Internet-Draft
draft-takahashi-spatial-privacy-scenario-00.txt
Expires: Jan 2002

Kenji Takahashi
NTT
Haitao Tang
Nokia

July 2001

Location-based Service Scenarios for Privacy Analysis
<draft-takahashi-spatial-privacy-scenario-00.txt>

Status of This Memo

Abstract

We propose a user scenario framework of location-based services to analyze security and privacy issues associated with the services. The framework is intended to cover the most of the location-based services available today and in near future. There are many kinds of existing and possible location-based services. Though, what is meant by location-based service varies widely. The framework gives people a common ground from where discussion on the security and privacy issues can start.

1. Introduction

There are many kinds of existing and future location-based services. However, the definition of location-based services is different among users and service providers. For example, what is a "push" service? Some people may say that the push service is a location based "handbill" delivery ? for example, when you come close to a pizza restaurant, you receive a mail message about the restaurant. Other people may say the push service is a guardian service that periodically pushes location information of kids to their guardians. The trust models are totally different in these two cases. In the former case, the anonymized location information of a person is obtained by the trusted party (e.g., an advertisement agency) if s/he is in a particular geographical area during an allowed time period. In the latter case, the location information of the specific persons is kept tracked by the trusted party

(e.g. parents).

We therefore propose a user scenario framework as a common ground to productively discuss the security and privacy in location-based services.

2. Definition

Throughout this document, we define and use the following terms

Owner
The owner is the person who rightfully owns the location information. The owner is the target of the location information if the target is a human, or is a human who owns the target if the target is a non-human object. For example, John is obviously the owner of his location information. John is also the owner of the location information of his dog.

Requester
A requester is a human or non-human entity that asks a responder for the location information of an owner. Requesters could be the owners, if, for example, the requesters themselves ask where they are.

Responder
A responder is a human or non-human entity that delivers a requester the location information. Responders could be the owners if, for example, the owners have GPS devices and the means that can send the location information obtained from the devices. Responders could also be proxies of the owners.

Proxy
A proxy is a computer entity that acts on behalf of one or more responders to deliver the location information and/or on behalf of one or more requesters to ask for the location information.

Location information
The information about where a human or non-human entity is geographically located. The location information can be represented in many ways, for example, a pair of longitude and latitude.

3. Security and privacy attacks

Regarding location-based services, we have identified the following four major types of security and privacy attacks:

Snoop
Attackers snoop and reveal (and decrypts) the payloads of packets. They may also modify the location information. Interestingly, the location data alone, e.g., longitude and latitude, may not be necessarily encrypted because the data is useless in many cases if the data is not associated to an owner. For example, "Kenji is at (35.55, 136.28)" is

very private information, while the disclosure of the data content, "(35.55, 136.28)" alone is not harmful to Kenji. This is fairly different from music data content distribution where the data itself is important and should be encrypted. Anonymous use of the location data could be easier to implement without encryption.

Replay attack
There are two types of replay attacks: those by "owner" and by "receiver". In former case, the attackers, who disguise the true owners, receive and send the false location information to requesters. In latter case, attackers, who disguise the true requester, send requests for the location information to the owners.

Traffic analysis
Traffic analysis reveals the source and destination of packets delivered by tapping network links and/or actively attacking routers. In particular, the source and destination of packets can be associated with location in mobile communication.

4. Basic episodes

Location-based services could be very complicated. However, we believe that it is possible to extract a limited number of common basic episodes, or building blocks of user scenarios, from the complicated services. Episodes are end-to-end transactions. Also for simplicity, we do not consider episodes in which proxies participate usually. Though, one exception is when a person is asking about oneself, s/he interacts with one's proxy that has the person's location information and can answer the person's question. By considering what users experience through location-based services, we can identify four perspectives:

Focus: Target / Place
Services focused on "place" handle basically request for reports on "whether someone/something is in a particular place", whereas those focused on "target" handle requests for reports "where a particular person/thing is". The different focuses make a significant difference in the interaction model. In target-focused services, responses include location data, whereas in place focused-services, requests include location data (and responses, for example, are just "yes", "no", or "how many").

Target: User's own position / Third party's position

Trigger: Requester-pull / Owner-push

Anonymity: Anonymous / Non-anonymous

As shown in Figure 1, there are 10 basic episodes from the combination of these four perspectives.

(Ep1) Owner asks Proxy where he is.
(Ep2) Owner tells anonymously Requester where he is.
(Ep3) Owner tells Requester where he is.
(Ep4) Requester asks Responder where an anonymous target is.
(Ep5) Requester asks Responder where Target Y is.
(Ep6) Owner asks Proxy whether he is in Place X.
(Ep7) Owner anonymously tells Requester whether he is in Place X.
(Ep8) Owner tells Requester whether he is in Place X.
(Ep9) Requester asks Responder whether an anonymous target is in Place X.
(Ep10) Requester asks Responder whether Target Y is in Place X.

