UC San Diego
Technical Reports

Title

Policy-Aware Sender Anonymity in Location Based Services

Permalink

https://escholarship.org/uc/item/2497x3bc

Authors

Deutsch, Alin
Hull, Richard
Vyas, Avinash
et al.

Publication Date

2009-03-17

Peer reviewed

Policy-Aware Sender Anonymity in Location Based Services

Alin Deutsch
deutsch@cs.ucsd.edu

Richard Hull
hull@us.ibm.com

Avinash Vyas
vyasa@alcatel-lucent.com

Kevin Keliang Zhao
kezhao@cs.ucsd.edu

March 17, 2009

Abstract

Sender anonymity in location-based services (LBS) attempts to hide the identity of a mobile device user who sends requests to the LBS provider for services in her proximity (e.g. "find the nearest gas station", "theater", "restaurant", etc.). The goal is to keep the requester's interests private even from attackers who (via hacking or subpoenas) gain access to the request and to the locations of the mobile user and other nearby users at the time of the request. In an LBS context, the best-studied privacy guarantee is known as *sender k-anonymity*, which is intended to insure that the request log and precise location information are insufficient to distinguish among the actual requester and k-1 other possible requester. We show that state-of-the art solutions for sender k-anonymity defend only against naive attackers who have no knowledge of the anonymization policy that is in use. We strengthen the privacy guarantee to defend against more realistic "policy-aware" attackers. Our implementation and experiments show that the novel privacy guarantee has potential for practical impact, being efficiently enforceable, with limited reduction in utility when compared to policy-unaware guarantees.

A copy of this technical report can be obtained by sending an email request to **deutsch@cs.ucsd.edu** or **vyasa@alcatel-lucent.com**.

1