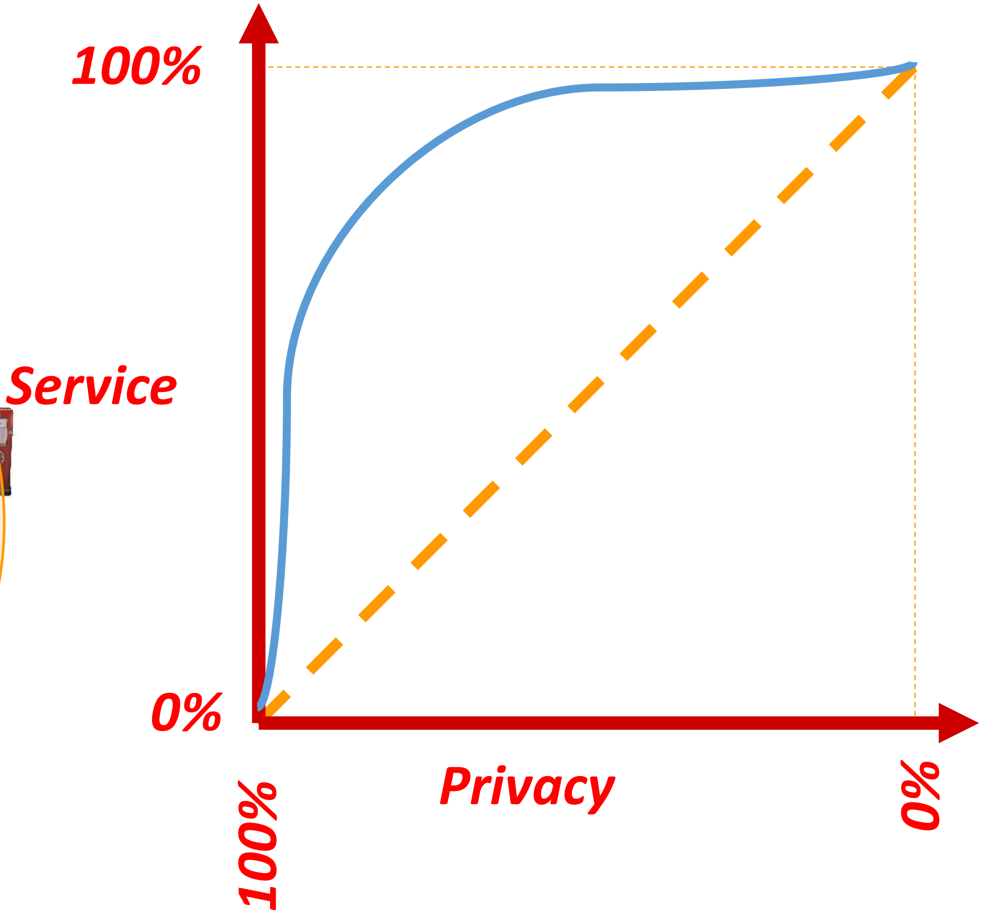
- Second extreme:
  - A user does NOT report her location → 0% service

Desired Trade-off: A user reports a perturbed version of her location → *x*% service

Service-Privacy Trade-off

- Example:: *What is my nearest gas station?*





Three Aspects of Anonymity

- Delay sensitivity
  - Lesser the delay, greater the privacy threat
- Position accuracy
  - Higher the accuracy, greater the privacy threat
- Frequency of access
  - Higher the frequency, greater the privacy threat

Road Hazard Detection

- Location: +- 10m
- Time: +- 1 day

Road Maps & Services

- Location: +- 100m
- Time: <1 sec

Driving Condition Monitoring

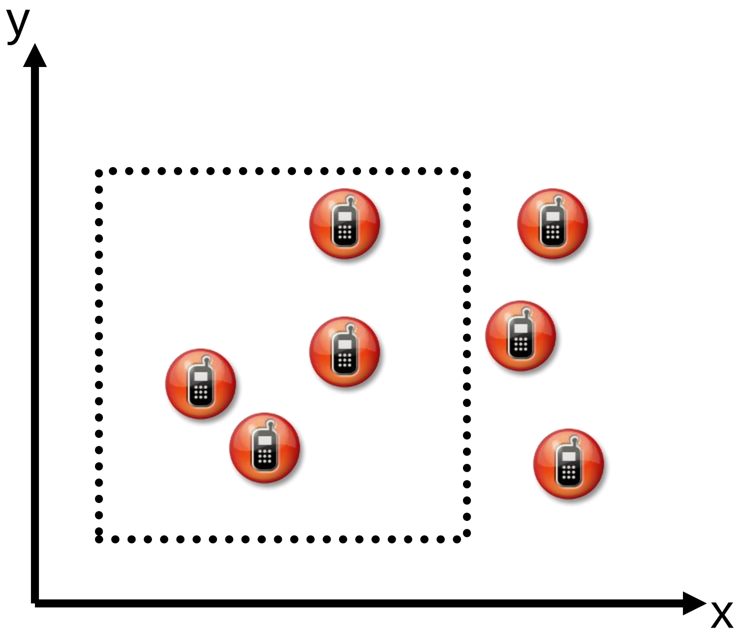
- Location: +- 50m
- Time: +-2-3 mins

Location k-Anonymity

- A message from a client to a location service is called “**location k-anonymous”** if the client cannot be identified by the service based on the client’s location from other k-1 clients.

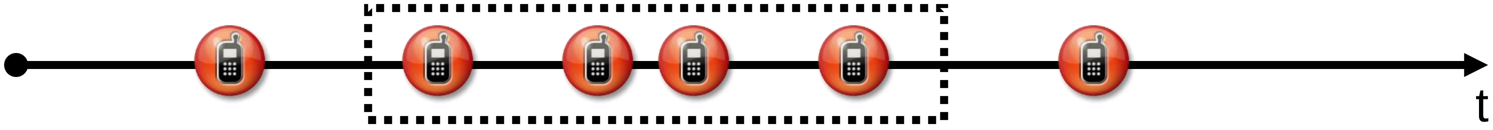
Spatial Cloaking

- Setting a range of space to be a single box, where all clients located within the range are said to be in the “same location”.



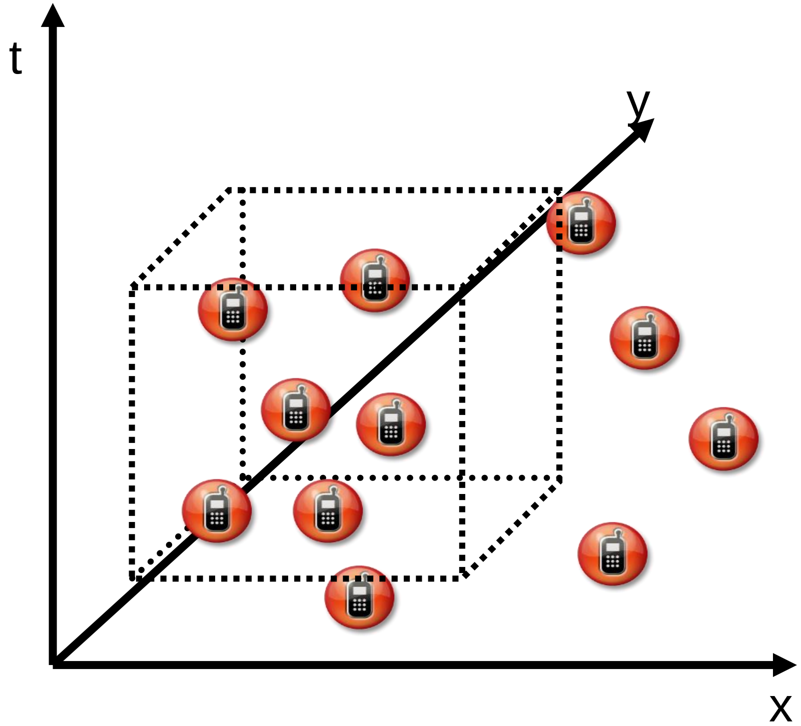
Temporal Cloaking

Setting a time interval, where all the clients in a specific location sending a message in that time interval are said to have sent the message in the "same time".



