Poster: Defending against Sybil Devices in Crowdsourced Mapping Services

Gang Wang[†], Bolun Wang[†], Tianyi Wang[†‡], Ana Nika[†], Haitao Zheng[†], Ben Y. Zhao[†]
[†]Department of Computer Science, UC Santa Barbara
[‡]Department of Electronic Engineering, Tsinghua University
{gangw, bolunwang, tianyi, anika, htzheng, ravenben}@cs.ucsb.edu

ABSTRACT

Crowdsourcing is a unique and practical approach to obtain personalized data and content. Its impact is especially significant in providing commentary, reviews and metadata, on a variety of location based services. In this study, we examine reliability of the Waze mapping service, and its vulnerability to a variety of location-based attacks. Our goals are to understand the severity of the problem, shed light on the general problem of location and device authentication, and explore the efficacy of potential defenses. Our preliminary results already show that a single attacker with limited resources can cause havoc on Waze, producing "virtual" congestion and accidents, automatically re-routing user traffic, and compromising user privacy by tracking users' precise movements via software while staying undetected.

1. ATTACKS AND INITIAL EXPERIMENTS

Waze is a popular crowdsourced mapping service with more than 50 million users globally as of June 2013 [1]. Waze enables its navigation and map services by leveraging crowdsourced data gathered from its large user community. It collects users' GPS information to infer traffic condition, and allows users to post real-time alerts on their routes.

While crowdsourcing data is the key enabler of Waze service, the lack of verification on this user generated data also makes Waze vulnerable to data manipulation. Today's mobile location data could be easily spoofed and there is no reliable, scalable mechanism for authentication. An attacker could easily feed fake information into Waze and manipulate operations like routing. Taking this attack to a massive scale, emulation of large amount of mobile devices is possible using low cost emulators or even scripts. This enables a resource-limited attacker to produce an army of "virtual" Waze users and produce enough data to take over Waze database in any desired area.

Attacks on Crowdsourced Maps. There are three primary attacks on crowdsourced mapping services like Waze [1]. *First*, an attacker can generate fake events, like accidents, construction, and speed traps. *Second*, an attacker can produce "virtual congestion" by reporting slow-moving GPS traces from a group of vehicles. *Finally*, a fake mobile user can "virtually" follow any individual user as long as their Waze application is active, even in the background. This presents the biggest risk to Waze users, as Waze locations can pinpoint users to within meters of their actual location.

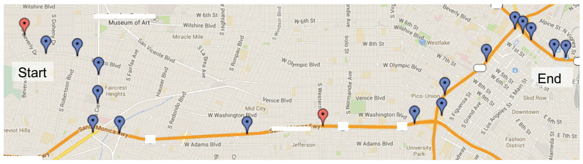

Figure 1: Tracking in downtown Los Angeles. Blue dots are captured points, while red dots are missed.

We have performed initial validation of all three attacks. Especially for invasive tracking, we were able to track ourselves driving with Waze turned on. We performed the experiment in high traffic and user density area, thus demonstrating that single users can be tracked even through crowded areas (Fig. 1).

As common ways of defense, better pruning and filtering on speed data could limit the impact of fake data. But such mechanisms could be easily overwhelmed by a sufficient number of cooperating virtual devices. As a proof of concept, we used a low-end server to simulate 1,000 Sybil devices, which is sufficient to launch all attacks mentioned above.

2. DEFENSE AND FUTURE DIRECTIONS

We propose a proximity-based authentication which prioritizes scalability and easy deployment. In a high level, our approach leverages the physical proximity between real devices to authenticate each other and propagate credibility. We bootstrap from an initial set of trusted users. When two devices come into proximity with each other, "trusted" user could propogate the credibility to the "untrusted" user by verifying each other via Waze. Waze provides one user with a time-varying WiFi SSID as a challenge, and tests if the other user can respond correctly. As trust propagates to the rest of users, we can detect Sybil devices using similar idea in community-based Sybil detection in social networks [2].

Future Directons Moving forward, we plan to extend the study to larger sets of mobile applications. Our goal is to better understand the severity of lack of location and device authentication. Also, we are exploring scalable and reliable approaches to authenticate physical devices.

3. REFERENCES

[1] V. Goel. Maps that live and breathe with data. The New York Times, June 2013.

[2] H. Yu et al. Sybilguard: defending against sybil attacks via social networks. In *Proc. of SIGCOMM*, 2006.

[1] This work is to appear in MobiSys'16.

MobiSys'16 Companion June 25-30, 2016, Singapore, Singapore

ACM ISBN 978-1-4503-4416-6/16/06.

DOI: http://dx.doi.org/10.1145/2938559.2938610