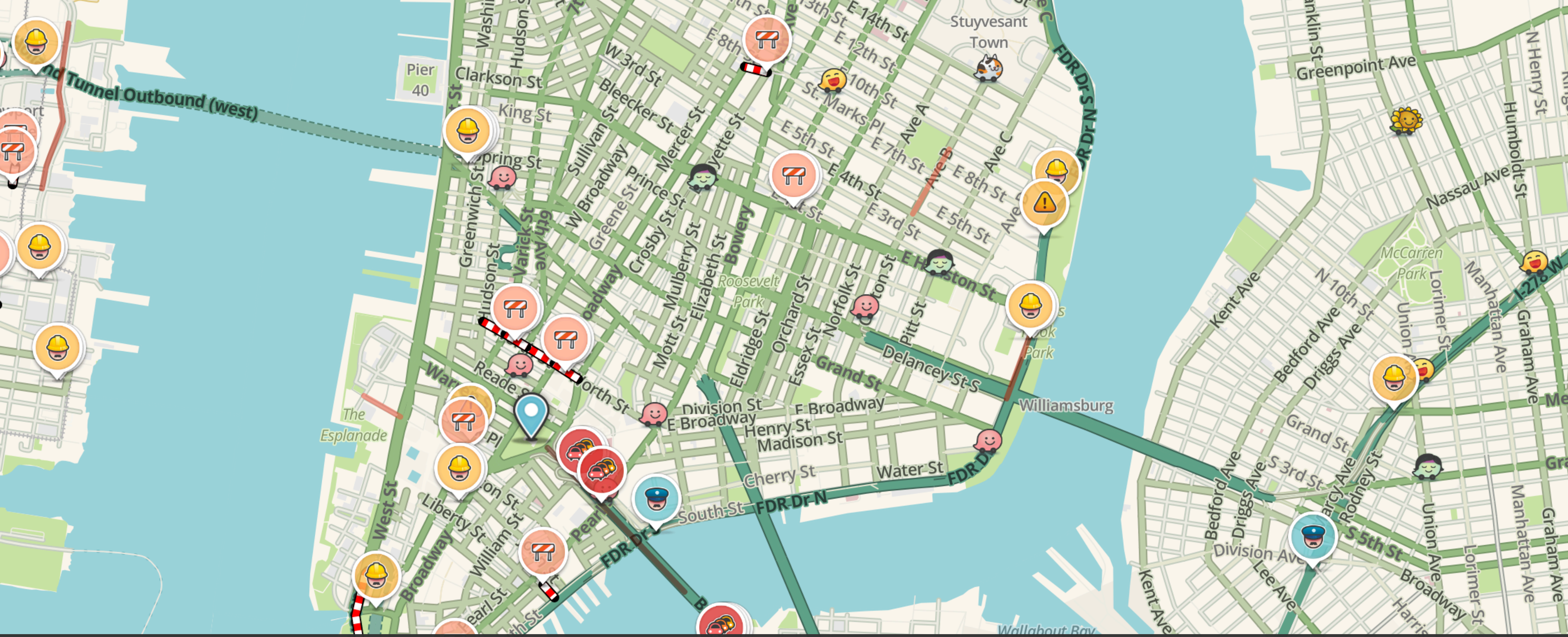


Sybil Devices in Crowdsourced Mapping Services

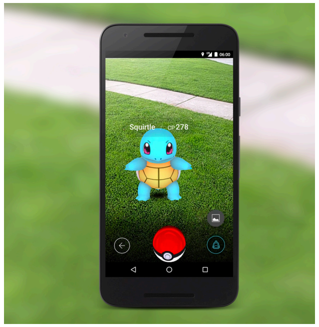
Gang Wang,[+] Bolun Wang, Tianyi Wang, Ana Nika, Haitao Zheng, Ben Zhao

[+]Virginia Tech UC Santa Barbara

gangwang@vt.edu

Mobile Phone = Your Identity?