Spatial-Temporal Cloaking

Setting a range of space and a time interval, where all the messages sent by client inside the range in that time interval. This spatial and temporal area is called a “cloaking box”.



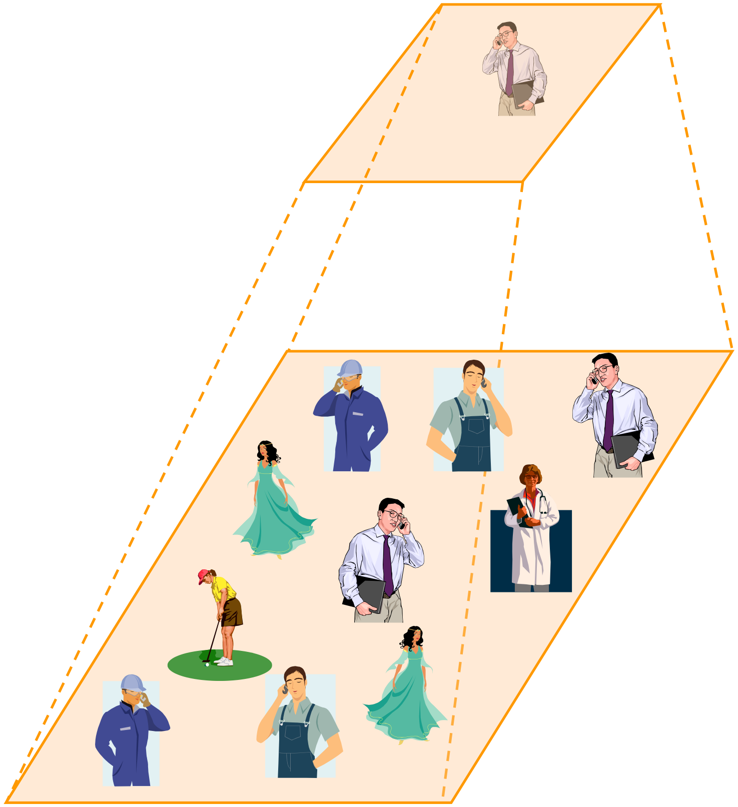
K-Anonymity with Cloaking

- The *cloaked* region contains at least *k* users

- The user is indistinguishable among other *k* users

- The cloaked area largely depends on the surrounding environment.

- A value of *k* =100 may result in a very small area if a user is located in the stadium or may result in a very large area if the user in the desert.



10-anonymity

Problems?

- Tradeoff privacy with quality of location services
    - Either sacrificing the accuracy of location services or adding delays to the services

CacheCloak

- Break away from this tradeoff between privacy and Quality of Localization

- Goals
  - Spatial accuracy
  - Real-time updates
  - Privacy guarantees
  - Even in sparse populations

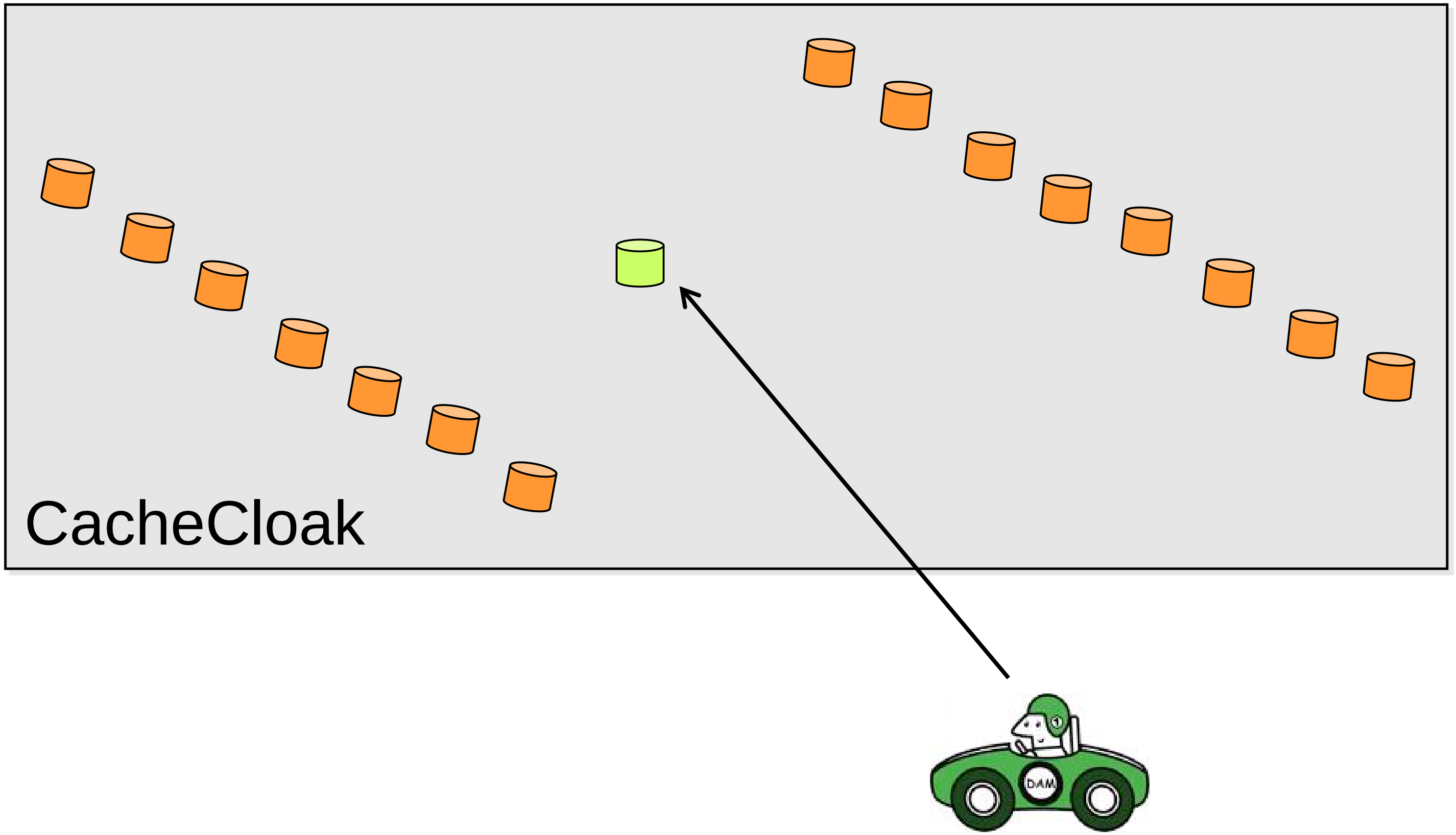
Main idea of "*CacheCloak*"

- Key Ideas
  - Query the (predicted) path not the point location and cache the results
  - Make paths untraceable by creating intersections
- Mechanism

