IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 1,Issue 1,Jan 2013

Ghost Riders: A New Approach based on Co-Location Edges

Arjumand Jamal

Abstract—

Real-time crowdsourced maps, suchas Waze provide timely updates on traffic, congestion, accidents, and points of interest. Inthis paper, we demonstrate how lack of strong location authentication allows creation of software-based Sybil devices that exposecrowdsourced map systems to a variety of security and privacy attacks. Our experiments show that a single Sybil device with limited resources can cause havoc on Waze, reporting false congestion and accidents and automatically rerouting user traffic. More importantly, we describe techniques to generate Sybil devices at scale, creating armies of virtual vehicles capable of remotely tracking precisemovements for large user populations while avoiding detection. To defend against Sybil devices, we propose a new approach based on co-location edges, authenticated records that attest to the one-time physical colocation of apair of devices. Over time, co-location edgescombine to form large proximity graphs that attest to physical interactions between devices, allowing scalable detection of virtual vehicles. We demonstrate the efficacy of this approach using large-scale simulations, and how they can be used to dramatically reduce the impact of the attacks. We have informed Waze/Google team of our research findings. Currently, we are in active collaboration with Waze team to improve the security and privacy of theirsystem.

Keywords: Crowd sourcing, Sybil attack, Collocation edges.

INTRODUCTION

Crowdsourcing is indispensable as a real-time data gathering tool for today‟s online servicesTake for example map and navigation services. Both Google Maps and Waze use periodic GPS readings from mobile devices to infer traffic speed and congestion levels on streets and highways. Waze, the most popular crowdsourced map service, offers users more ways to actively share information on accidents, police cars, and even contribute content like editing roads, landmarks, and local fuel prices. This and the ability to interact withnearby users made Waze extremely popular, with an estimated 50 million users when it was acquired by Google for a reported $1.3 Billion USD in June 2013. Today, Google integrates selected crowdsourced data (e.g. accidents) from Waze into its own Maps application.

Assistant professor, Department of Computer Science and engineering, Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad, 500059

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 1,Issue 1,Jan 2013

Unfortunately,systems that rely on crowdsourced data are inherently vulnerable to mischievous or malicious users seeking to disrupt or game the system [1]. For example, business owners can badmouth competitors by falsifying negative reviews on Yelp or TripAdvisor, and FourSquare users can forge their physical locations for discounts [2], [3]. For location-based services, these attacks are possible because there are no widely deployed tools to authenticate the location of mobile devices. In fact, there are few effective tools today to identify whether the origin of traffic requests are real mobile devices or software scripts.

FIGURE:1. Example for Sybil attack

Waze is the most popular crowdsourced navigation app on smartphones, with more than 50 million users when it was acquired by Google in June 2013 [9]. Waze collects GPS values of users‟ devices to estimate real-time traffic. It also allows users to report on-road events such as accidents, road closures and police vehicles, as well as editing roads and even updating local fuel prices.Waze‟s main feature is assist users to find the best route to their destination and turn-by-turn navigation. Waze generates aggregated real-time traffic updates using GPS data from its users, and optimizes user routes both during trip planning and during navigation. If and when traffic congestions is detected, Waze automatically re-routes users towards an alternative.

RELATED WORK

You Unlocked the Mt.Everest Badge on Foursquare! Countering Location Fraud in GeoSocial Networks [2]GeoSocial Networks (GSNs) are online interpersonal organizations fixated on the area data of their clients. Clients "registration" their area and use it to procure area based unique status (e.g., identifications, mayorships) and get setting subordinate prizes. The technique of compensating client investment anyway makes duping a gainful conduct. In this paper we present XACT , a suite of setting focused secure area confirmation components that empower scenes and GSN suppliers to guarantee the areas asserted by clients. We demonstrate that XACT is right, secure and simple to utilize. We approve the requirement for secure area check systemsby gathering and breaking down information from the most well known GSNs today: 780,000 foursquare clients and 143,000 Gowalla clients. Through a proof-of-idea execution on a RevisionC4 BeagleBoard implanted framework we show that XACT is anything but difficult to send and financially suitable. We systematically and experimentally demonstrate that XACT distinguishes area bamboozling assaults.In this paper we study area misrepresentation issues in

ISSN 2347–3657
Volume 1,Issue 1,Jan 2013

geosocial systems. We propose Wi-Fi, QR-code and approach field based area confirmations arrangements. Through a proof- of-idea BeagleBoard execution, we show thatthey are simple and modest to send just as easy to understand. We demonstrate that our barriers power the nearness of in any event one assailant at an objective setting, while wormhole assaults are recognized through the observable extradeferrals over genuine client practices. In future work we will address the time synchronization necessities between the supplier and setting conveyed gadgets.