- Mobile phones for content, payment, authentication



BOARDING PASS

Wiebke Moehle

Seat 18A | Board at Rear Door of aircraft

Flight EZY147 | Date 04 Jun 14

London Luton LTN ✈ Aberdeen ABZ

Flight Departs 7:00 PM | Gate Closes 6:30 PM | Booking EMJ7B4T

Queue 2 | Type S | Seq. number 505 | Doc. number

YOU'RE

Username

Password

□ Remember Me

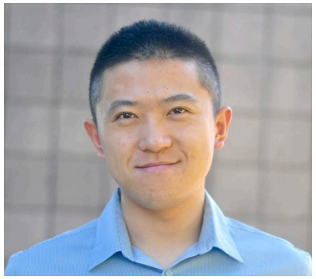
Log In

Lost your password?

← Back to Jack Reichert

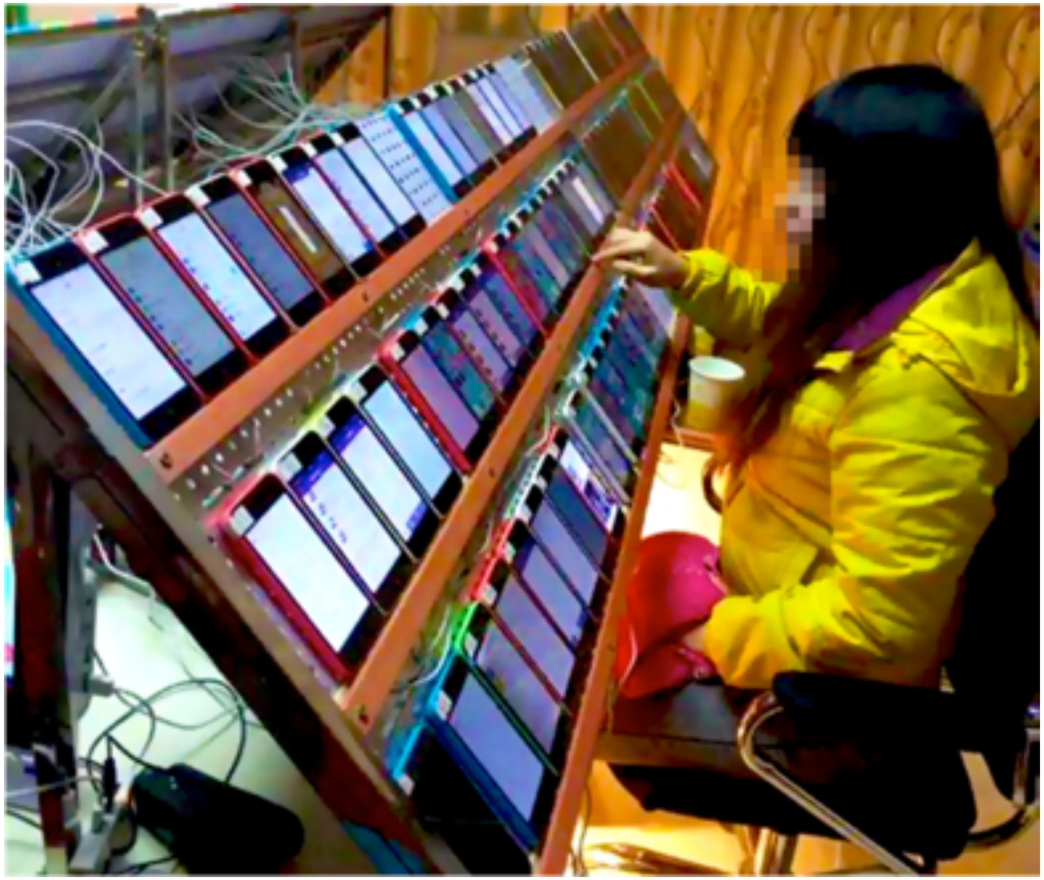
- Mobile devices are virtual representations of ourselves.