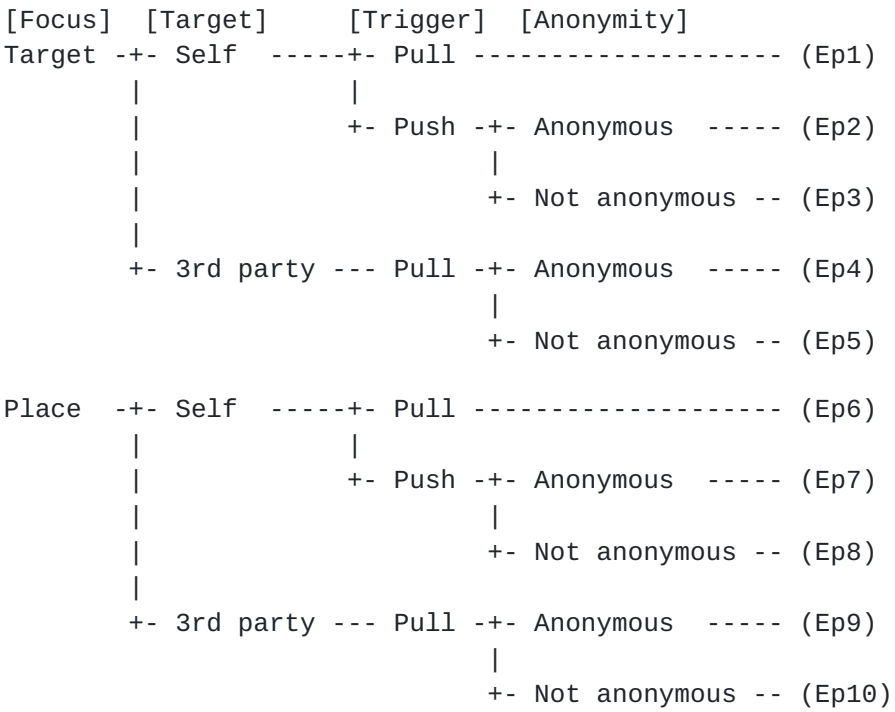

Figure 1. Basic episodes in location-based service

5. Composite scenarios

There can be an unlimited number of location services that comprise of the basic episodes. Here we illustrate how three scenarios consist of the episodes. Certainly, these scenarios could be specified in more detail and may contain more intermediaries. However, we describe here the simplest cases.

(1) Where is the nearest pizza restaurant?
A person looking for a nearest pizza restaurant can start this scenario by using a location service for Ep1 ("Owner asks Proxy where he is."), or getting the position locally, e.g., via using GPS. Then the person uses a service for Ep2 ("Owner anonymously tells Requester where he is") to let the service provider know where he is. At last the service provider gives the person the information about the nearest pizza restaurant. The last interaction looks like a simple information delivery, while there is still a potential risk of the disclosure of location information. An attacker can know that the person may go to the restaurant if the attacker can snoop the information that the person got and identify whom the person is.

(2) Location-based advertisement distribution.
Suppose that a person subscribes to an advertisement provider and allow it to use the information about his location in a limited manner. A person may start with Ep2, Ep3, Ep7, or Ep8, depending on the trust relationship between the person and the provider, to tell the provider where s/he is or whether s/he is in a specific place. Then the provider distributes the advertisement information to the person based on where s/he is. There is a potential risk where attackers know where s/he is by associating the advertisement with its receivers.

(3) Web-based "whereabouts" service
A service provider provides users a service to tell them where a person is. A user starts with Ep5 ("Requester asks Responder where Target Y is"). Then the provider, as a proxy of the person (the location owner) , executes Ep3 ("Owner tells Requester where he is"). In this scenario, the provider should get the permission from the location owner to use his location report.

6. Conclusion

The location privacy and security problems are usually specific to certain application(s) of the location information. It would be very

difficult to design an effective privacy and security scheme for something, unless the associated use cases are analysed. We therefore propose to solve these problems inside the applications rather than by considering the location something alone.

Author's Addresses

Haitao Tang
P.O. Box 407, FIN-00045 Nokia

Finland
Email: haitao.tang@nokia.com

Kenji Takahashi
NTT
3-9-11 Midoricho
Musashino, Tokyo 180-8585 Japan
Email: takahashi.kenji@lab.ntt.co.jp