Protecting Privacy Against Location-Based Personal Identification

C. Bettini, X.S. Wang, S. Jajodia

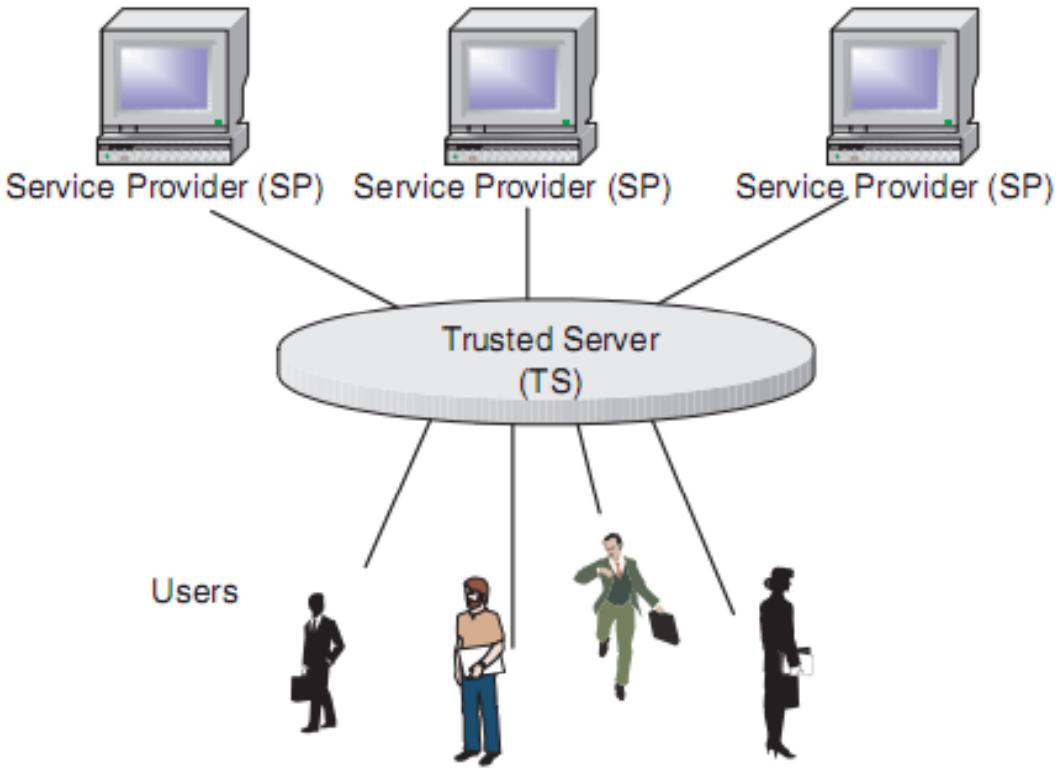
Secure Data Management (SDM 2005), pp. 185-199, 2005.

DOI: 10.1007/11552338_13.

David MacDonald

Summary

As mobile devices enable location specific details (such as the nearest hospital), we need methods to maintain the privacy of individuals: we do not want a service provider to identify us when we make a request!



A user contacts the service provider but the user does not want the service provider to know their identity.

An Adjustable System

- A service provider will find that *k* individuals appear ‘the same’ – an attacker cannot identify any individual within this group.
- Since *k* is arbitrary the user can customise the privacy level to suit their needs (or paranoia!).
- And this is based on potential senders – the trusted server don’t need to find *k* individuals that actually send a request.

What Does This Mean For a User?

- Mentions low/medium/high levels of security for users in practice – but fails to describe this any further in the paper.
- What are the applications?

What Does This Mean For a User?

- What does a low/medium/high level of security mean?
- Does this mean we vary the *k* value to include more or fewer individuals?
- Does this mean the location history identifier (such as our daily patterns)?

What Does This Mean For a User?

- Who decides on what each of the levels of security should be?
- The trusted server? The mobile device manager? The Consumer?
- And the further difficulty is that a low level of privacy in one culture might mean a high level of privacy in another.
- One size does not fit all!

Question:

- Do users really care about their privacy? How much are we willing to pay for our privacy?