Exploiting Social Navigation

MEITAL BEN SINAI
NIMROD PARTUSH
SHIR YADID
ERAN YAHAV

Technion, Israel

black hat®
ASIA 2015

Outline

- Intro
- Goals & Motivation
- Attacks
- Defense
- Summary & Conclusions

Intro

- Navigation (like most content) is becoming social
  - *Waze* has over 50 Million Users
- The data is being crowdsourced
  - But the crowd is oblivious to consequences
- What kind of attacks can be applied in this context?
  - Can the crowdsourcing process be exploited?
- How to mitigate?

How did this happen?

- while driving out of congested Jerusalem with *Waze* on, on a Thursday afternoon.

As a joke, called and told my adviser

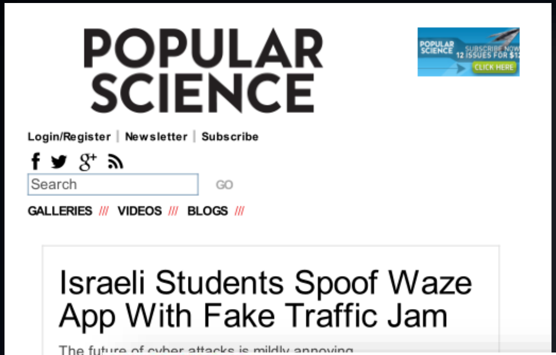
He took it too seriously..

Enter undergrads*!

+ =

Israeli Students Spoof Waze App With Fake Traffic Jam

Kelsey D. Atherton at 04:46 AM Apr 1 2014 Tweet 0 Like 0 0 Comments



POPULAR SCIENCE

Login/Register | Newsletter | Subscribe

Search GO

GALLERIES /// VIDEOS /// BLOGS ///

Israeli Students Spoof Waze App With Fake Traffic Jam

The future of cyber attacks is mildly annoying

By Kelse

The Hacker News™
Security in a serious way

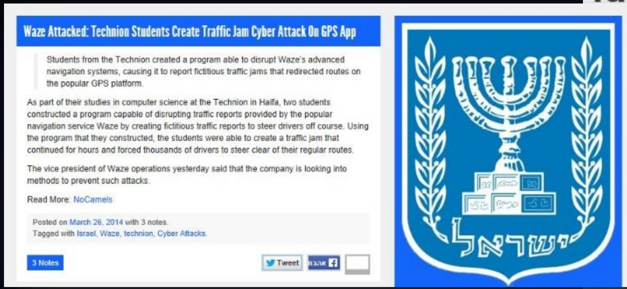
Popular Navigation App hijacked with Fake Bots to Cause Traffic Jam

Friday, April 04, 2014 by Swati Khandelwal

GEOLOCALIZADO

Estudiantes reportan un embotellamiento falso en Waze que duró horas

eban Zamorano 26 Marzo 2014



Waze Attacked: Technion Students Create Traffic Jam Cyber Attack On GPS App

> Students from the Technion created a program able to disrupt Waze's advanced navigation systems, causing it to report fictitious traffic jams that redirected routes on the popular GPS platform.

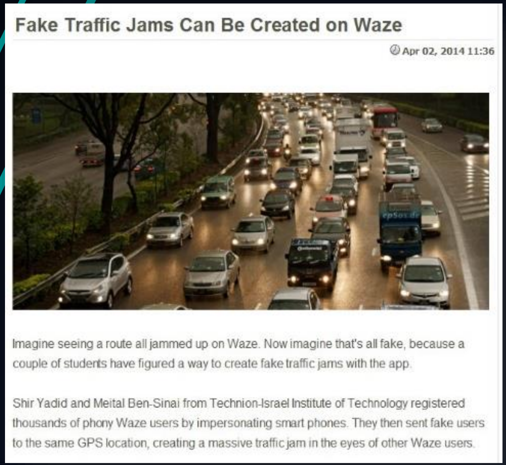
As part of their studies in computer science at the Technion in Haifa, two students constructed a program capable of disrupting traffic reports provided by the popular navigation service Waze by creating fictitious traffic reports to steer drivers off course. Using the program that they constructed, the students were able to create a traffic jam that continued for hours and forced thousands of drivers to steer clear of their regular routes.

The vice president of Waze operations yesterday said that the company is looking into methods to prevent such attacks.

Read More: NoCamels

Posted on March 26, 2014 with 3 notes.
Tagged with Israel, Waze, technion, Cyber Attacks.

3 Notes Tweet

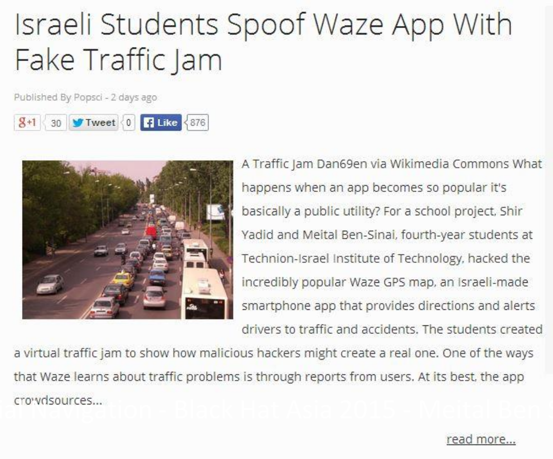


Fake Traffic Jams Can Be Created on Waze

Apr 02, 2014 11:36

Imagine seeing a route all jammed up on Waze. Now imagine that's all fake, because a couple of students have figured a way to create fake traffic jams with the app.

Shir Yadid and Meital Ben-Sinai from Technion-Israel Institute of Technology registered thousands of phony Waze users by impersonating smart phones. They then sent fake users to the same GPS location, creating a massive traffic jam in the eyes of other Waze users.



Israeli Students Spoof Waze App With Fake Traffic Jam

Published By Popsci - 2 days ago

g+1 30 Tweet 0 Like 876

A Traffic Jam Dan69en via Wikimedia Commons What happens when an app becomes so popular it's basically a public utility? For a school project, Shir Yadid and Meital Ben-Sinai, fourth-year students at Technion-Israel Institute of Technology, hacked the incredibly popular Waze GPS map, an Israeli-made smartphone app that provides directions and alerts drivers to traffic and accidents. The students created a virtual traffic jam to show how malicious hackers might create a real one. One of the ways that Waze learns about traffic problems is through reports from users. At its best, the app crowdsources...

read more...

THE PRINCIPAL

HOT How to buy integrity

Headlines Australia - Canada - New Zealand United Kingdom - United Sta

Technology

Students hack Waze, send in army of traffic bots

Posted on March 25, 2014 by admin | 240 Views

successfully hacked popular
social GPS map and traffic app Waze, causing it to report a
nonexistent traffic jam.

The attack, somewhat reminiscent of the wonderfully ridiculous *Die Hard 4.0* plot, was carried out by Shir Yadid and Meital Ben-Sinai, two software engineering students in their fourth year at the Israel Institute of Technology.

By Nicholas Tufnell,

Waze under attack: Israeli students fake traffic jam on popular map app

For a school project, two software engineering students at the Technion caused Waze to report a nonexistent traffic jam.

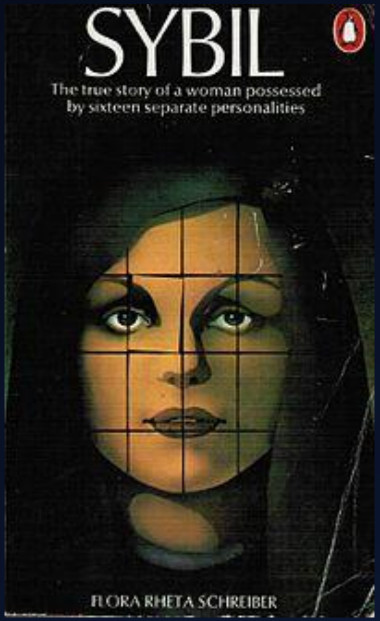
By Ido Efrati | Mar. 25, 2014 | 2:18 AM

2 g+1 Tweet 33 Recommend Share 53 people recommend this. Be the first of your frien

Turn here? Are you sure? Photo by Reuters

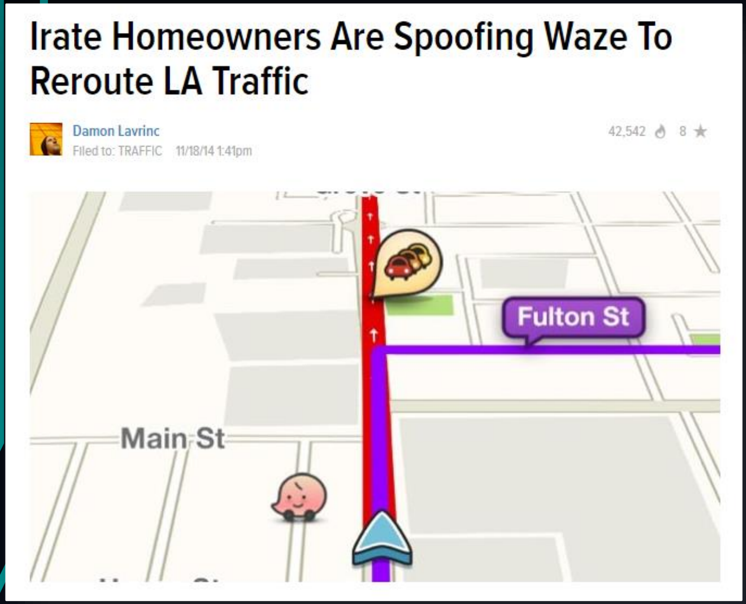
Research Goal

- Successfully apply a ***Sybil Attack*** to a social navigation system
  - And explore what can be gained


SYBIL
The true story of a woman possessed by sixteen separate personalities
FLORA RHETA SCHREIBER

"In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence"

Motivation

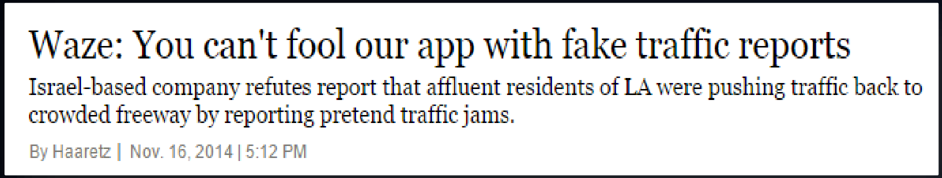


Irate Homeowners Are Spoofing Waze To Reroute LA Traffic

Damon Lavrinc 42,542 8 ★
Filed to: TRAFFIC 11/18/14 1:41pm

PISSED OFF L.A. HOMEOWNERS
WAZE IS THE DEVIL!

