Exploiting Social Navigation

MEITAL BEN SINAI
NIMROD PARTUSH
SHIR YADID
ERAN YAHAV

Technion, Israel
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*!
Exploiting Social Navigation - Black Hat Asia 2015

Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav

Israeli Students Spoof Waze App With Fake Traffic Jam

Estudiantes reportan un embotellamiento falso en Waze que duró horas

Fake Traffic Jams Can Be Created on Waze

Israeli Students Spoof Waze App With Fake Traffic Jam

A traffic jam generated via Waze. The image shows a map with a traffic jam, possibly demonstrating the concept of creating fake traffic jams using the Waze app.

Read more...
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”
Motivation

Irate Homeowners Are Spoofing Waze To Reroute LA Traffic

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?

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

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

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

Exploiting Social Navigation - Black Hat Asia 2015 - Meital Ben Sinai, Nimrod Partush
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!
nimi@csl-circus:~$ bash StartAndLogin.sh
Exploiting Social Navigation - Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav
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
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

- Presumably, 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
You're Never Fully Dressed Without A Smile
Exploiting Social Navigation - Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav
Exploiting Social Navigation - Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav
Points
Rank
Joined
Points: 52724
Rank: 385646
Joined one year ago
Speed: around 25 mph

HectorOrrantia
Exploiting Social Navigation - Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav
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 public 😊

• 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?