black hat ASIA 2015

Exploiting Social Navigation

Meital Ben Sinai

Nimrod Partush

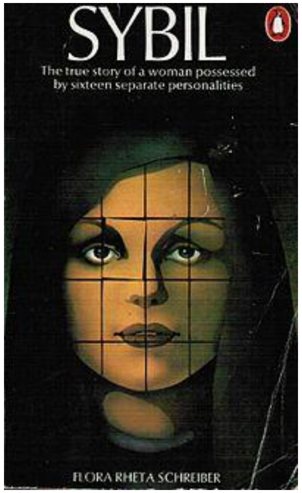
Shir Yadid

Eran Yahav

Research Goal

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

"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"


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

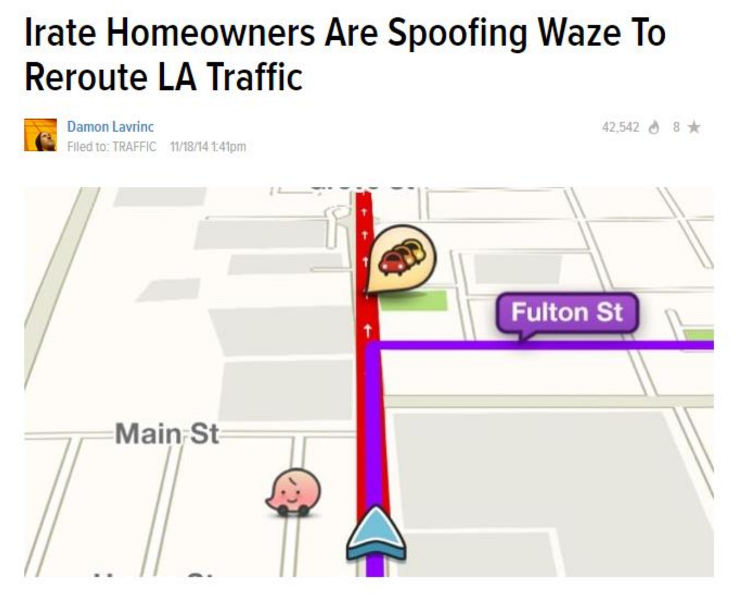
Social Navigation

- Social navigation apps **collect all their data from users**
  - Including maps and routes, congestion data etc.
  - They use the data to calculate routes and send users on the fastest one
- Waze is the prominent social navigation application
  - Used by over 50 million users
  - Affects **Google Maps**, Radio & TV Stations, etc.

Motivation

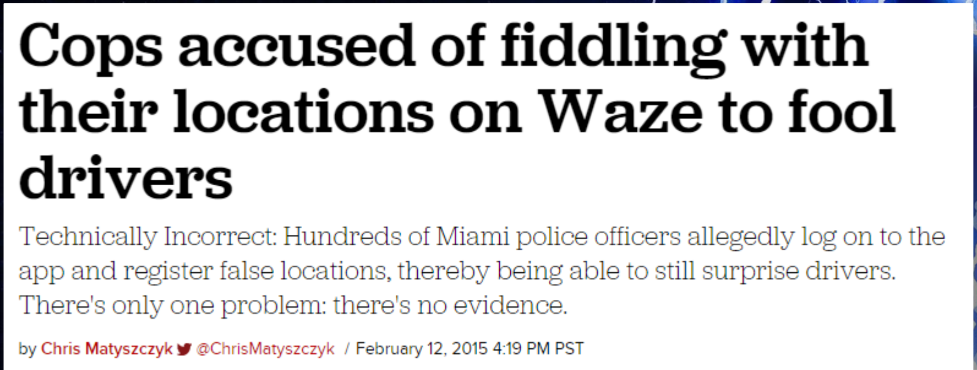
- Social data is becoming **reliable** data
  - — Facebook, 4Square, Swarmly, Waze
- Sybil attack never carried out in the navigation context
- Virtually no research done in attacking navigation applications
  - — One previous replay attack on Google floating car data published in BlackHat 13"

Motivation



Irate Homeowners Are Spoofing Waze To Reroute LA Traffic

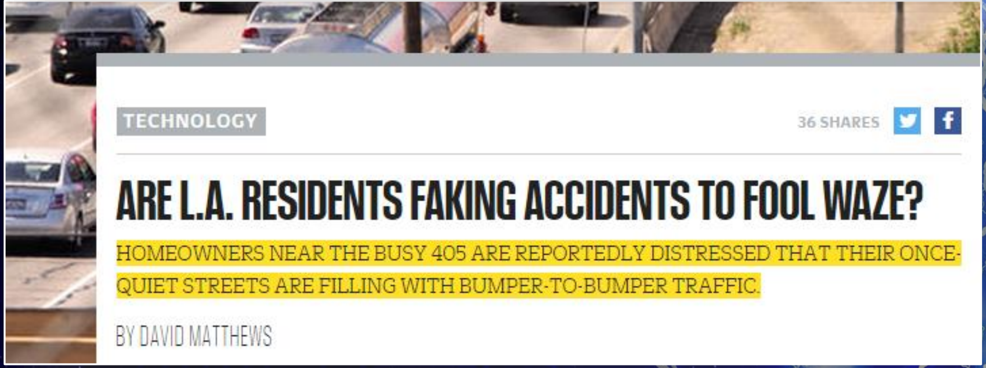
Damon Lavrinc 42,542 8
Filed to: TRAFFIC 11/18/14 1:41pm



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



TECHNOLOGY 36 SHARES

ARE L.A. RESIDENTS FAKING ACCIDENTS TO FOOL WAZE?

