

**Ghost Riders: Sybil Attacks on Crowdsourced Mobile Mapping Services**

**Abstract:**

Real-time crowdsourced maps, such as Waze provide timely updates on traffic, congestion, accidents, and points of interest. In this paper, we demonstrate how lack of strong location authentication allows creation of software-based *Sybil devices* that expose crowdsourced 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 precise movements 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 a pair of devices. Over time, co-location edges combine 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 their system.

**Existing System:**

First is simple *event forgery*, where devices can generate fake events to the Waze server, including congestion, acci-dents or police activity that might affect user routes. Second, we describe techniques to reverse engineer mobile app APIs, thus allowing attackers to create lightweight scripts that effectively emulate a large number of virtual vehicles that collude under the control of a single attacker. We call Sybil devices in Waze “ghost riders.” These Sybils can effectively magnify the efficacy of any attack, and overwhelm contributions from any legitimate users. Finally, we discover a significant privacy attack where ghost riders can silently and invisibly “follow” and precisely track

individual Waze users throughout their day, precisely mapping out their movement to work, stores, hotels, gas station, and home. We experimentally confirmed the accuracy of this attack against our own vehicles, quantifying the accuracy of the attack against GPS coordinates. Magnified by an army of ghost riders, an attacker can potentially track the constant whereabouts of millions of users, all without any risk of detection.

**Proposed System:**

We explore limits and impacts of single device attacks on Waze, *e.g.*, artificial congestion and events.

We describe techniques to create light-weight ghost riders, virtual vehicles emulated by client-side scripts, through reverse engineering of the Waze app’s communication protocol with the server.

We identify a new privacy attack that allows ghost riders to virtually follow and track individualWaze users in realtime, and describe techniques to produce precise, robust location updates.

We propose and evaluate defenses against ghost riders, using *proximity graphs* constructed with edges representing authenticated collocation events between pairs of devices. Since collocation can only occur between pairs of physical devices, proximity graphs limit the number of edges between real devices and ghost riders, thus isolating groups of ghost riders and making them detectable using community detection algorithms.