User	CacheCloak	LBS
Request location-centric data	In cache: **return cached data**	Data is retrieved by the database
	Not in cache: **obtain new data** **Predicted path** extends until intersecting with other previously predicted paths	Privacy: Only sees requests from a series of interweaving paths

In Steady State …

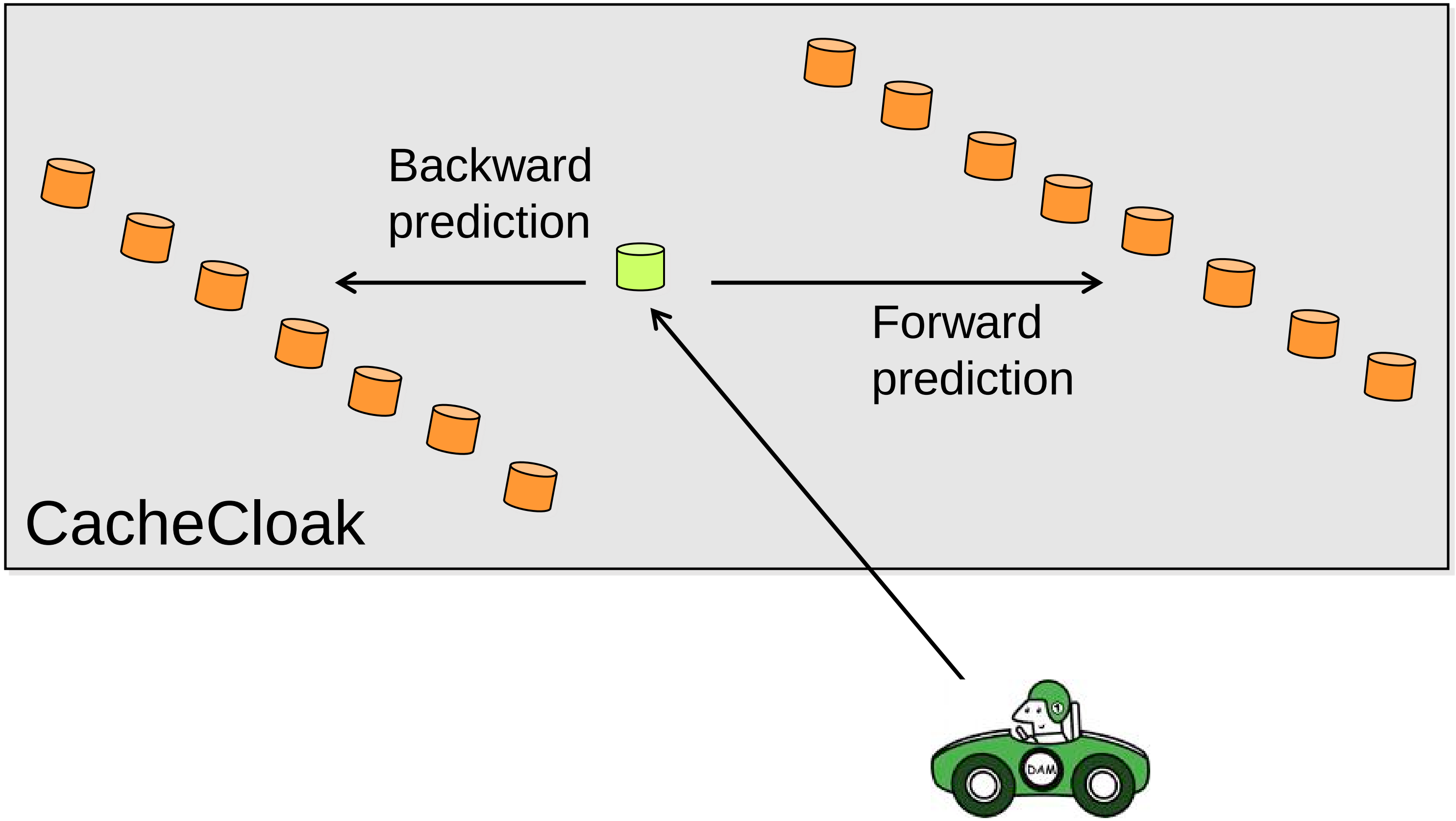
Location Based Service (LBS Database)



CacheCloak

Prediction

Location Based Service (LBS Database)