On the Validity of Geosocial Mobility Traces [3]

Versatile systems administration specialists have since a long time ago scanned for largescale, fine-grained hints of human development, whichhave stayed subtle for both security and strategic reasons. As of late, specialists have started to concentrate on geosocial versatility follows, for example foursquare checkin follows, on account of their accessibility and scale. However, would we say we are surrendering accuracy in our energy for information? In this paper, we make beginning strides towards evaluating the estimation of geosocial datasets utilizing an enormous ground truth dataset assembled from aclient study. By looking at GPS follows against Foursquare checkins, we locate that a huge part of visited areas is absent from checkins, andmost checkin occasions are either manufactured or pointless occasions. We portray superfluous checkins, depict potential procedures for theirdiscovery, and show that both incidental and missing checkins bring huge mistakes intoapplications driven by these follows.

In this paper, we utilized ground-truth GPS follows from a client concentrate to approve the capacity of geosocial follows to catch human portability. We locate that 75% of occasions infoursquare checkin follows are unessential checkins produced by clients to accomplish in-framework rewards, and checkin occasions just catch 10% of genuine visited areas from genuine physical portability follows. We additionally show that these disparities mean noteworthy deviations in consequences of uses depending onthese follows.

FRAMEWORK

In this paper, we propose a practical solution that limits the ability of Sybil devices to amplify the potential damage incurred by any single attacker. We introduce collocation edges, authenticated records that attest to the one-time physical proximity of a pair of mobile devices. The creation of collocation edges can be triggered opportunistically by the mapping service, e.g., Waze. Over time, collocation edgescombine to form large proximity graphs, network structures that attest to physical interactions between devices. Since ghost riders cannot physically interact with real devices, theycannot form direct edges with real devices, only indirectly through a small number of real devices operated by the attacker. Thus, the edgesbetween an attacker and

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 1,Issue 1,Jan 2013

the rest of the network are limited by the number of real physical devices she has, regardless of how many ghost riders are under her control. This reduces theproblem of detecting ghost riders to a community detection problem on the proximity graph (The graph is seeded by a small number oftrusted infrastructure locations).

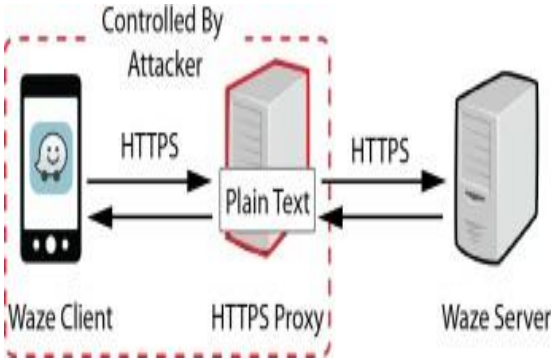
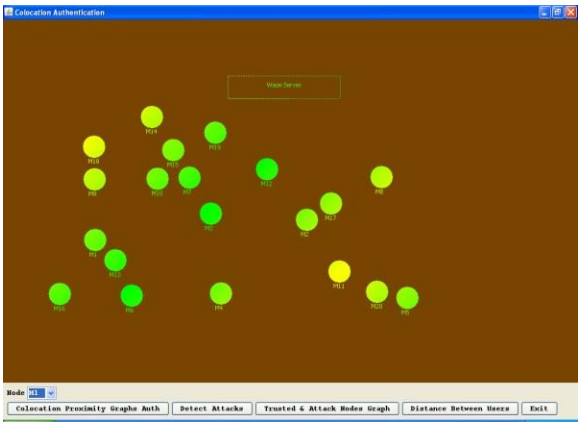


FIGURE: 2. System Architecture



we describe a powerful new attack on user privacy, where virtual vehicles can track Waze users continuously without risking detection themselves. By exploiting a key social functionality in Waze, attackers can remotely follow (or stalk) any individual user in real time. This is possible with single device emulation, but greatly amplified with the help of large groups of ghost riders, possibly tracking large user populations simultaneously and putting user(location) privacy at great risk. We start by examining the feasibility (and key enablers) of this attack. We then present a simple but highly effective tracking algorithm that follows individual users in real time, which we have validated using real life experiments (with ourselves as the targets).

EXPERIMENTAL RESULTS

We use a very small number of trusted nodes only to bootstrap trust in the graph. We assume asmall number of infrastructure access points are known to Waze servers, e.g., hotels and public

WiFi networks associated with physical locations stored in IP-location databases (used for geolocation by Apple and Google). Any Waze device that communicates with the Waze server under their IPs (and reports a GPS location consistent with the IP) automatically creates a new collocation edge to the trusted node.We focus on evaluating the feasibility and cost for attackers to maintain a large number of Sybils after the Sybil detection is in place.

