TechXplore

An encryption system that hides your travel data from Uber

June 30 2017, by Anne-Muriel Brouet

Our protocol was designed to make it impossible to track the passengers' and the drivers' movements. Credit: iStock

Researchers from EPFL and UNIL have developed an encryption protocol that can put drivers in touch with passengers while keeping their personal data secret.

The apps created by Uber and its competitors put peers in touch with each other when one of them is looking for a ride. But the online platforms these companies have developed also collect users' personal data – from passengers and drivers alike. Multiplied by millions of users each day, that comes out to be a goldmine of information, especially in the era of Big Data. Researchers from EPFL and the Faculty of Business and Economics at UNIL looked at how the same level of service could be achieved without disclosing users' personal data. Their software, called ORide (O for oblivious), can be used to set up a ride where only the driver and passenger know the starting point, route and destination.

"Ride-hailing apps like Uber have created a lot of buzz and controversy. But the issue of data protection has been less discussed," says Jean-Pierre Hubaux, a professor at EPFL's School of Computer and Communication Sciences. Some data security concerns have already been reported in the press, such as a flaw that revealed data about hundreds of drivers and – even worse – a threat by a Uber executive to dig up dirt on unfriendly journalists. The members of the project team, who are all experts on data protection, could not pass up the challenge of seeing whether it would be technically possible to keep personal data confidential in ride-hailing platforms. They will present the results of their research at two conferences in North America this summer.

Still convenient and fast

ORide uses a cryptographic system similar to homomorphic encryption. It can carry out operations on encrypted data and get the same result as if the data was not encrypted. For example, it can add an encrypted 2 + 2 to get an encrypted 4. So when someone uses ORide to search for a driver, the system will receive encrypted location data about the passenger and the drivers who are available. It will then identify the closest drivers, and – still using encrypted data – let the passenger select a driver. Once the two app users are matched up, ORide will display the location of each one on the other's smartphone.

The route that the driver takes is also coded in the users' smartphones. The only data seen by the ride-hailing company is the distance travelled and the cost of the ride, since this information is what the company will use to take its cut of the fee and what passengers will use as a record of their travel expense. What's more, ORide doesn't affect the app's convenience – passengers can still pay with their credit cards and evaluate their drivers. "Our protocol was designed not to provide complete anonymity, but to make it very hard to track the passengers' and the drivers' movements," says Hubaux. The researchers also realized that their system needs to allow passengers to hunt down a lost item or provide evidence in case of a dispute with a driver. In the event of such a dispute, the data can be re-identified, but only with the agreement of the party making the complaint.

Confidentiality: a selling point

The project team tested their system using public data on New York taxi drivers. They wanted to make sure in particular that the encryption protocol doesn't slow down the process of searching for a driver. New York – whose population is roughly the same size as Switzerland's – has just as many Uber and Lyft drivers as taxi drivers. "The encryption with a high-security key adds just a few milliseconds to the search time and doesn't require a faster internet connection," says Hubaux. "On the downside, ORide won't necessarily find the closest driver, which means passengers could have to wait one or two extra minutes."

Uber and its rivals are now free to decide whether they're interested – especially since the researchers purposely chose not to patent their technology. "This is a highly competitive market, and confidentiality could be a selling point or a way to avoid a legal battle if a firm has to share the data it has access to with the secret services," adds Hubaux.

Provided by Ecole Polytechnique Federale de Lausanne

Citation: An encryption system that hides your travel data from Uber (2017, June 30) retrieved 23 September 2023 from https://techxplore.com/news/2017-06-encryption-uber.html