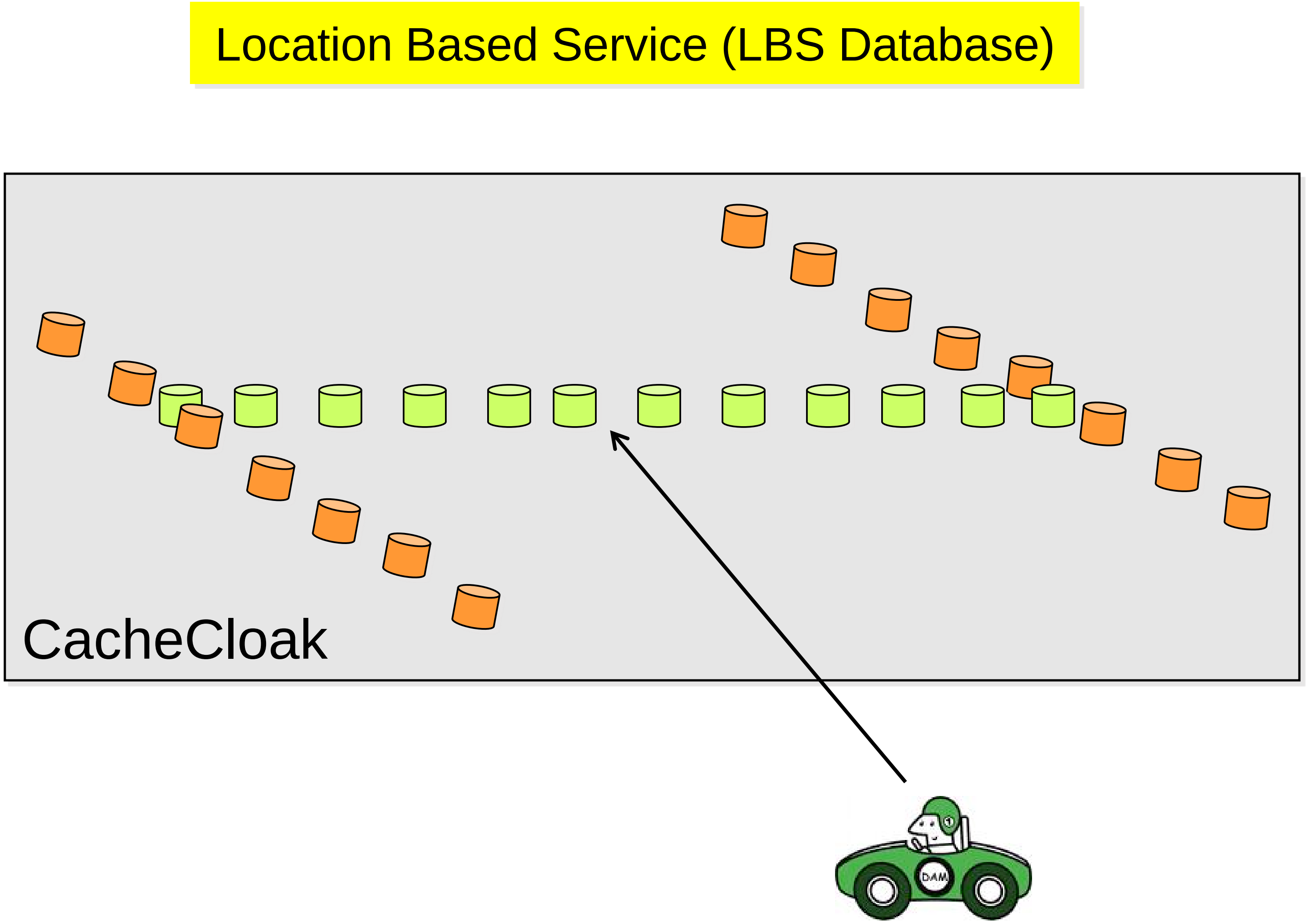


Backward prediction

Forward prediction

CacheCloak

Prediction

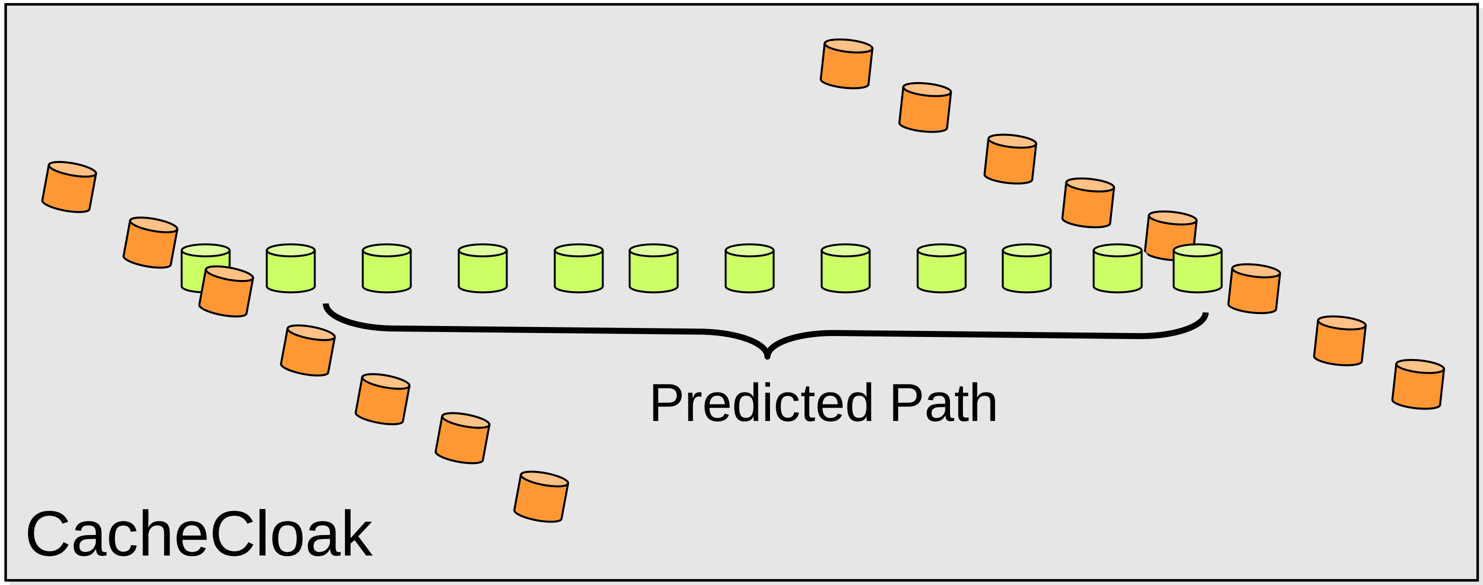


Location Based Service (LBS Database)

CacheCloak

Predicted Intersection

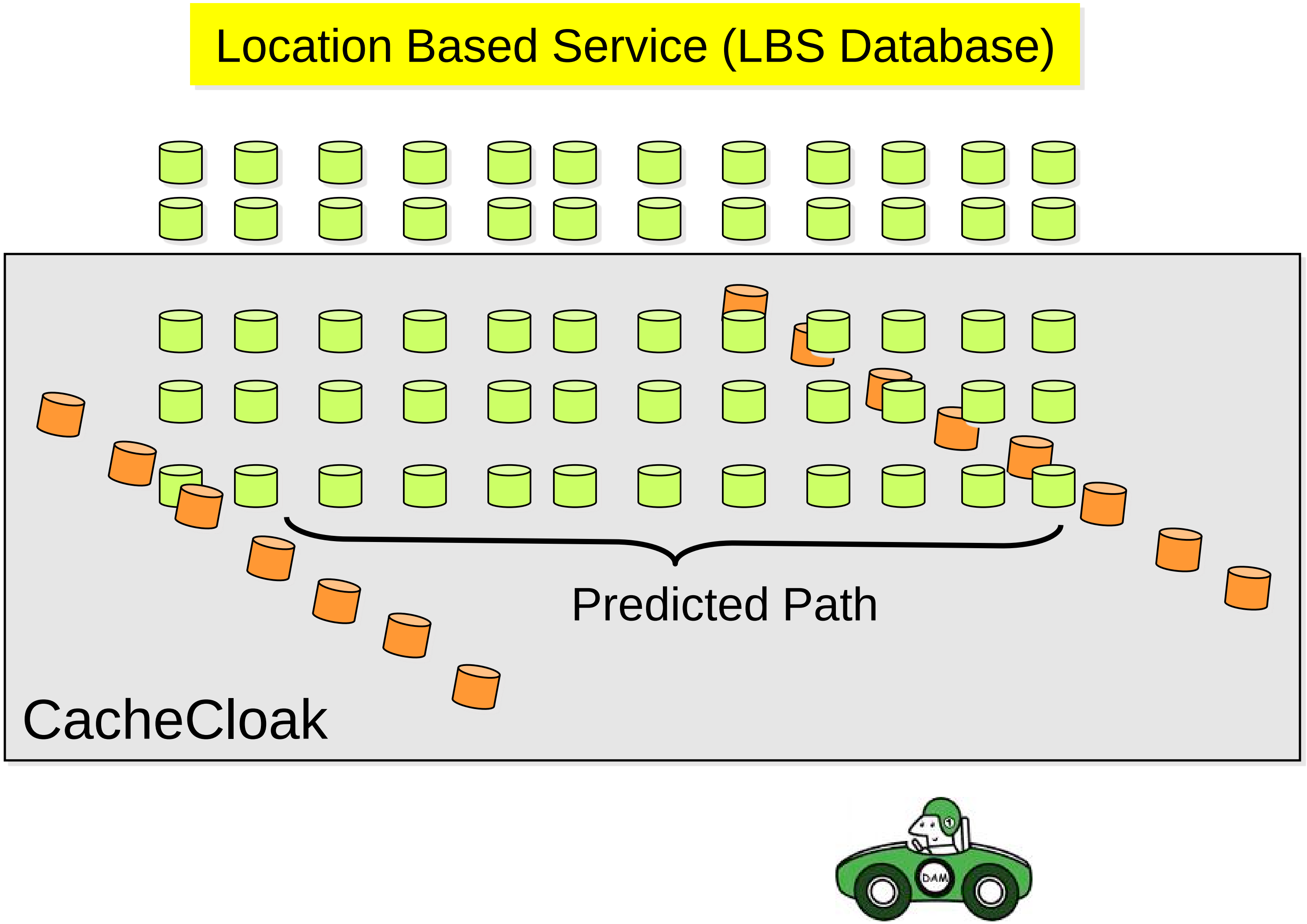
Location Based Service (LBS Database)