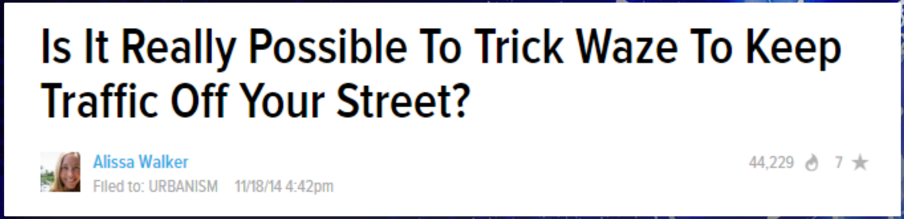
HOMEOWNERS NEAR THE BUSY 405 ARE REPORTEDLY DISTRESSED THAT THEIR ONCE-QUIET STREETS ARE FILLING WITH BUMPER-TO-BUMPER TRAFFIC.

BY DAVID MATTHEWS

PISSED OFF L.A. HOMEOWNERS

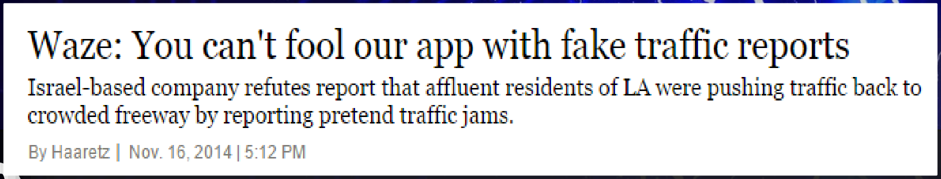
WAZE IS THE DEVIL!

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



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



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

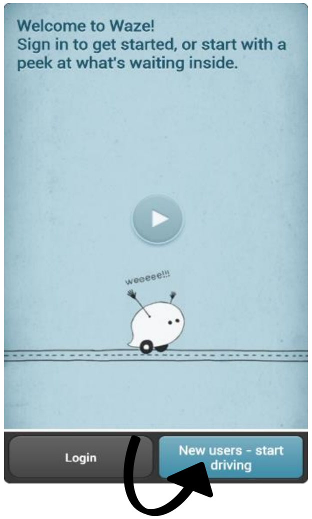
Attacks

Attack #1 – Creating False Congestion & Affecting Routing

- (Insert Demo Here)

Creating Bot Drivers

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



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

Creating False Congestion

- WAZE deduces traffic congestion and routing time information from location and movement data reported by its users
  - This algorithm resides on the server side of the WAZE system and was never publicly disclosed
- The main challenge of this work, was experimentally deducing and exploiting this algorithm.
- Our experiments consisted of explorative adjustment of the following parameters:
  - Data set size (# of bots)
  - Drive duration
  - Speed and movement pattern

Creating False Congestion

- Initially, we spawned botnets of increasing sizes and scattered them at the target area
  - No congestion was reported
- 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
    - Still, no jam ☹
- The WAZE congestion reporting algorithm is a relative one
  - 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 included an initial phase of fast driving, followed by a gradual slowdown

Affecting Routing

- Faking congestion affects WAZE routing
  - Sends users on other routes
- Vast financial and security implications.
  - Clear roads for attacker
  - Waste time & fuel of benign users
  - Make users avoid congested toll roads, businesses in congested regions
  - Force users down an attacker controlled road
  - Etc.

Attack #2: Tracking Users

- (Insert Demo Here)

Tracking Users

- Bots are deployed over the target area
- The surroundings are analyzed to find users, display their data and extract text
  - Using OpenCV, Tesseract
  - This requires no RE
- The data, along with GPS coordinates and time of day are stored in a DB
- The DB is searched to correlate re-appearing handles and join them into routes

Tracking Anonymous Users

- Using location data and knowing a probable route for a (real life) individual could supply you with their Waze handle
  - — And then you can target the tracking better and even affect their routing ☺
- Note that changing the handle will not help

Attack System

- Attack #1:
  - WAZE clients emulated using the ADT emulator
  - Mock GPS locations generated via android application
  - Emulators controlled using the Android Debug Bridge
    - Controlled via python scripting
  - All running on faculty servers
- Attack #2:
  - WAZE clients were actual devices
    - Since we required good images for manipulation

Defense

Mitigating Attacks

- We discuss two approaches for mitigating the 1st attack:

1. **Behavioral** analysis
2. Relying on **carrier data**

- We compare these by parameters of **simplicity**, **user experience**, **security level** and **cost**

Behavioral Analysis

- Relying on existing validation mechanisms
  - Add CAPTCHAS or use Google\Facebook validation
    - And give better standing to these users
- Network Traffic Analysis
  - Give better standing to 3G addresses
- Analyzing user Creation, Movement & Report patterns
  - bots were created together, drove repeatedly on the same road, with same movement patterns
  - Could detect based on **individual** or **group** behavior
- **Overall: Cheap** & relatively **user friendly** but **complex** and **less secure**

Relying on Carrier Data

- Upon registration, WAZE can retrieve and validate user cellular number
  - Force attackers to buy SIM cards
  - Registration process no longer easily automated
- Query the carrier to receive the cell tower the user is currently near
  - Using the user provided phone number
- Cross reference with their reported GPS location
  - Mark those who fail as potential bots
- Simple, secure and user friendly solution.
  - Is it 100% secure?

Mitigating Attacks

- Waze allows you to opt-out of appearing on the live map
  - This is sufficient to mitigate the attack
- However that is not that default, and the user is not notified of the risk
- Showing fellow users without displaying their data will mitigate the attack as well

Summary

- A Sybil attack on Social navigation is possible
- We demonstrated two cheap, easily facilitated attack
- Successfully created false congestion reports
  - — Reproducible
  - — Routing affected
  - — Vast implications
  - — Two approaches for mitigating
    - Simple, secure and expensive vs. Complex, breakable and cheap.
- Successfully tracked users