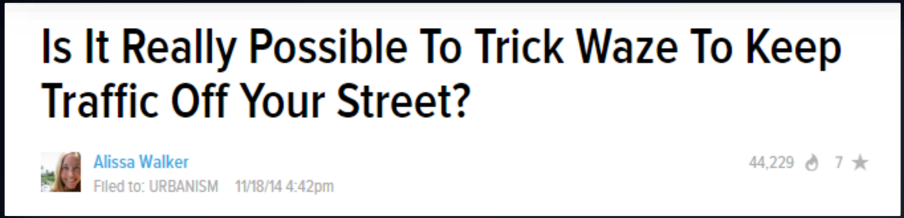
11/14/2014 12:40 AM PST BY TMZ STAFF



Waze: You can't fool our app with fake traffic reports

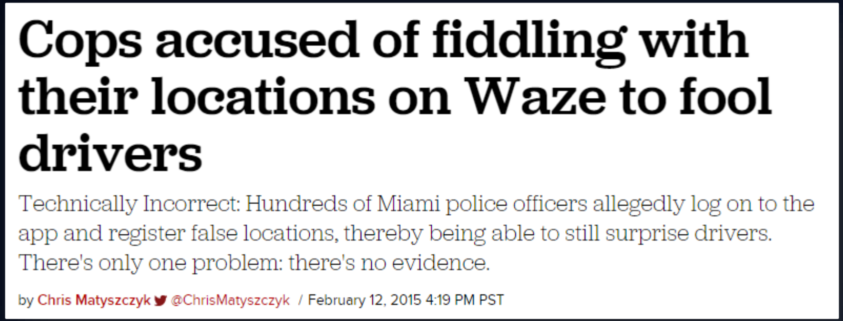
Israel-based company refutes report that affluent residents of LA were pushing traffic back to crowded freeway by reporting pretend traffic jams.

By Haaretz | Nov. 16, 2014 | 5:12 PM



Is It Really Possible To Trick Waze To Keep Traffic Off Your Street?

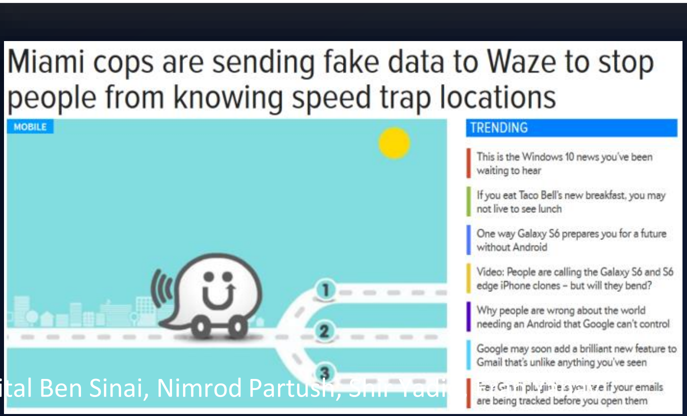
Alissa Walker 44,229 7 ★
Filed to: URBANISM 11/18/14 4:42pm



Cops accused of fiddling with their locations on Waze to fool drivers

Technically Incorrect: Hundreds of Miami police officers allegedly log on to the app and register false locations, thereby being able to still surprise drivers. There's only one problem: there's no evidence.

by Chris Matyszczyk @ChrisMatyszczyk / February 12, 2015 4:19 PM PST



Miami cops are sending fake data to Waze to stop people from knowing speed trap locations

TRENDING

- This is the Windows 10 news you've been waiting to hear
- If you eat Taco Bell's new breakfast, you may not live to see lunch
- One way Galaxy S6 prepares you for a future without Android
- Video: People are calling the Galaxy S6 and S6 edge iPhone clones – but will they bend?
- Why people are wrong about the world needing an Android that Google can't control
- Google may soon add a brilliant new feature to Gmail that's unlike anything you've seen
- Free Gmail plugin lets you see if your emails are being tracked before you open them

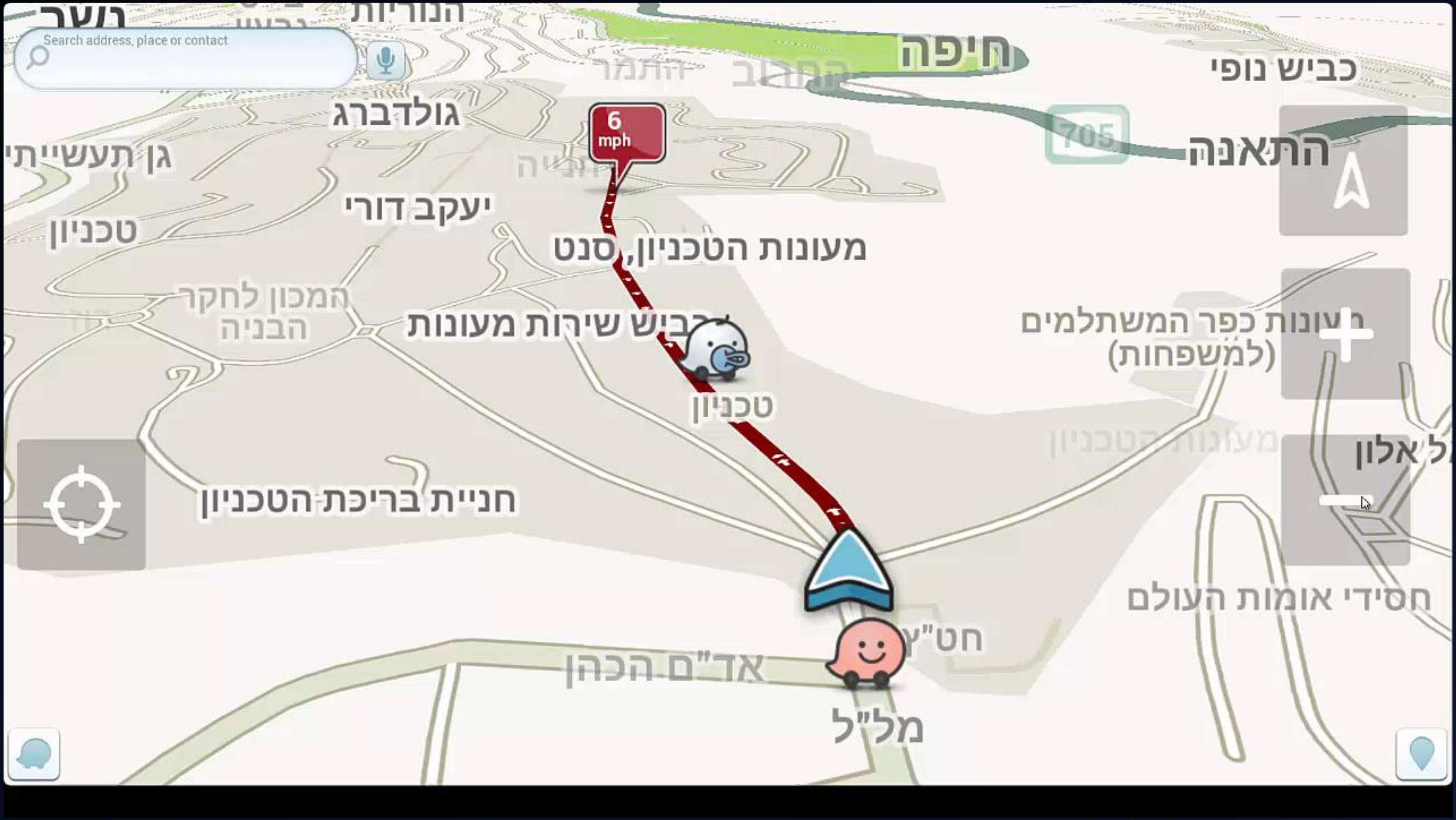
Attack #1

CREATING FALSE CONGESTION & AFFECTING ROUTING

Navigation

Successful Attack

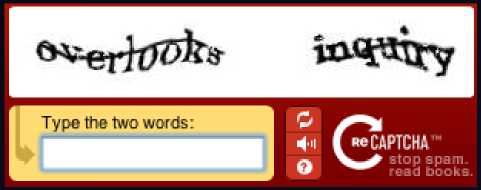
Navigation has Changed!