Predicted Path

CacheCloak

Query

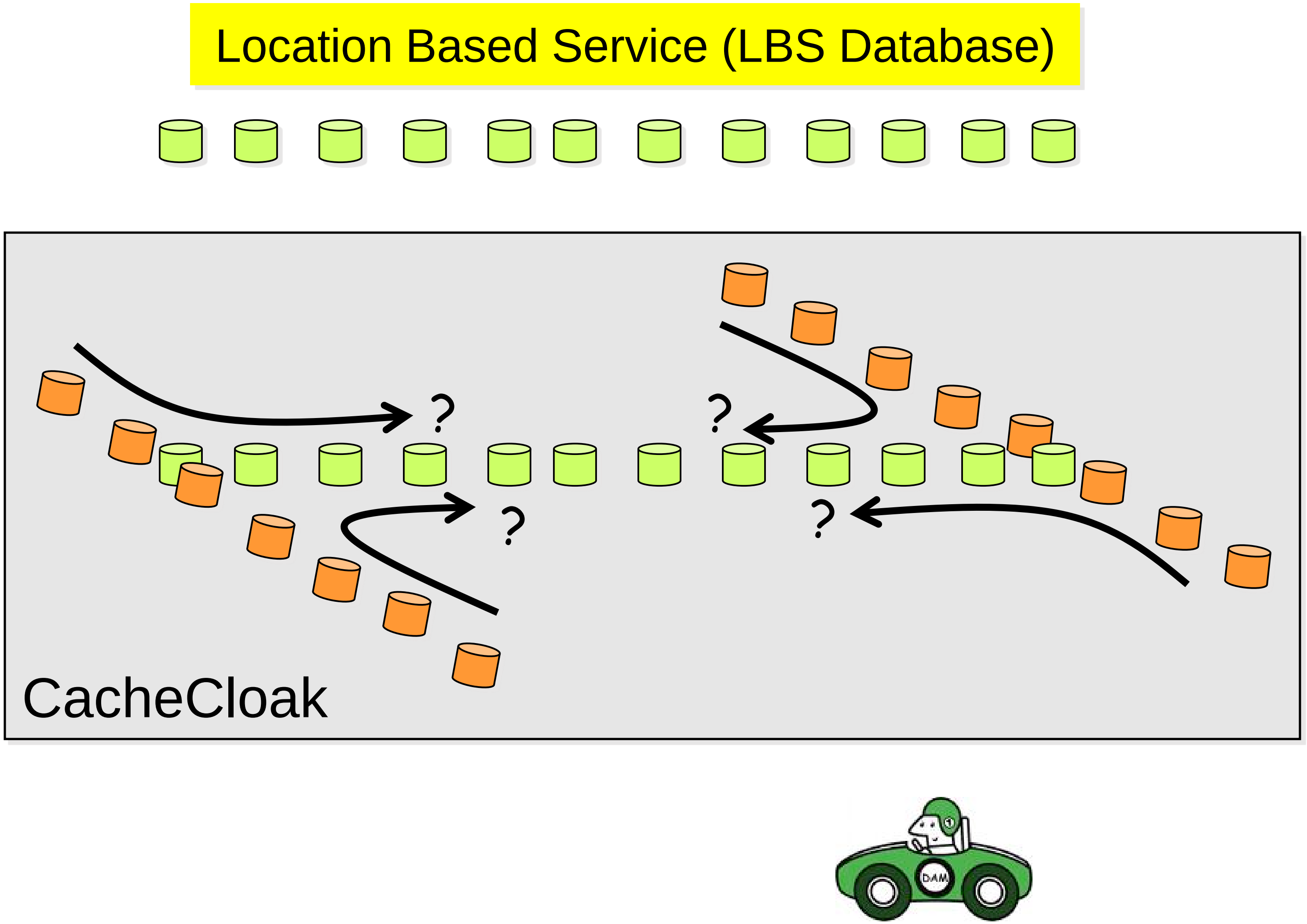


Location Based Service (LBS Database)

Predicted Path

CacheCloak

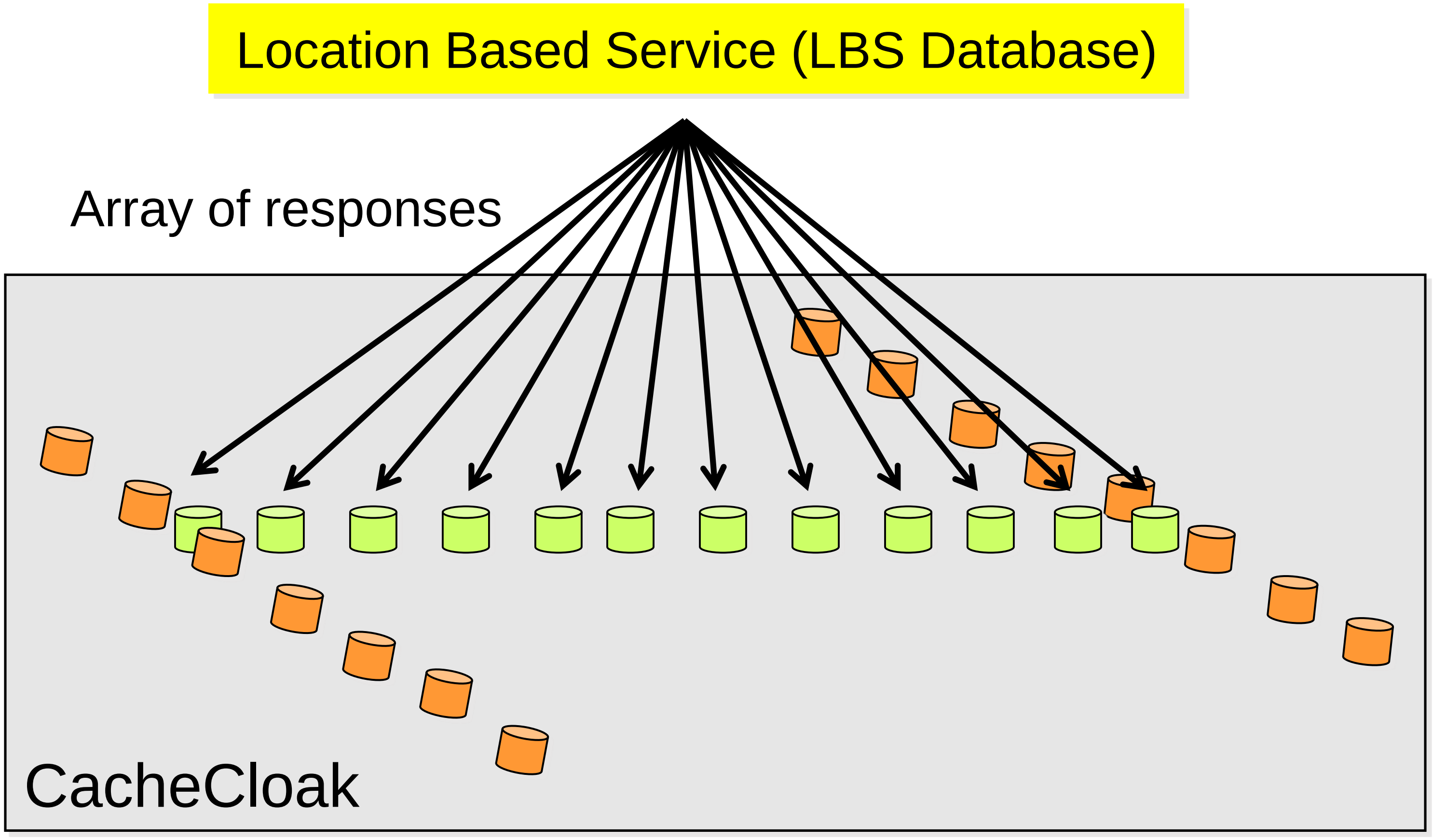
Query



Location Based Service (LBS Database)