FIGURE:3. Simulation Screen

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 1,Issue 1,Jan 2013

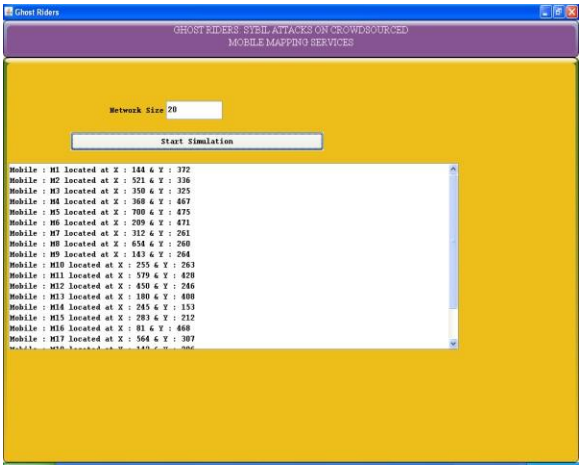


FIGURE:4. Location of Mobile Screen

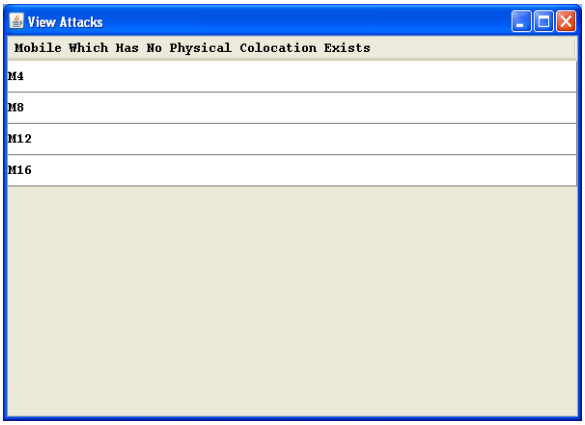


FIGURE:5. View Attack Screen

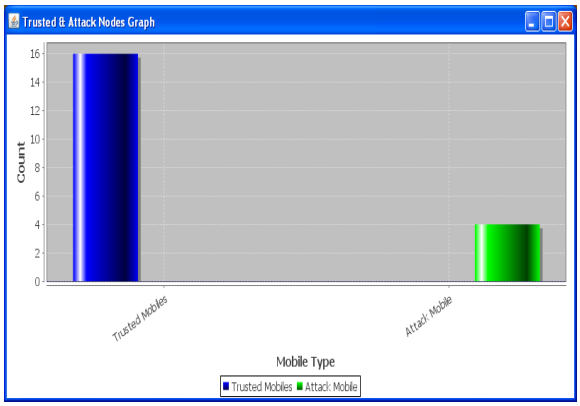


FIGURE:6. Trusted & Attack Nodes GraphScreen

CONCLUSION

Our work shows that today‟s mapping services are highly vulnerable to software agents controlled by malicious users, and both the stability of these services and the privacy of millions of users are at stake. While our study and experiments focus on the Waze system, we believe the large majority of our results can be generalized to crowdsourced apps as a group. We propose and validate a suite of techniques that help services build proximity graphs and usethem to effectively detect Sybil devices. Throughout this work, we have taken active steps to isolate our experiments and prevent any negative consequence on real Waze users.We also proactively informed Waze team of theses attacks, and worked with them to mitigate the threat.

FUTURE SCOPE

We further discuss the need for social network security and the effects of Sybil attacks in social networks, classification of Sybil attacks to understand about the sources of the attack, examples of systems vulnerable to Sybil attacks and a summary of the current trends in Sybil defenses.

REFERENCES

[1] N. Stefanovitch, A. Alshamsi, M. Cebrian, and I. Rahwan, “Error and attack tolerance of collective problem solving: The DARPA shredder challenge,” EPJ Data Sci., vol. 3, no. 1, pp. 1–27, 2014.

ISSN 2347–3657
Volume 1,Issue 1,Jan 2013

[2] B. Carbunar and R. Potharaju, "You unlocked the Mt. Everest badge on Foursquare! Countering location fraud in geosocial networks," in Proc. MASS, 2012, pp. 182–190.

[3] Z. Zhang et al., "On the validity of geosocial mobility traces," in Proc. HotNets, 2013, p. 11.

[4] J. R. Douceur, "The Sybil attack," in Proc. IPTPS, 2002, pp. 251–260.S. Cheng, Uber‟s Terrifying „Ghost Drivers‟ are Freaking out Passengers in China. New York, NY, USA: Quartz, Sep. 2016.

[5] Y. Wang, "Ghost drivers are just one of Uber China‟s problems following DIDI takeover," Forbes, Sep. 2016.

[6] M. Wehner, "How to cheat at Pokémon Go and catch any Pokemon you want without leaving your couch," DailyDot, Jul. 2016.

[7] How to Avoid Getting Banned in Pokemon Go While Location Spoofing, Cydiageeks, San Francisco, CA, USA, Jul. 2016.

[8] V. Goel, "Maps that live and breathe with data," The New York Times, New York, NY, USA, Tech. Rep., Jun. 2013. [Online]. Available: https://www.nytimes.com/2013/06/11/technolo g y/mobile-companiescrave-maps-that-live-and- breathe.html

[9] Google Maps and Waze, Outsmarting Traffic Together, Google Official Blog, Google, Mountain View, CA, USA, Jun. 2013.