Exploiting Social Navigation

MEITAL BEN SINAI
NIMROD PARTUSH
SHIR YADID
ERAN YAHAV

Technion, Israel
Outline

• Intro
• Goals & Motivation
• Attacks (+Demos \(^{(^o^)}\)/)
• 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

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”
Motivation

Irate Homeowners Are Spoofing Waze To Reroute LA Traffic

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

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

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

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

Miami cops are sending fake data to Waze to stop people from knowing speed trap locations
Attacks
Attack #1: Creating False Congestion & Affecting Routing

• (Insert Demo Here)
Navigation
Successful Attack
Navigation has Changed!
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

- (Insert Demo Here)
Exploiting Social Navigation - Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav
Exploiting Social Navigation - Meital Ben Sinai, Nimrod Partush, Shir Yadid, Eran Yahav
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

HectorOrrantia

52724 385646

one year ago
Points: 52724  Rank: 385646
Joined one year ago
Speed: around 25 mph
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

• Undergrads* can be useful
Questions?