CacheCloak

LBS Responds

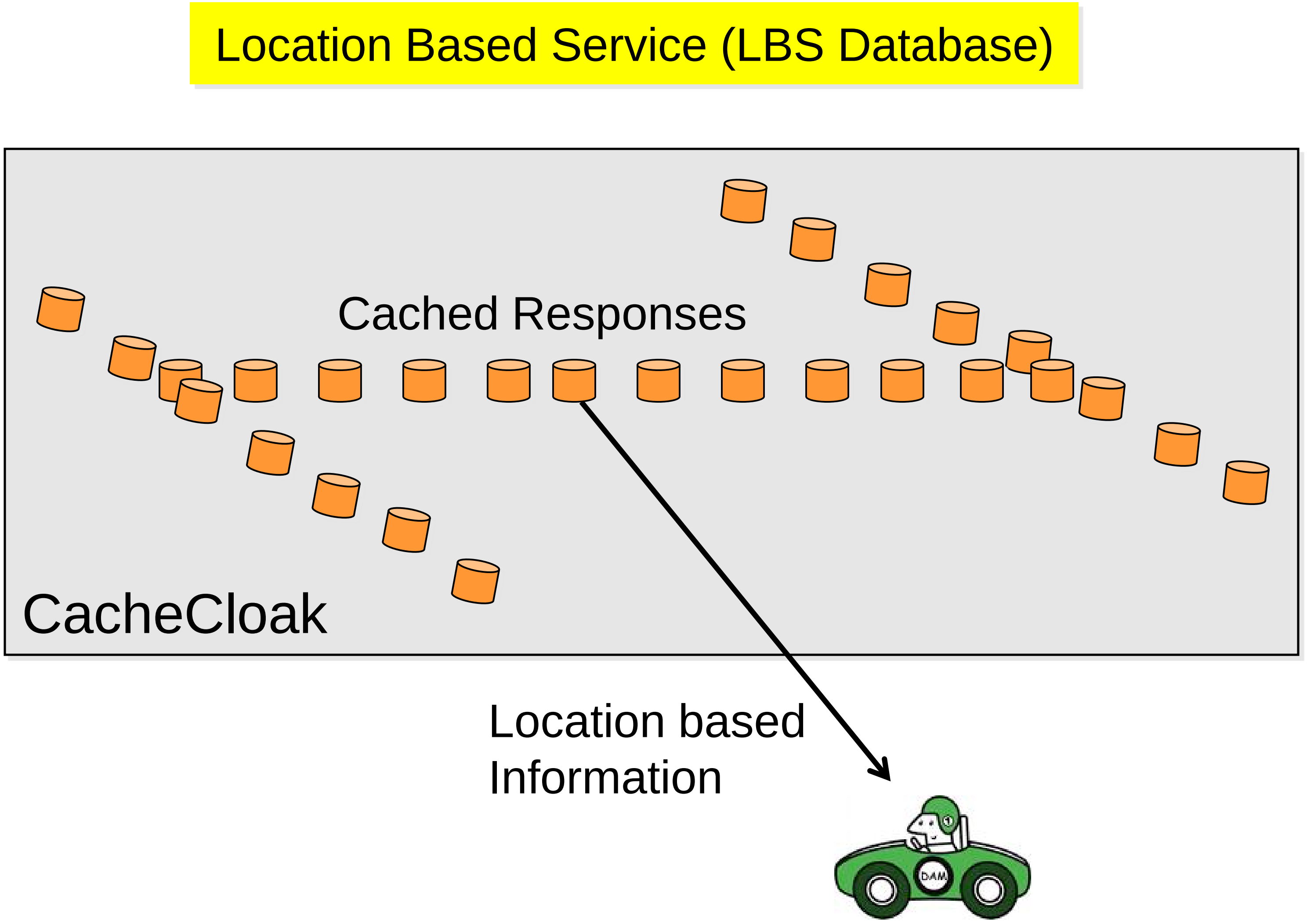


Location Based Service (LBS Database)

Array of responses

CacheCloak

Cached



Location Based Service (LBS Database)

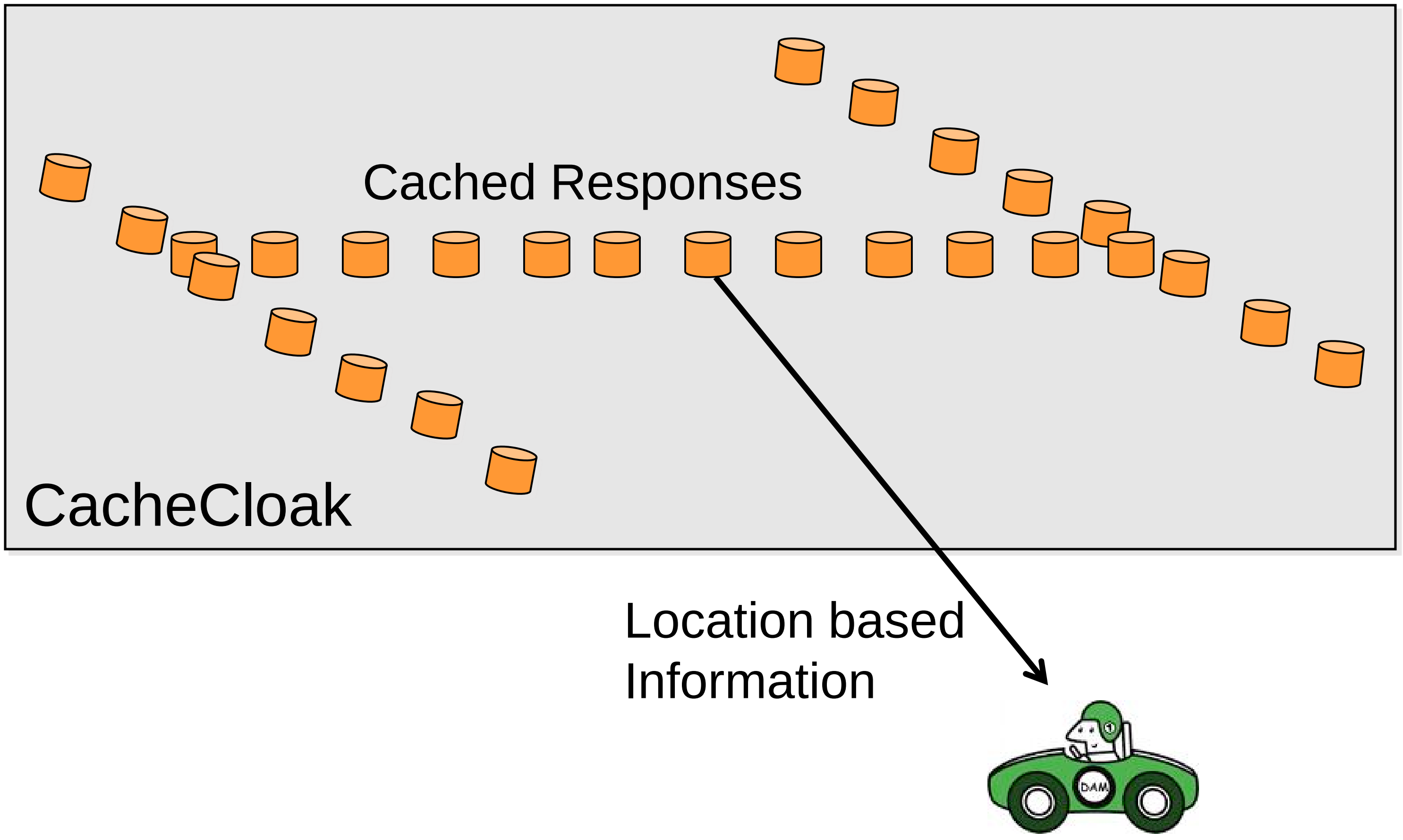
Cached Responses

CacheCloak

Location based Information

Cached Response

Location Based Service (LBS Database)