Attack #1 – Creating False Congestion & Affecting Routing

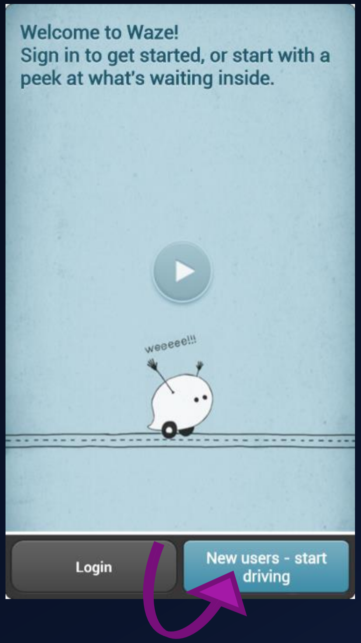
Creating Bot Drivers

- Becoming an influential part of the WAZE community requires a single click
- Registration does not require validation
  - Intentionally avoided?
  - CAPTCHA required for deleting account!

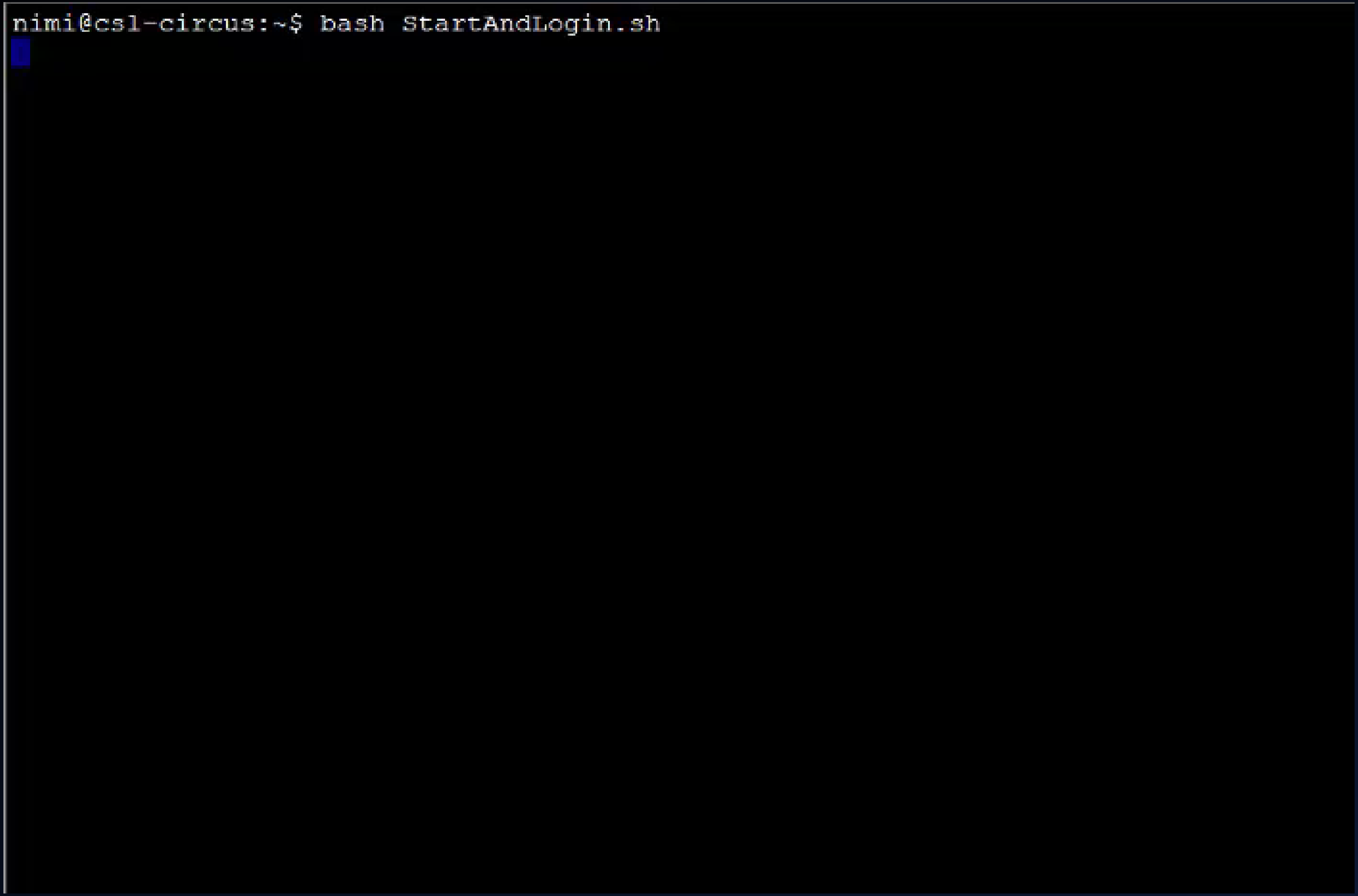


overlooks inquiry

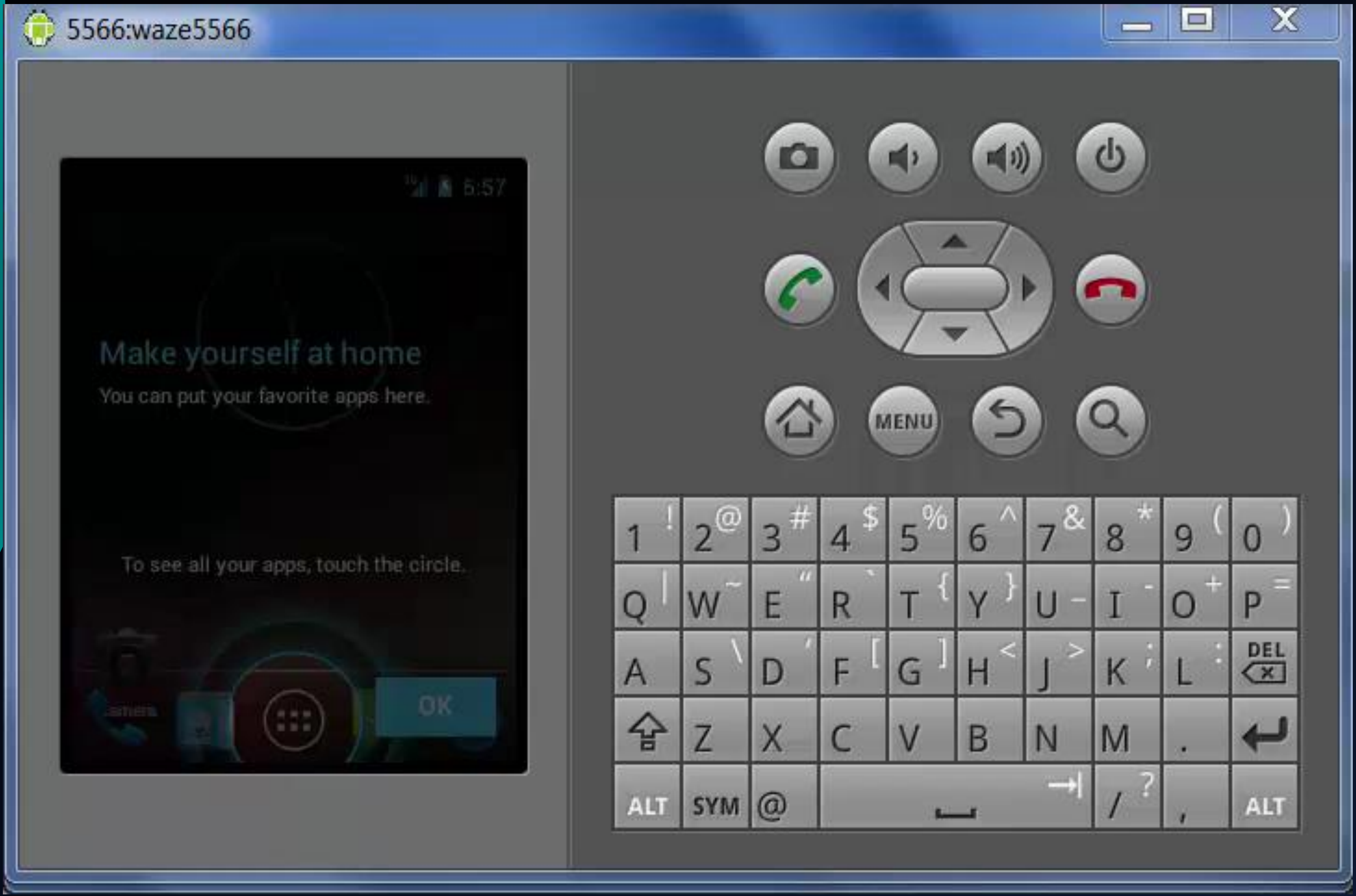
Type the two words:



Welcome to Waze!
Sign in to get started, or start with a peek at what's waiting inside.



```
nimi@csl-circus:~$ bash StartAndLogin.sh
```