=

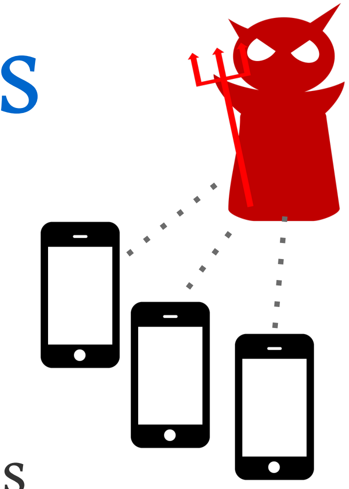


But Is This a Safe Assumption?

- An app user = 1 real phone + 1 real person



Threat of Sybil Devices



- Sybil devices
  - Software scripts emulating as real devices
  - Allowing a single user to control many devices
- In the context of Waze (popular navigation app)
  - Creating a large number of Sybil devices with low costs
  - Attacks: injecting fake events, user location tracking
  - Generalizable to other mobile communities

waze Key Features

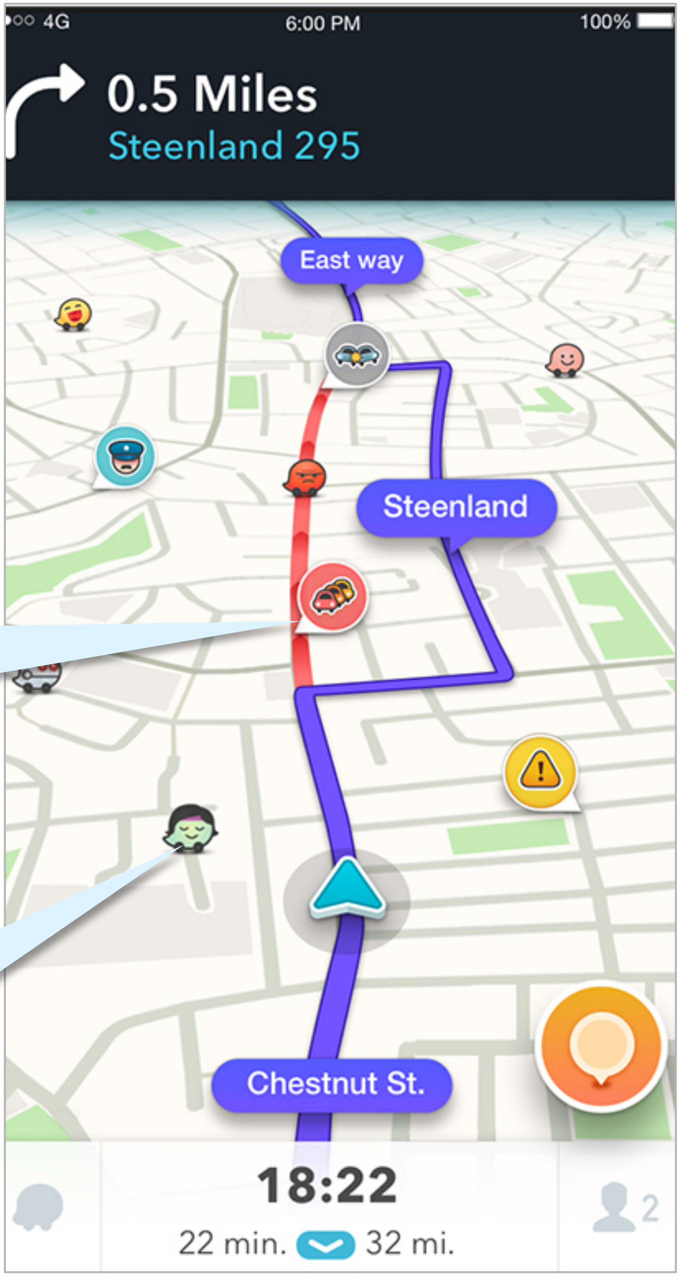
- 50M active users
- Real-time traffic update using millions of users' locations