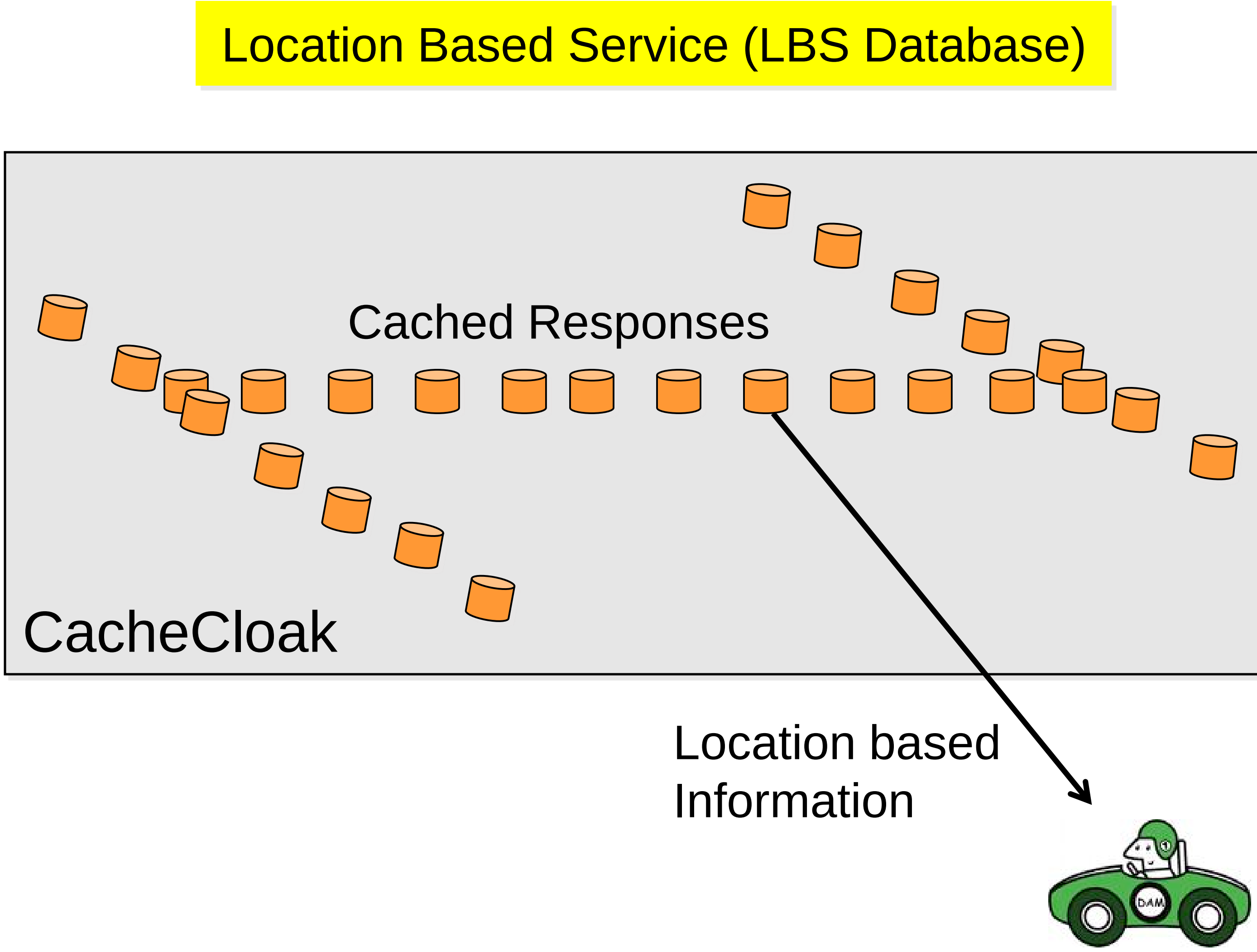


Cached Responses

CacheCloak

Location based Information

Cached Response



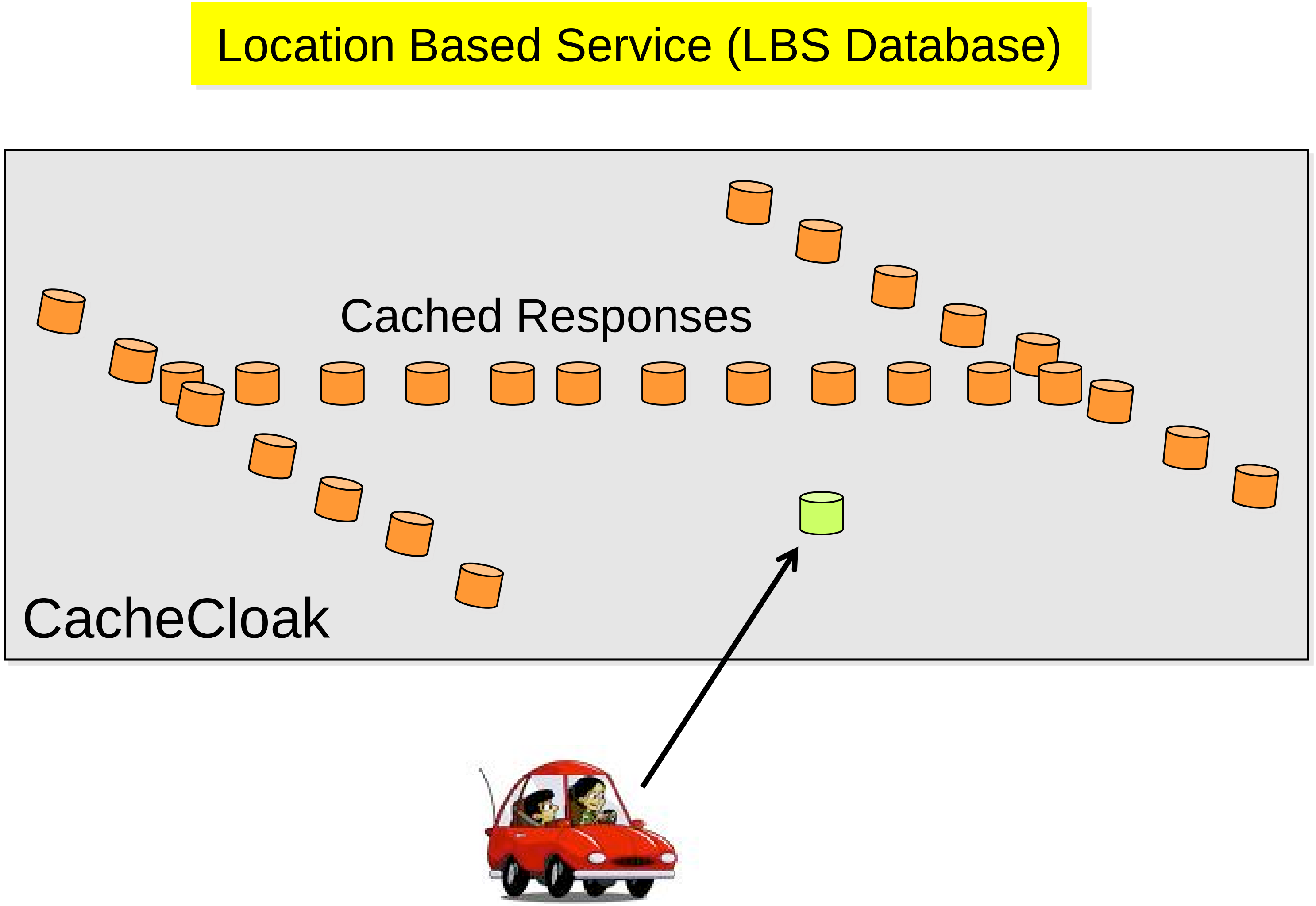
Location Based Service (LBS Database)