5566:waze5566

6:57

Make yourself at home

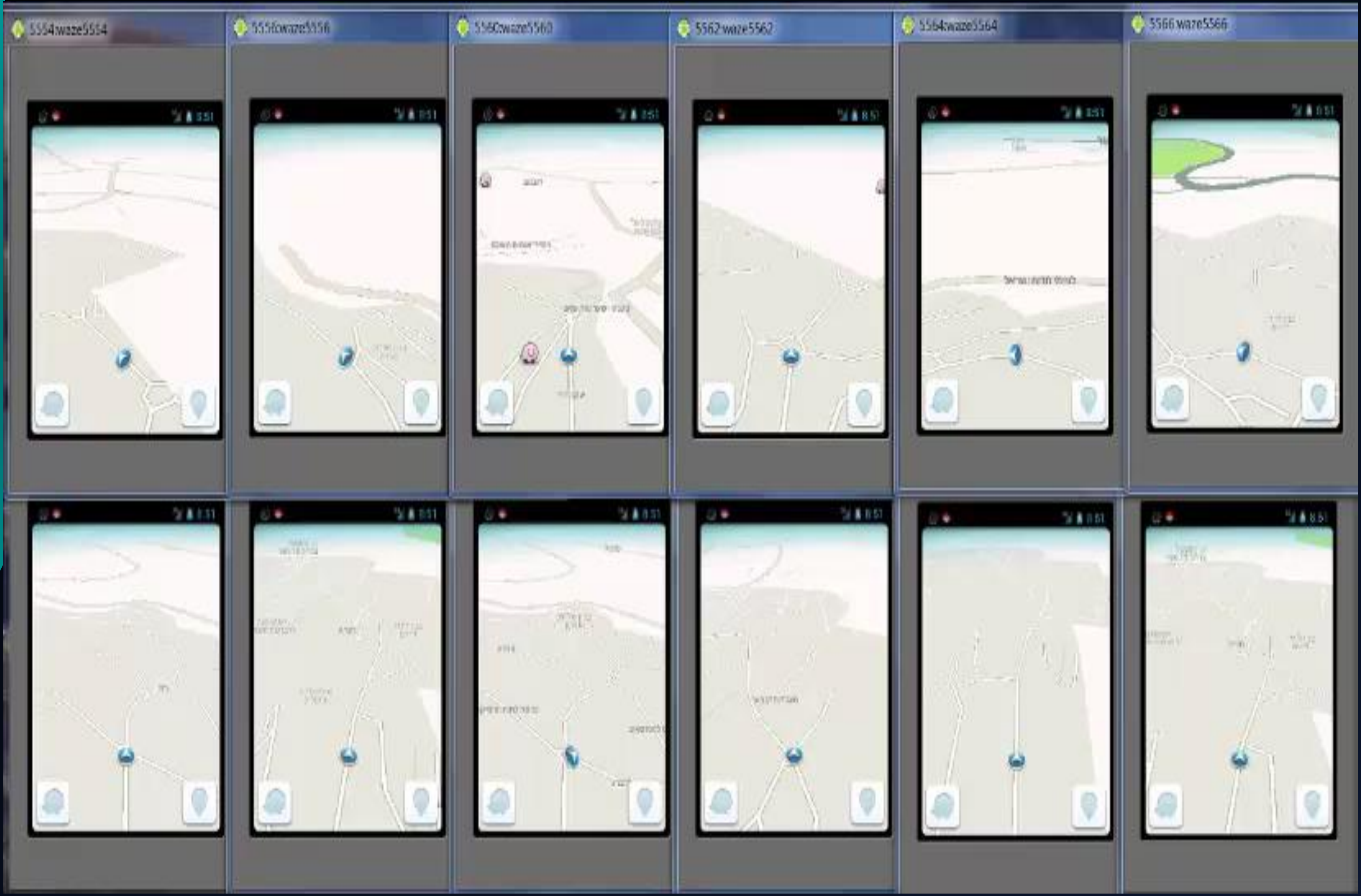
You can put your favorite apps here.

To see all your apps, touch the circle.

OK

Creating Reputed Bots

- WAZE has a user rating system
  - The more you drive the higher you rate
- Bots can be “trained” to achieve higher rating
  - Mitigation idea: detect bots based on human behavior pattern
    - Study human user movement patterns
    - Filter users that don’t match the criteria
  - Problem: human behavior could be easily mimicked (in the geo context)
    - Still, some effort could be made
- All of the experiments were carried out with (almost) 0 reputation bots


5554:waze5554
5556:waze5556
5560:waze5560
5562:waze5562
5564:waze5564
5566:waze5566

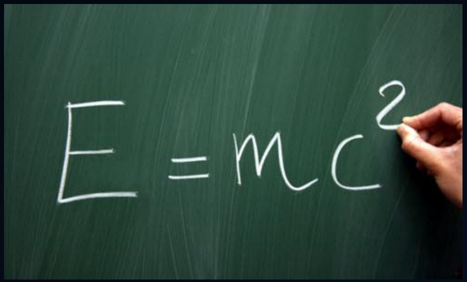
Simulating Standstill Traffic

- Initially, we spawned botnets of increasing sizes and scattered them at the target area
    - No congestion was reported
        - Why?
- Hypothesis 1: WAZE attributes these to drivers about to start driving
- Hypothesis 2: in real life, traffic jams are created **continuously**

Simulating Slowdown

- Our next round of experiments consisted of simulating a gradual slowdown in traffic.
- We sent increasingly larger groups of bots to the target location
- but this time they moved through the area in gradually slower speeds
  - Each “run” is ~20 minutes long
  - Later on, stops were incorporated
- Still, no jam ☹

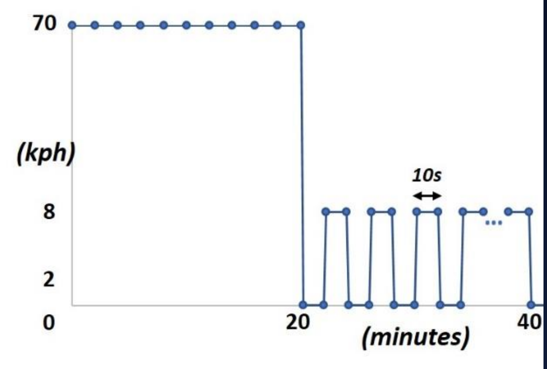
Speed is relative



- We used increasingly larger groups of bots
- We explored various slowdown patterns
- No congestion
- -> This means that the WAZE algorithm takes other, non user-related parameters into effect!
  - These may include: time of day, weather conditions, ***road information***, etc.
    - Would you expect a congestion to be reported in a back-alley?

Speed is relative

- Presumabley, the WAZE congestion reporting algorithm is a relative one, i.e., a route is congested if its current average speed is considerably lower relative to former known speeds.
- Thus, we “taught” WAZE that you can drive 70kph inside the Technion (don’t try this at home)
- Final speed pattern:



Spoof Attack: Responses

- *"These students may be in an "excellence program" but obviously they, and more so the academic adviser,* ***have lost their moral compass*** *which is far more important for providing direction than Waze. Even if the project was done as a prank or as an academic exercise,* ***the results are no different than physically going out and blocking a major roadway****, something that presumably would not be tolerated by the legal system. And to then go and brag about it?* ***Why are they not swiftly being investigated by the police..****"*

Spoof Attack: Disclosure

- We notified *Waze* of the attack 2 months before publishing
- We saw a change in the registration process roughly 6 months after publishing (+8 months)
- 6 months later, the attack seemed to have been patched
  - At least in the small setting of our experiment