User reported events

- Accidents, police trap, etc.
- Alert users of nearby events

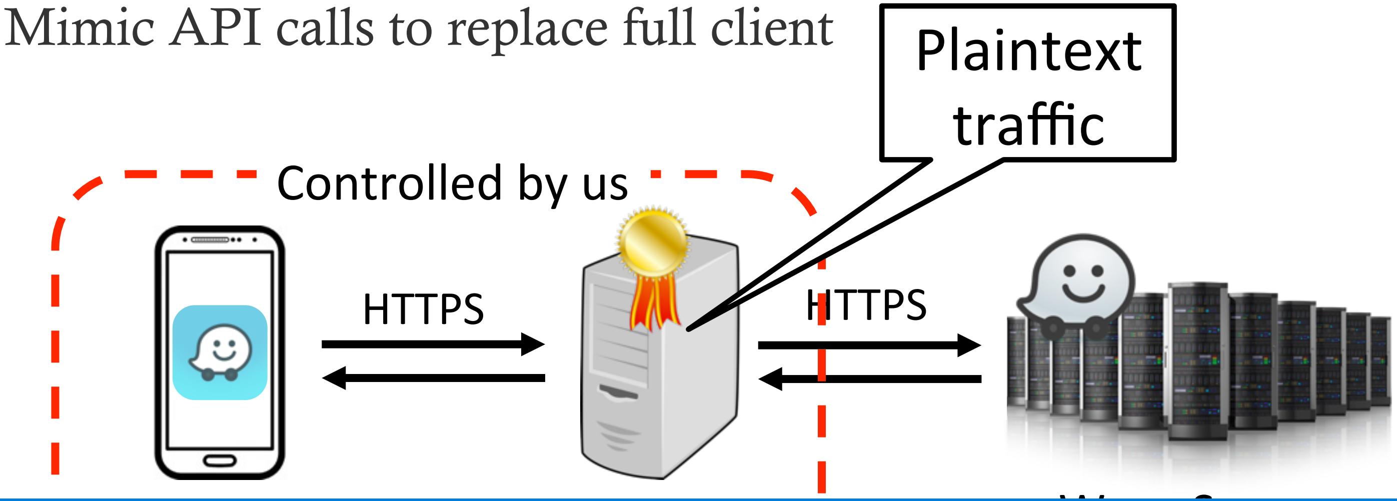
Social features

- See nearby users on the map
- Say "hi"/msg nearby users



Creating Sybil Devices

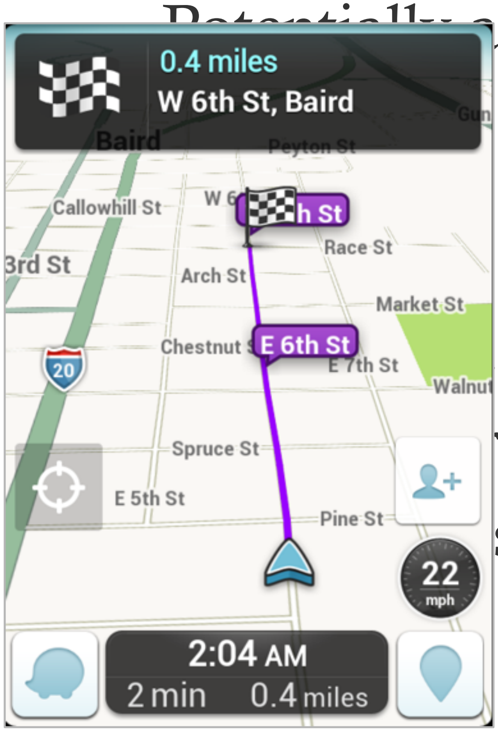
- Naïve approach: mobile emulators
  - Not scalable: ~10 emulators per PC
- Our way: emulate a mobile client using scripts
  - Server communicates with client via limited APIs
  - Mimic API calls to replace full client