Cached Responses

CacheCloak

Location based
Information

Cache Miss



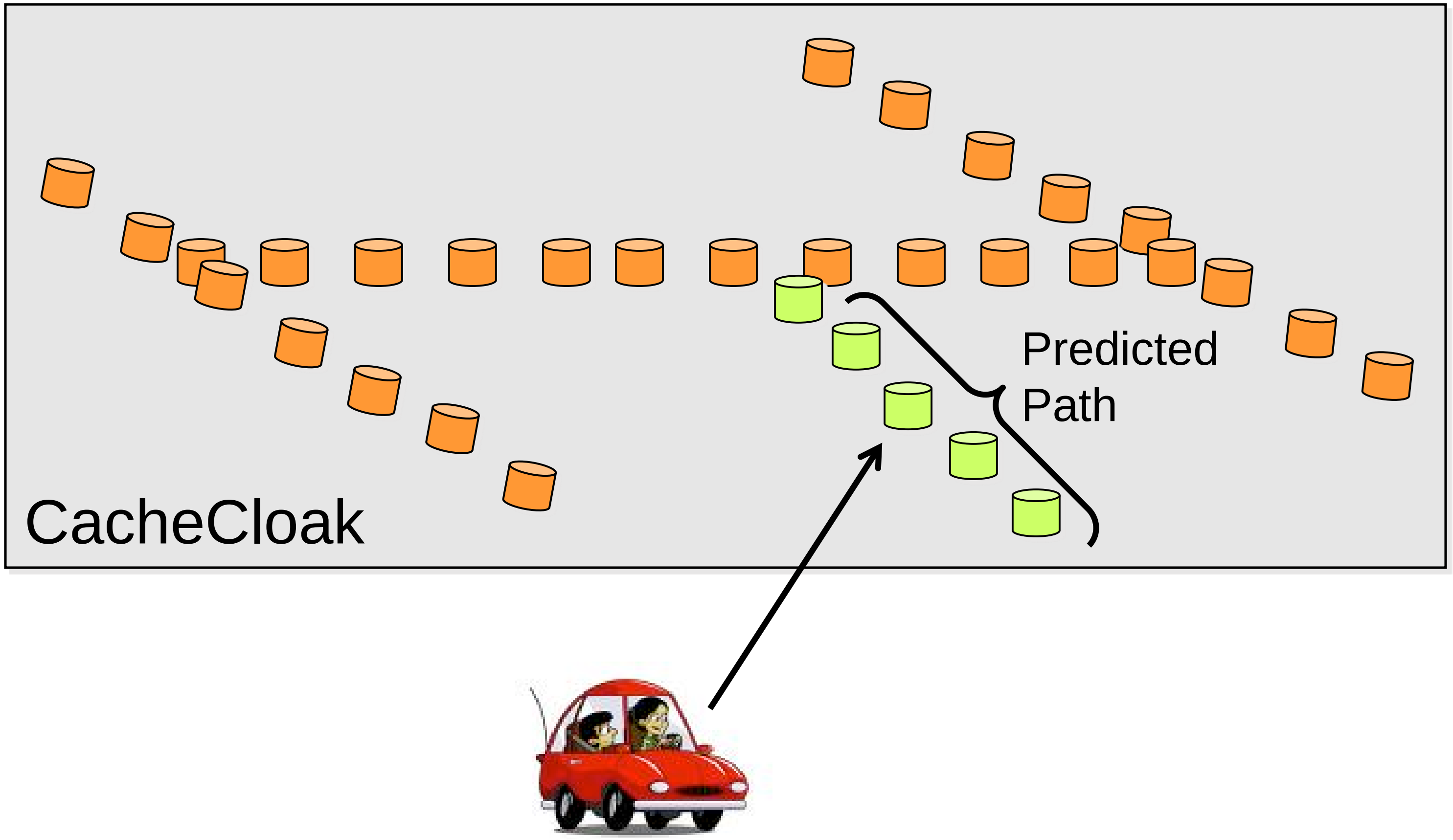
Location Based Service (LBS Database)

Cached Responses

CacheCloak

Cache Miss

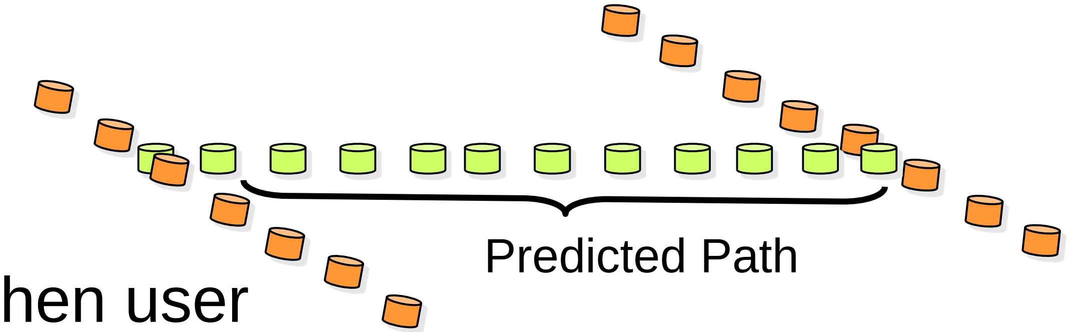
Location Based Service (LBS Database)



Predicted Path

CacheCloak

Benefits



- Real-time
  - Response ready when user arrives at predicted location
- High QoL
  - Responses can be specific to location
  - Overhead on the wired backbone (caching helps)
- Entropy guarantees
  - Entropy increases at traffic intersections
- Sparse population
  - Can be handled with dummy users, false branching

References

- More about CacheCloak can be found at
  - https://synrg.csl.illinois.edu/papers/cachecloak.pdf

- Look also for
  - I-Diversity
  - Differential Privacy

Final Presentation

- June 11 Tuesday (3:30pm –)
  - All 7 teams will present
  - 15 min. presentation followed by 5 min. QnA

- Notes
  - Refer to the guideline for the midterm presentation
  - Make sure to demonstrate the app
  - Focus on what were done after the midterm
  - Include reflections and future plans (if any)

Final Exam

- June 14 Friday 2-4pm

- Scope: Lecture notes and papers presented
  - week 14 papers are excluded

- Closed book