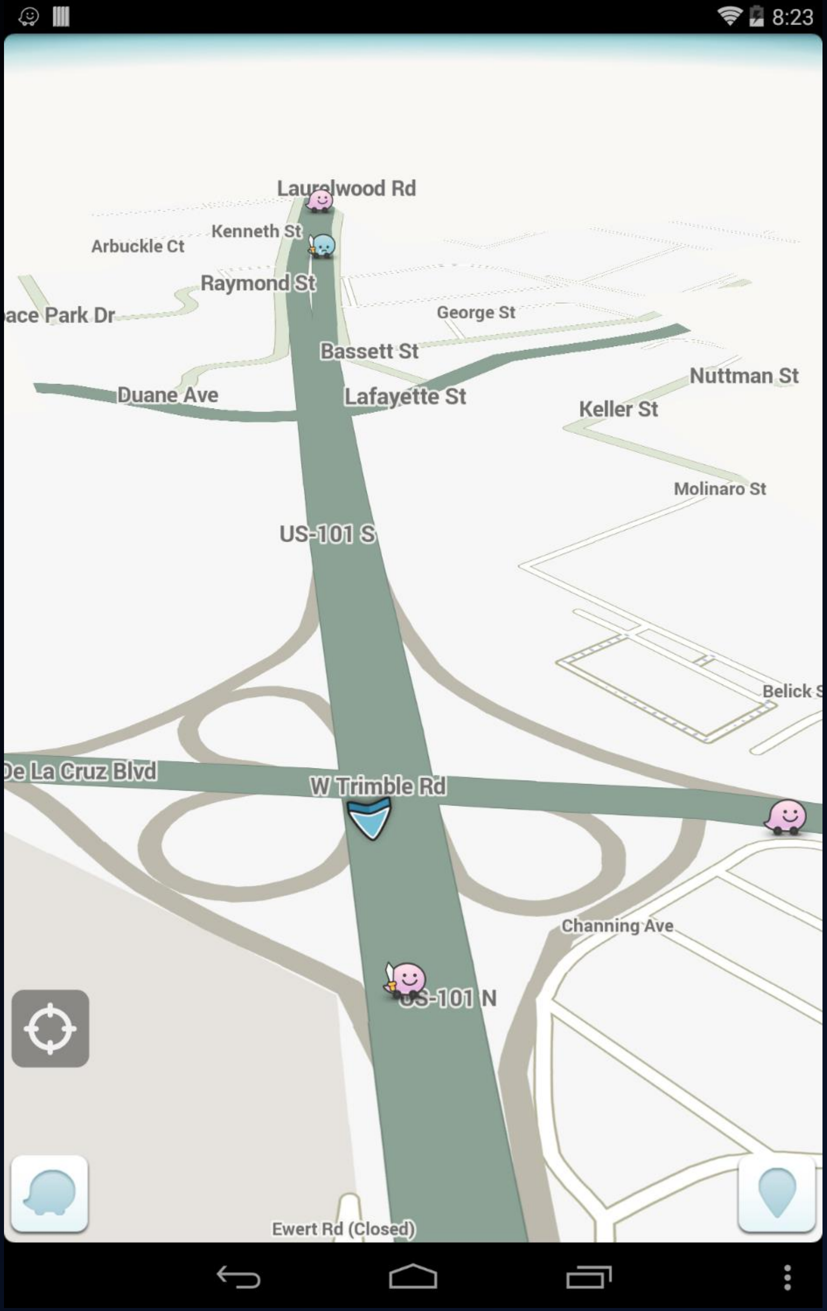
Spoof Attack: Implications

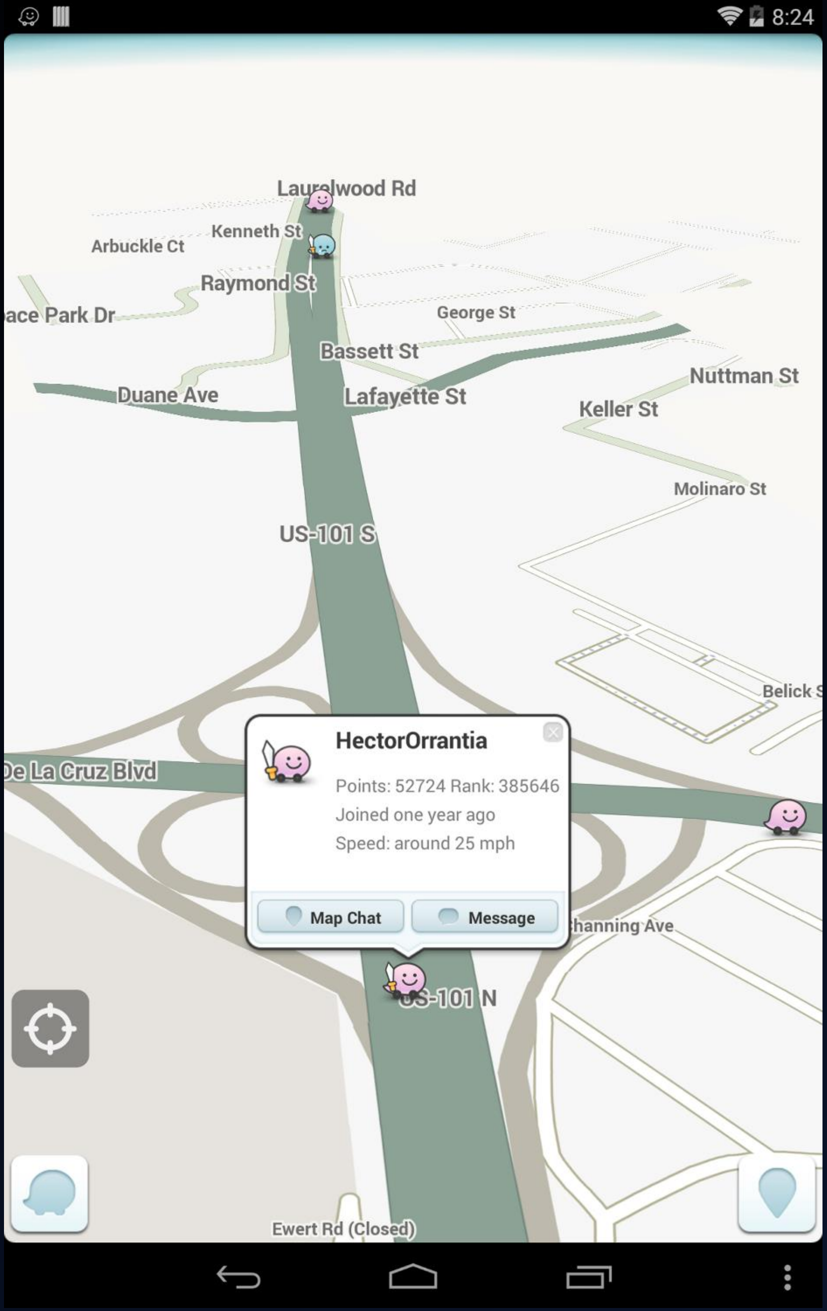
- National
  - Render the system useless
  - Waste time & fuel (& pollution) of users
- Private Financial
  - Congest (free) roads near toll roads
  - Make people drive by my restaurant\sign
  - Create congestion near the competition
- Criminal
  - Lead a target down an attacker controlled path
- Personal
  - Clear roads to save time
  - Get people out (or in?) of your neighborhood

Attack #2

TRACKING USERS

mockLocation
6:10


8:23
Laurelwood Rd
Kenneth St
Arbuckle Ct
Raymond St
ace Park Dr
George St
Bassett St
Nuttman St
Duane Ave
Lafayette St
Keller St
Molinaro St
US-101 S
Belick S
De La Cruz Blvd
W Trimble Rd
Channing Ave
US-101 N
Ewert Rd (Closed)