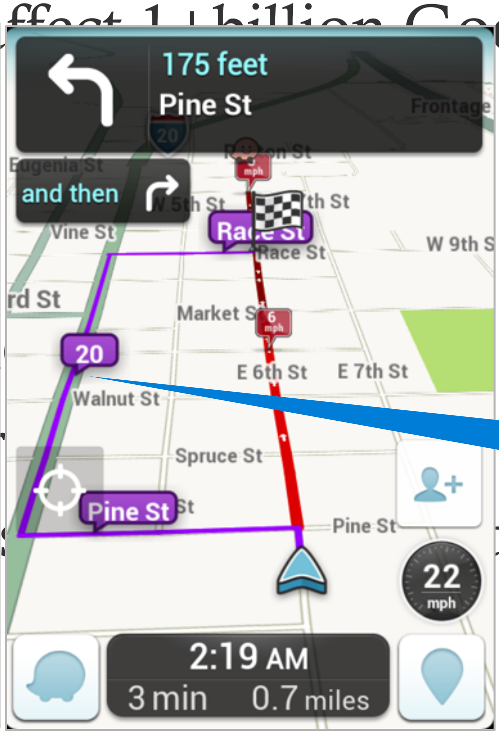
We can create 10,000 Sybil devices on a single PC

Attack #1: Polluting Waze Database

- Fake road-side events.
  - Any type of event at any location
  - Potentially affect 1+billion Google Maps users



