New research exposes security risk for e-scooters and riders

January 27 2020, by Milady Nazir

Computer science experts at UTSA have published the first review of the security and privacy risks posed by e-scooters and their related software services and applications. Credit:MusicFox Fx on Unsplash

Micromobility vehicles, such as e-scooters, zip in and out of traffic. In San Antonio alone, over 12,000 scooters are on the road. For this reason, micromobility is seen as an alleviating trend to help tackle traffic congestion.

However, new research out of UTSA finds e-scooters have risks beyond the perils of potential collisions. Computer science experts at UTSA have published the first review of the security and privacy risks posed by e-scooters and their related software services and applications.

"We were already investigating the risks posed by these micromobility vehicles to pedestrians' safety. During that study, we also realized that besides significant safety concerns, this new transportation paradigm brings forth new cybersecurity and privacy risks as well," noted Murtuza Jadliwala, an assistant professor in the Department of Computer Science who led this study.

According to the review, which will soon appear in the proceedings of the 2nd ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec 2020), hackers can cause a series of attacks, including eavesdropping on users and even spoof GPS systems to direct riders to unintended locations. Vendors of e-scooters can suffer denial-of-service attacks and data leaks.

"We've identified and outlined a variety of weak points or attack surfaces in the current ride-sharing, or micromobility, ecosystem that could potentially be exploited by malicious adversaries right from inferring the riders' private data to causing economic losses to service providers and remotely controlling the vehicles' behavior and operation," said Jadliwala.

Some e-scooter models communicate with the rider's smartphone over a Bluetooth Low Energy channel. Someone with malicious intent could

eavesdrop on these wireless channels and listen to data exchanges between the scooter and riders' smartphone app by means of easily and cheaply accessible hardware and software tools such as Ubertooth and WireShark.

Those who sign up to use e-scooters also offer up a great deal of personal and sensitive data beyond just billing information. According to the study, providers automatically collect other analytics, such as location and individual vehicle information. This data can be pieced together to generate an individual profile that can even include a rider's preferred route, personal interests, and home and work locations.

"Cities are experiencing explosive population growth. Micromobility promises to transport people in a more sustainable, faster and economical fashion," added Jadliwala. "To ensure that this industry stays viable, companies should think not only about rider and pedestrian safety but also how to protect consumers and themselves from significant cybersecurity and privacy threats enabled by this new technology."

This study was produced in UTSA's Security, Privacy, Trust and Ethics in Computing Lab, which was also behind the recent publication on how smart bulbs can be hacked. The lab is dedicated to examining privacy and security issues in ubiquitous devices.

The micromobility e-scooter analysis was conducted by Jadliwala alongside graduate students Nisha Vinayaga-Sureshkanth, Raveen Wijewickrama and postdoctoral fellow Anindya Maiti.

Provided by University of Texas at San Antonio

Citation: New research exposes security risk for e-scooters and riders (2020, January 27) retrieved 26 April 2024 from

https://techxplore.com/news/2020-01-exposes-e-scooters-riders.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.