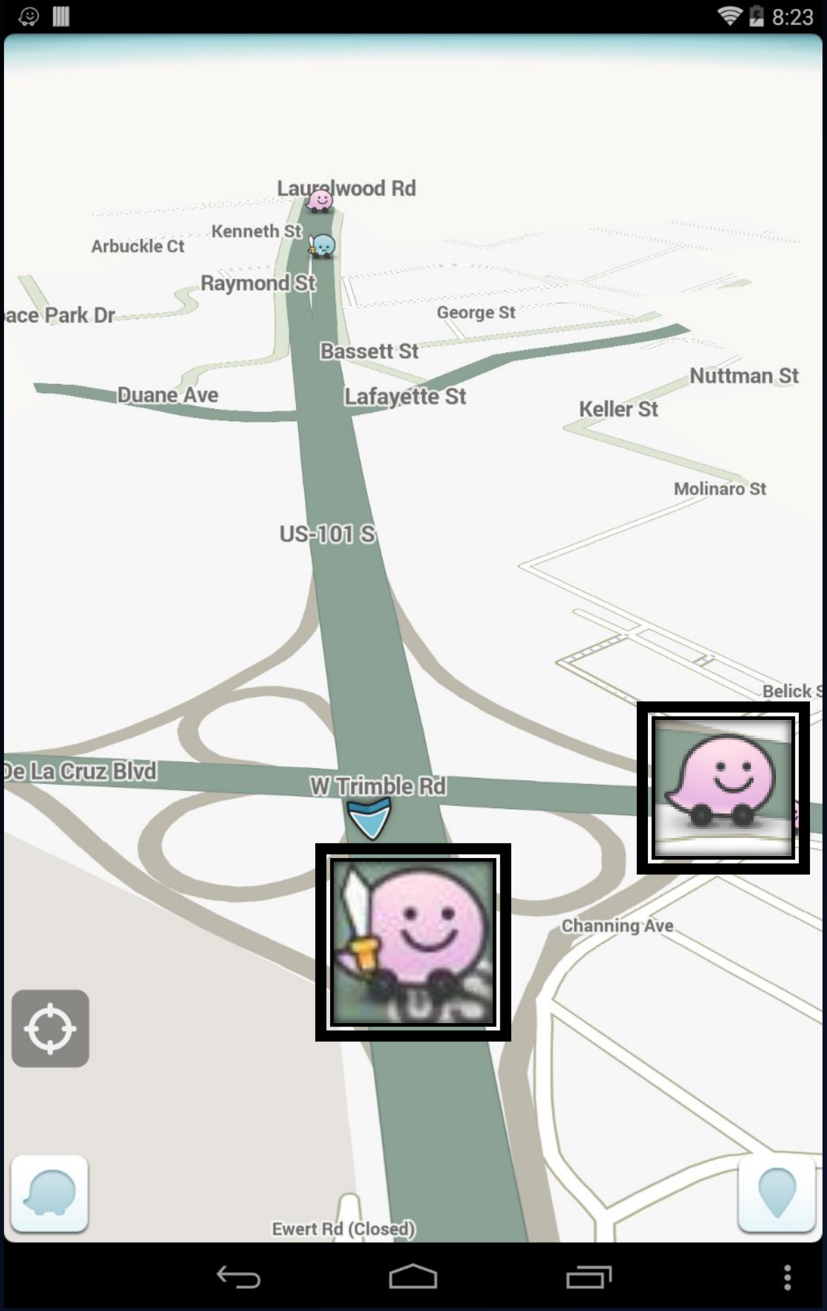


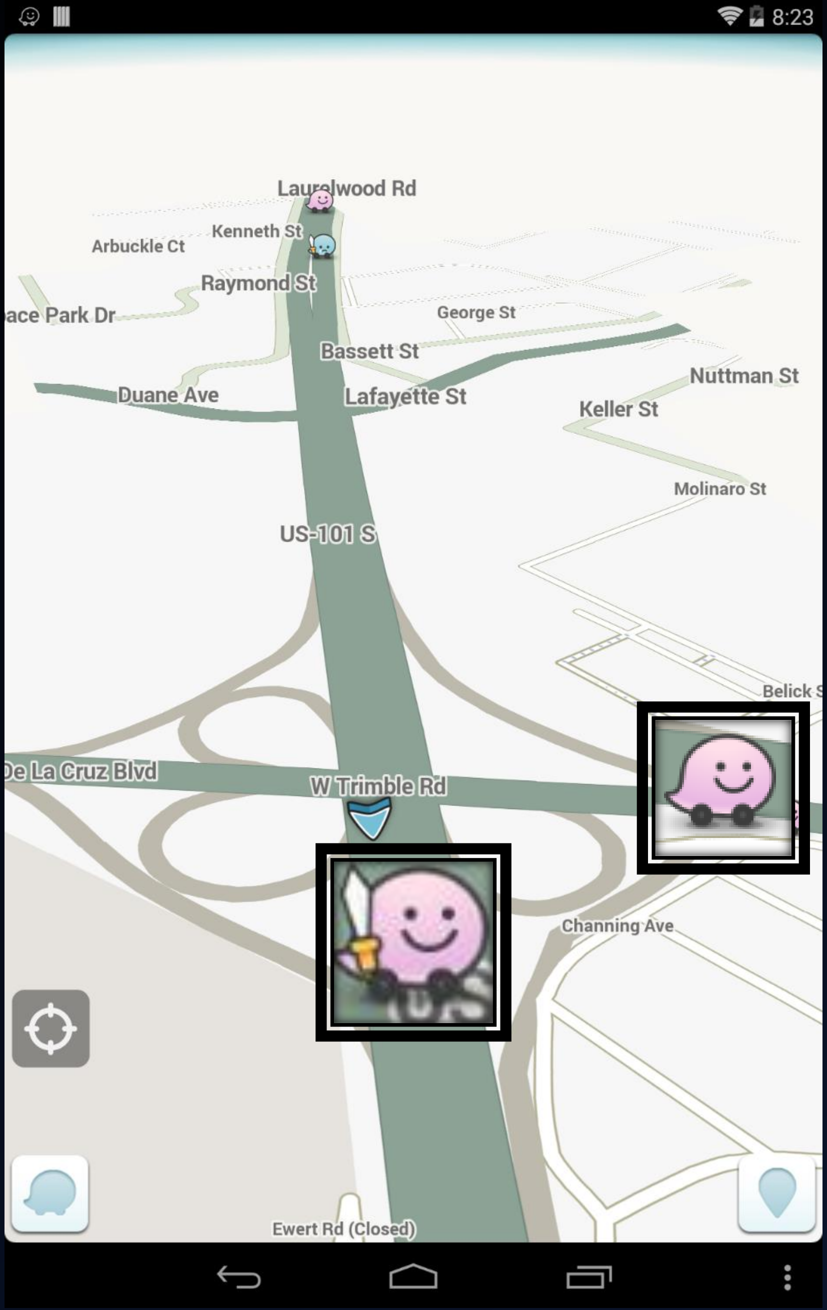
HectorOrrantia

Points: 52724 Rank: 385646

Joined one year ago

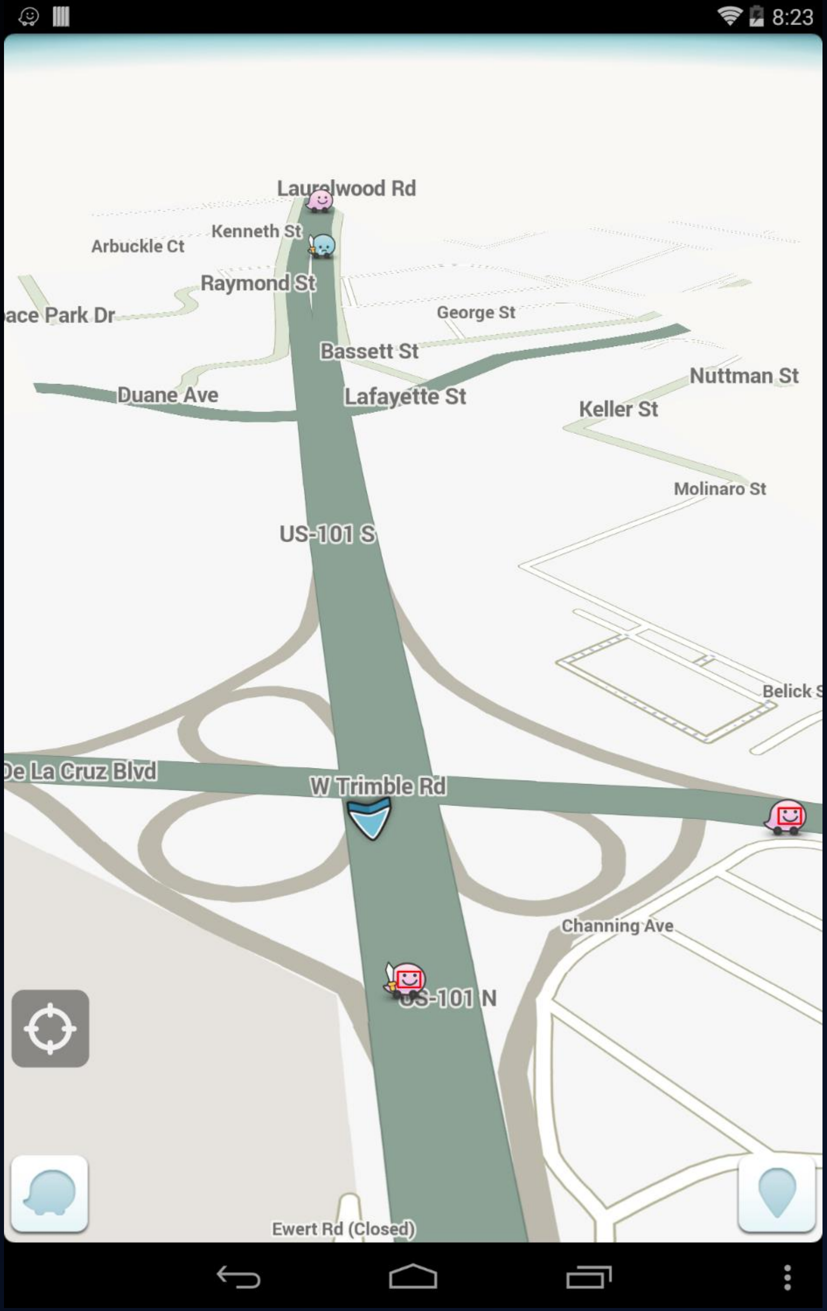
Speed: around 25 mph

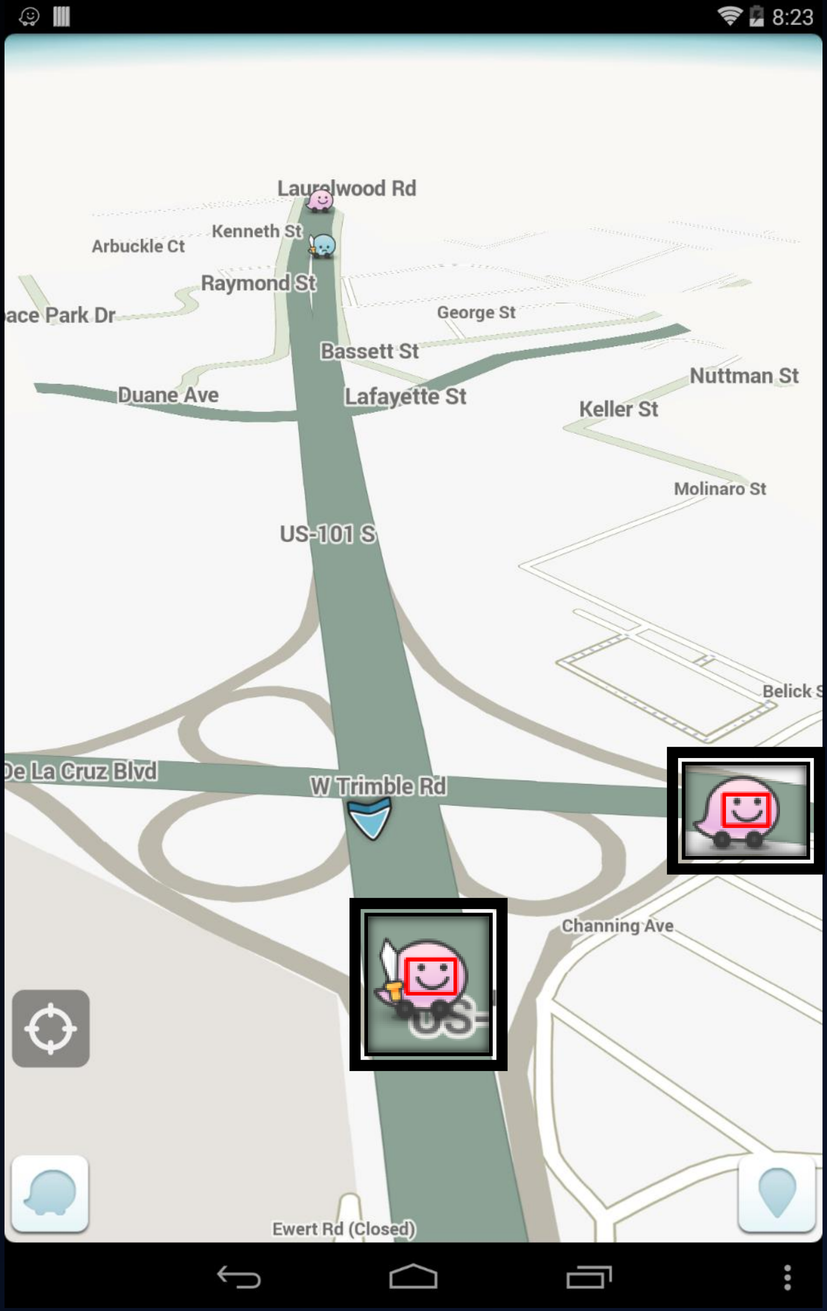

8:23
Laurelwood Rd
Kenneth St
Arbuckle Ct
Raymond St
ace Park Dr
George St
Bassett St
Duane Ave
Lafayette St
Nuttman St
Keller St
Molinaro St
US-101 S
Belick S
De La Cruz Blvd
W Trimble Rd
Channing Ave
Ewert Rd (Closed)