Before

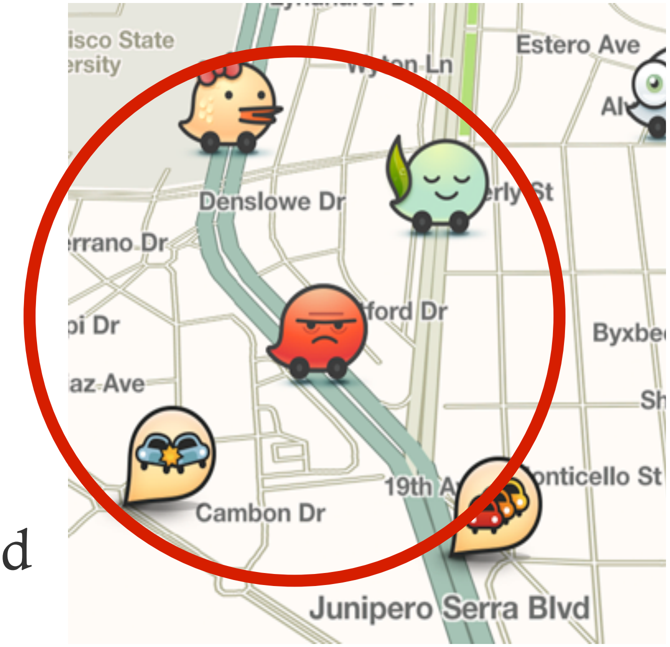


After

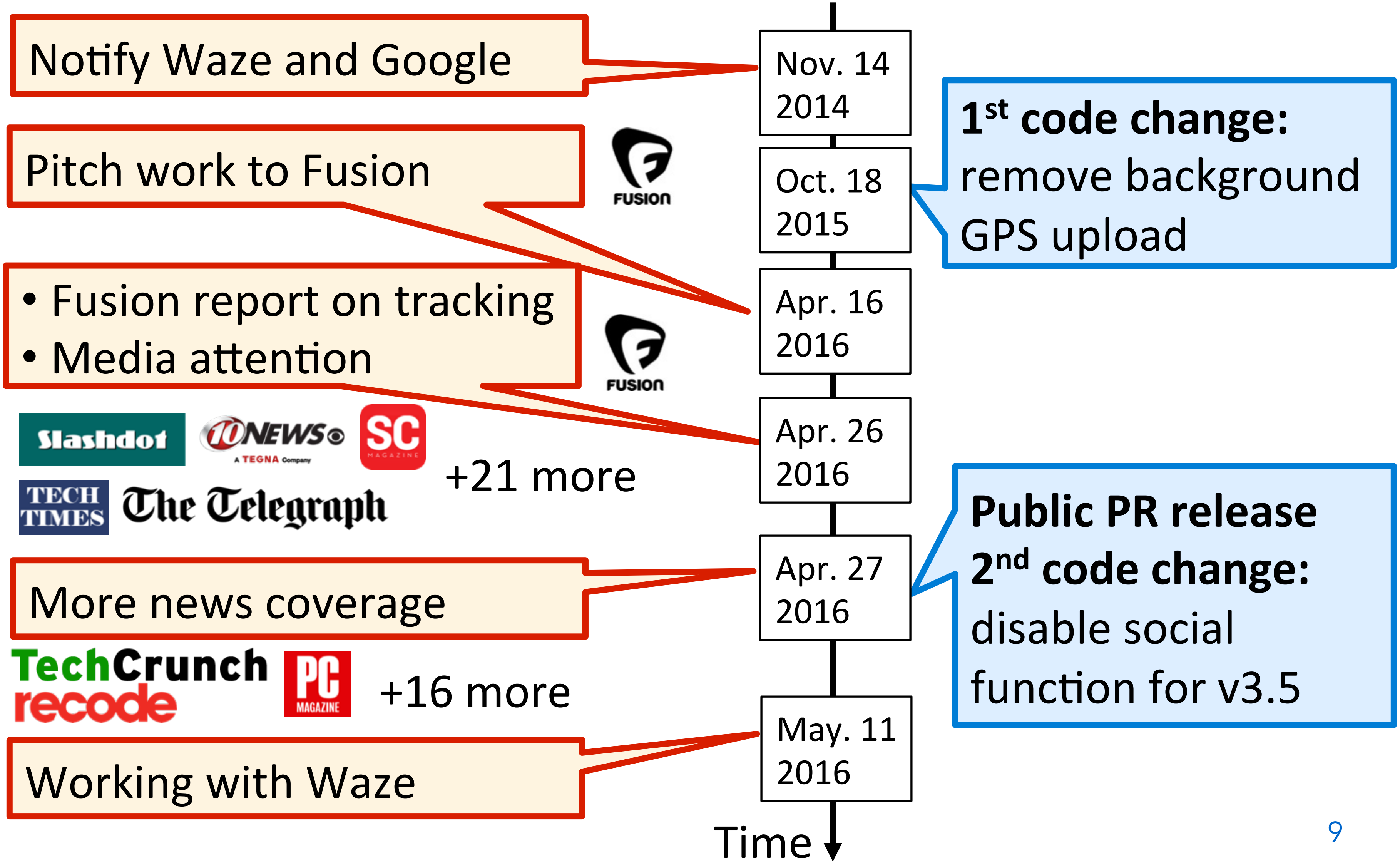
Users are re-routed

Attack #2: User Location Tracking

- Follow (stalk) any Waze user in real-time
  - Waze marks nearby users on the map
- Pinpoint to exact GPS location
  - Specific hotels, gas stations, etc.
- Remain invisible
  - Move in and out quickly
- Track users in the background
  - Waze uploads GPS in the background
- Track users across days
  - Use creation time as GUID



