Latest Advances in ML-enabled Location Privacy Attacks and Protection Mechanisms

Sonia Ben Mokhtar

CNRS Senior Researcher
The LIRIS Laboratory (UMR 5205), Lyon, France
https://sites.google.com/site/soniabm/

Biography

Sonia Ben Mokhtar is a CNRS research director at the LIRIS laboratory (UMR 5205) and the head of the distributed systems and information retrieval group (DRIM). She received her PhD in 2007 from Université Pierre et Marie Curie before spending two years at University College London (UK). Her research focuses on the design of resilient and privacy-preserving distributed systems. Sonia has co-authored 70+ papers in peer-reviewed conferences and journals and has served on the editorial board of IEEE Transactions on Dependable and Secure Computing and co-chaired major conferences in the field of distributed systems (e.g., ACM Middleware, IEEE DSN). Sonia has served as chair of ACM SIGOPS France and is currently the vice-chair of GDR RSD a national academic network of researchers in distributed systems and networks.

Summary

The widespread adoption of continuously connected smartphones and tablets drove the proliferation of mobile applications, among which many use location to provide a geolocated service. The usefulness of these services is no more to be demonstrated; getting directions to work in the morning, leaving a check-in at a restaurant at noon and checking next day's weather in the evening is possible from any mobile device embedding a GPS chip. In these applications, locations are sent to a server often hosted on untrusted cloud platforms, which uses them to provide personalized answers. However, nothing prevents these platforms from gathering, analyzing and possibly sharing the collected information. This opens the door for many threats, as location information allows to infer sensitive information about users, among which one's home, workplace or even religious/political preferences. For this reason, many schemes have been proposed these last years to enhance location privacy while still allowing people to enjoy geolocated services. During this presentation, I will present the latest advances in location privacy by focusing on : (1) advances brought by ML techniques for better understanding the threats to users' location privacy and (2) advances brought by ML for the design of novel protection mechanisms.