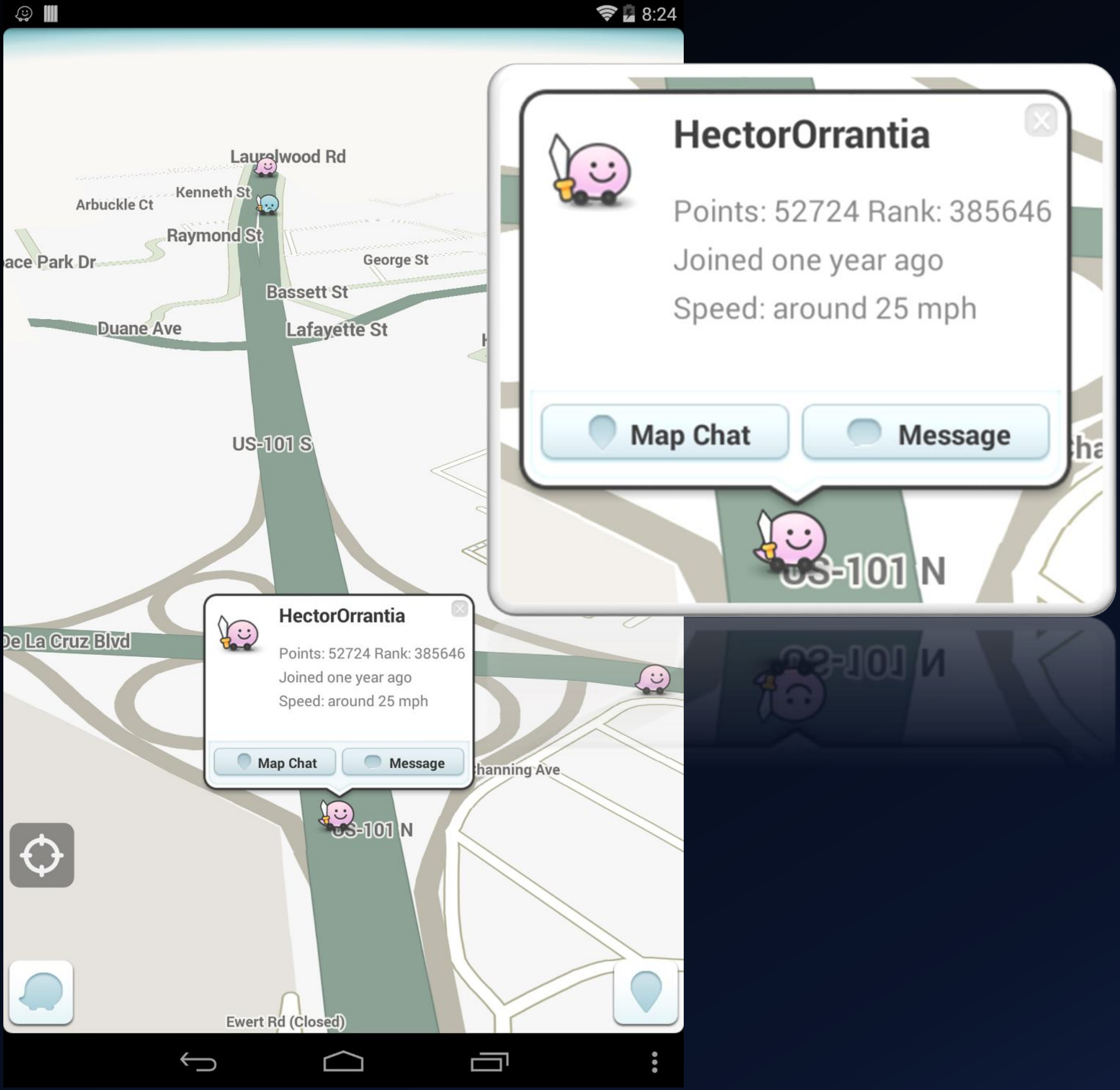

8:23
Laurelwood Rd
Kenneth St
Arbuckle Ct
Raymond St
ace Park Dr
George St
Bassett St
Duane Ave
Lafayette St
Nuttman St
Keller St
Molinaro St
US-101 S
Belick S
De La Cruz Blvd
W Trimble Rd
Channing Ave
Ewert Rd (Closed)

(:

You're Never Fully Dressed Without A Smile


8:23
Laurelwood Rd
Kenneth St
Arbuckle Ct
Raymond St
ace Park Dr
George St
Bassett St
Nuttman St
Duane Ave
Lafayette St
Keller St
Molinaro St
US-101 S
Belick S
De La Cruz Blvd
W Trimble Rd
Channing Ave
US-101 N
Ewert Rd (Closed)


8:23
Laurelwood Rd
Kenneth St
Arbuckle Ct
Raymond St
ace Park Dr
George St
Bassett St
Nuttman St
Duane Ave
Lafayette St
Keller St
Molinaro St
US-101 S
Belick S
De La Cruz Blvd
W Trimble Rd
Channing Ave
US-
Ewert Rd (Closed)