Conversation With Waze



Notify Waze and Google

Nov. 14 2014

Pitch work to Fusion

Oct. 18 2015

1st code change: remove background GPS upload

- Fusion report on tracking
- Media attention

Apr. 16 2016

Apr. 26 2016

+21 more

Apr. 27 2016

More news coverage

+16 more

Public PR release

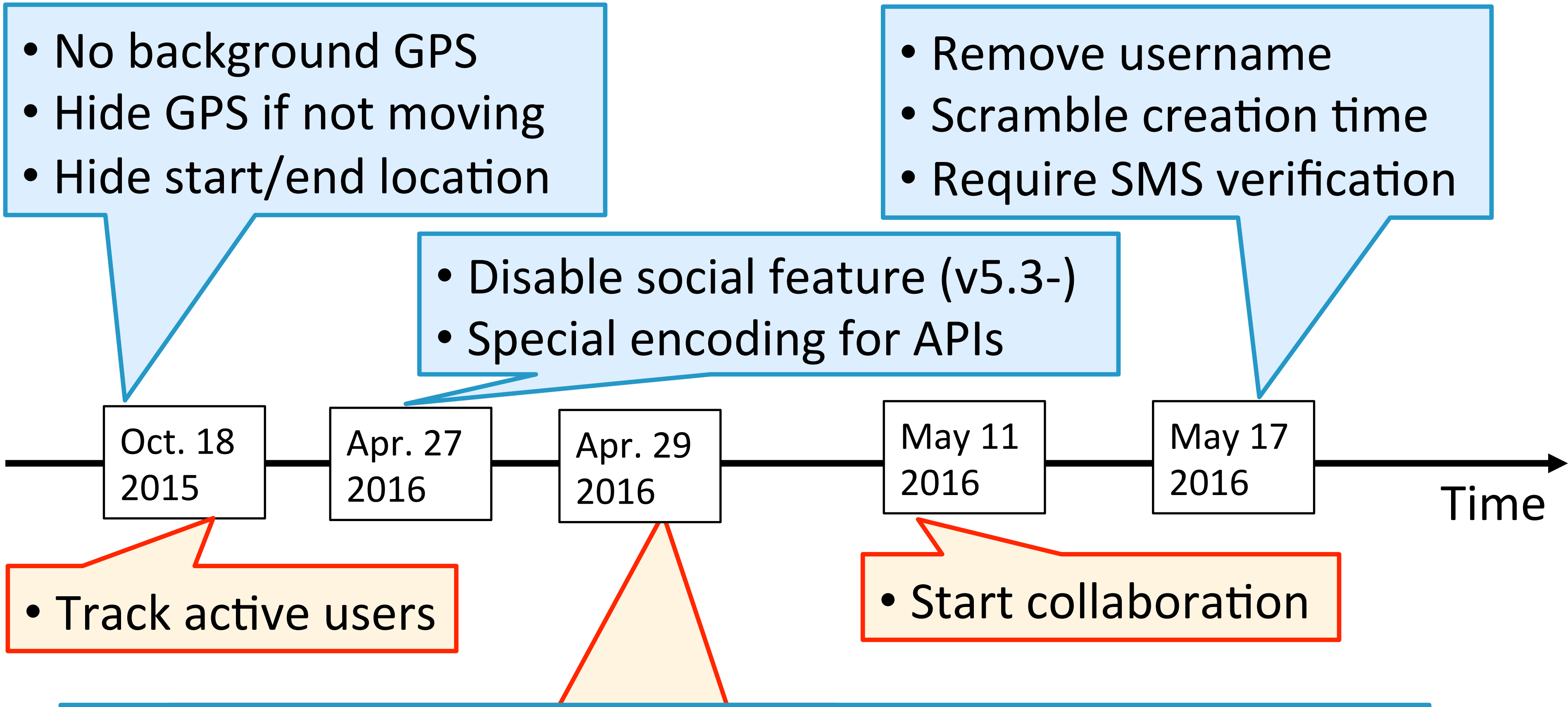
2nd code change: disable social function for v3.5

Working with Waze

May. 11 2016

Time

Waze's Security Measures



- No background GPS
- Hide GPS if not moving
- Hide start/end location

- Disable social feature (v5.3-)
- Special encoding for APIs

- Remove username
- Scramble creation time
- Require SMS verification

Oct. 18 2015

Apr. 27 2016

Apr. 29 2016

May 11 2016

May 17 2016

Time

- Track active users

- Start collaboration

- Yes, we can still track Waze users
- Much less location information being shared

Discussion

- How to defend against Sybil devices?
  - Sybil detection based on *physical proximity* [our paper]
  - Device authentication

- Apply similar methods to DAT research?
  - Understanding mobile APIs, improving transparency
  - Understanding data disclosure for better privacy

- What ethical principles should we follow?