HectorOrrantia

Points: 52724 Rank: 385646

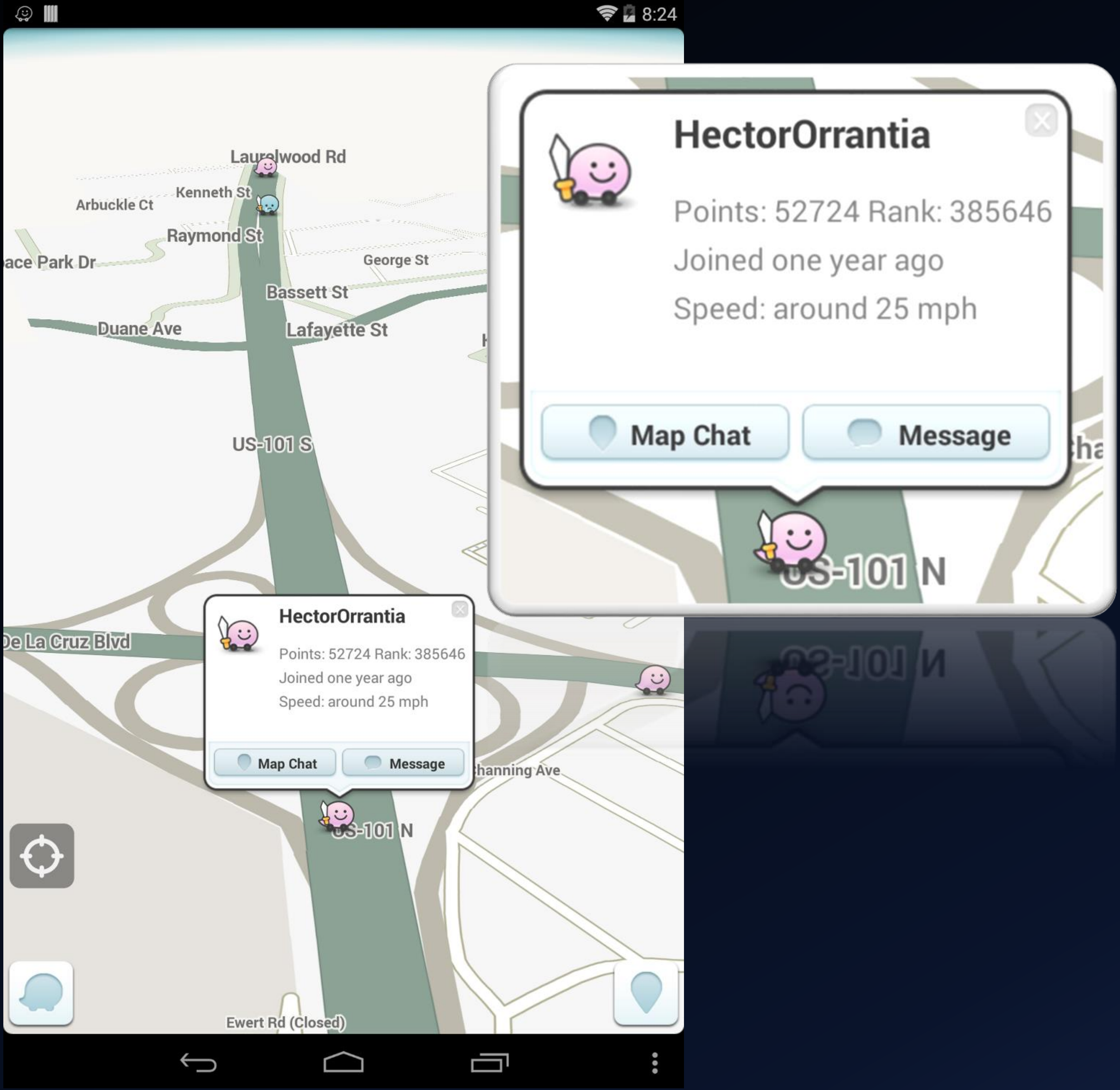
Joined one year ago

Speed: around 25 mph

Points

Rank

Joined



HectorOrrantia

Points: 52724 Rank: 385646

Joined one year ago

Speed: around 25 mph

HectorOrrantia

Points: 52724 Rank: 385646

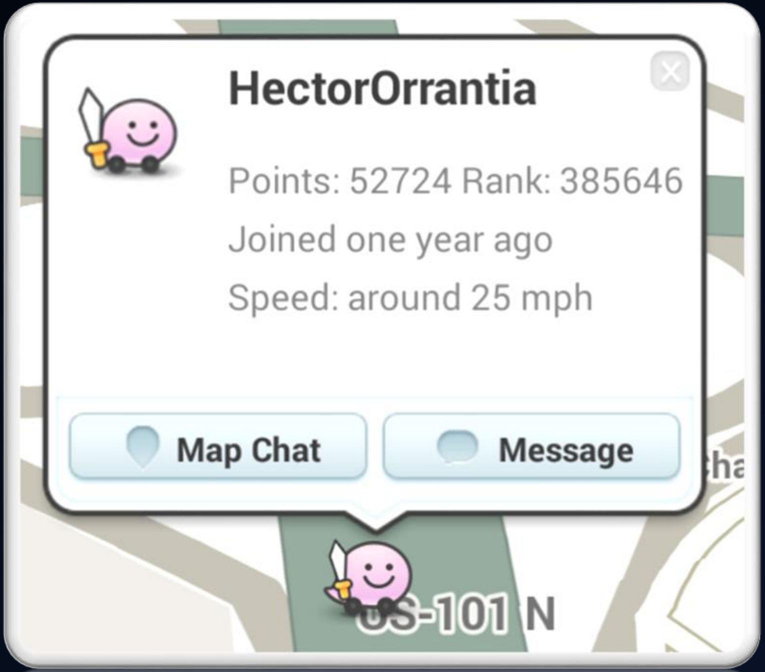
Joined one year ago

Speed: around 25 mph

Points

Rank

Joined



HectorOrrantia

Points: 52724 Rank: 385646

Joined one year ago

Speed: around 25 mph

HectorOrrantia

52724

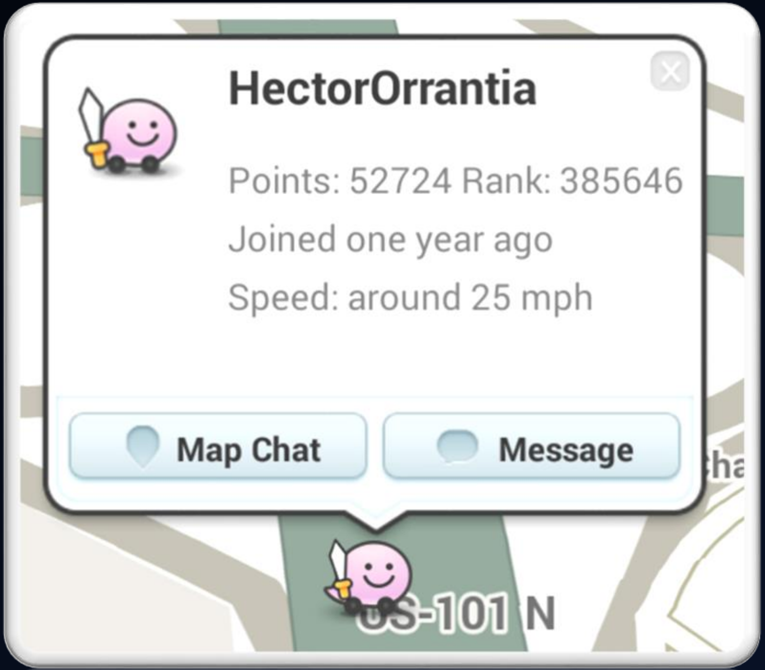
385646

one year ago

Points

Rank

Joined



HectorOrrantia

Points: 52724 Rank: 385646

Joined one year ago

Speed: around 25 mph

HectorOrrantia

52724

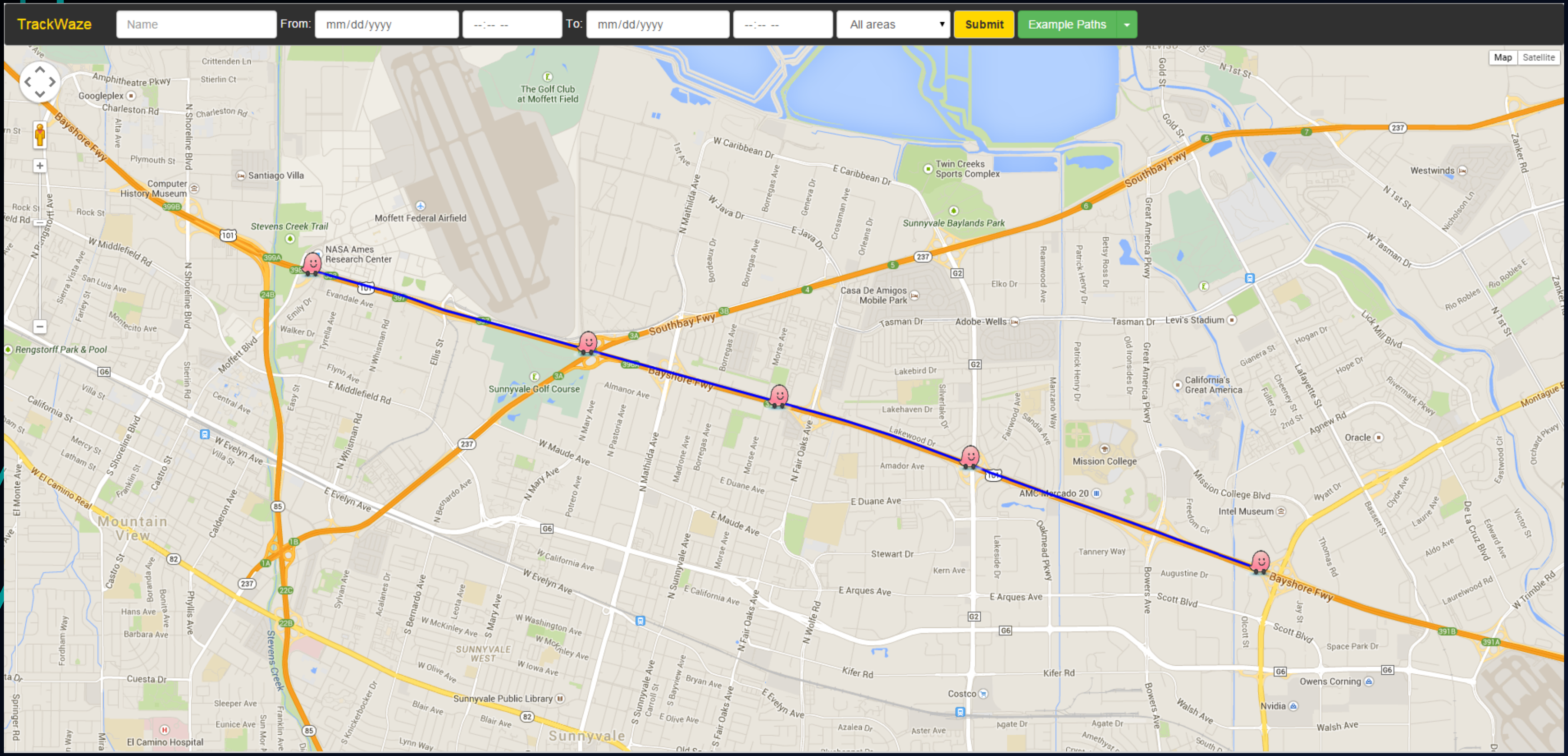
385646

one year ago

Hectororrantia

52724 385646

one year ago


TrackWaze
Name
From:
mm/dd/yyyy
--:-- --
To:
mm/dd/yyyy
--:-- --
All areas
Submit
Example Paths
Map
Satellite
Bayshore Fwy
Southbay Fwy
NASA Ames Research Center
Moffett Federal Airfield
The Golf Club at Moffett Field
Sunnyvale Golf Course
Googleplex
Computer History Museum
Santiago Villa
Stevens Creek Trail
Twin Creeks Sports Complex
Sunnyvale Baylands Park
Casa De Amigos Mobile Park
Adobe-Wells
Levi's Stadium
California's Great America
Mission College
AMC Mercado 20
Intel Museum
Oracle
Westwinds
Owens Corning
Nvidia
Costco
Sunnyvale Public Library
El Camino Hospital
Rengstorff Park &amp; Pool
Mountain View
Sunnyvale
SUNNYVALE WEST
Tasman Dr
Mission College Blvd
E Duane Ave
Kifer Rd
Scott Blvd
E Arques Ave
W El Camino Real
E Evelyn Ave
N Mathilda Ave
N Fair Oaks Ave
Lawrence Expy
Great America Pkwy
Montague Expy

Privacy Attack: Implications

- 2-way street
  - Track location from identity
    - Spy on people
    - Know if a target is near you
  - Infer identity from location
  - Infer persons of interest from location
- Attack can be focused
- R\W
  - Tracking is read, Spoofing is write

Mitigating Attacks

- Tracking attack: Waze allows you to opt out of the ‘Live map’
  - But this is not the default option
- Spoofing attack: Can be mitigated by using carrier information
  - Waze started doing this after the attack became pubic ☺
- Read more in the white paper!

Summary

- A Sybil attack on Social navigation is possible
- We demonstrated a spoofing & tracking attack
  - Attacks requires no RE-ing, uses the Waze mechanism against itself
- Tracked thousands of users
- Successfully created false congestion reports
  - Reproducible
  - Routing affected
  - **Vast implications**
- Suggested mitigation
  - Adapted by *Waze* (??)

Conclusions

- Users should beware of blindly trusting social applications
    - Even in reliable applications such as *Waze*
- Applications with millions of users can and should put more effort into security

Questions?