Location Spoofing

Richard Glassey
Department of Computer and Information Sciences
University of Strathclyde
Glasgow, Scotland
rjg@cis.strath.ac.uk

1. AUTHOR BIOGRAPHY

Current research involves investigating the possibilities of providing middleware for scalable location-aware computing using spatially distributed object graphs to represent entities, relations and locations. Richard Glassey is a PhD student attending the University of Strathclyde, Glasgow, where he previously achieved a B.Sc. (Hons) in Computer Science.

2. OPINION

At present, it is possible with existing infrastructure to determine the location of people, with varying degrees of precision. Authorities, should they wish too, can monitor mobile phone movements, CCTV footage, ATM transactions and various other means of locating someone. Effectively the Orwellian nightmare so vividly described by the media is all but in place. However people do not yet have reasonable access to their personal location information for their benefit. Public resistance to new developments in location awareness, such as protests against tagging of products in supermarkets, reduces the chance that people will ever see the benefits. Despite this caution it is possible to look into the near future, when we begin to fully realise the implications of an information saturated age, where location plays an increasingly important role in making sense of it all.

One aspect of interest is how people, given the responsibility of access control, will manage their location information. Rather than lament about the possible misuse of location for malevolent reasons, this short note discusses how location spoofing, that is, to blur or lie regarding one's location, can be used for benevolent reasons.

To Blur

Fundamental to encouraging the uptake of location-aware applications is relinquishing the responsibility of access control to the end user. Further, the degree of access must allow for a spectrum of control from no access to full access. Whilst there will be more than one aspect to access control, the most prominent is controlling the resolution of location information, effectively blurring what is presented.

Given a choice of location resolution, city, street, less than 20 metres, less than 5 metres, not everyone will choose the same level. This level will certainly change depending upon the context we may be in or application we may be using. If we consider a location-aware city guide, the ability to tune the level of location information in terms of resolution becomes a very effective way of filtering relevant information. At the city resolution we have access to more abstract information such as an overview of public transport, areas of importance and city-wide services. By choosing this level we filter information that we are not interested in, such as restaurants and shops, within our immediate surroundings. However, the converse is also useful when we are attempting to locate a nearby service based on our location. At a street resolution we only receive information concerning our immediate vicinity, thus reducing the effort to find what we require.

Not only will the ability to blur the resolution of location information reassure people that they are in control, it will also serve a very useful purpose when it comes to filtering large quantities of spatial information we will have to face.

To Lie

At first glance the proposition of lying about one's location, to serve a legal purpose, seems ridiculous. What decent law abiding citizen would ever want to lie about where they are, assuming they are willing to take part in an onymous location system? Surely they must be up to no good. Take the example of the employee who removes their RFID badge, pins it to their office chair and proceeds to spend the rest of the working day relaxing in the park. Short of the rather unpopular implanted ID chips it is very easy to fool the system regarding your location in this example. So just how could the ability to lie about your location prove useful?

There are times when we want other people to think we are somewhere we are not. One good example would be leaving our house unoccupied for any period of time. Attempts to spoof location currently only go as far as timed light switches or radios left playing, strategies that are easily defeated by burglars. Consider a smart home environment, designed to assist with daily tasks, that also records sensed movement and activity. This data is used to construct a model of behaviour for the home. If the occupants leave, the smart home can be instructed to use the model to derive reasonable sequences of behaviour to execute in their absence, giving the impression of somebody at home. Whilst this example is quite simple, other applications may also have to lie about the location of valuable assets for protection against theft.

The ability to blur and lie about our location does deserve consideration and should not be treated as entirely malevolent. It will be up to designers to allow the user to have full responsibility and freedom over the access control of their location information, rather than force adherence to uncomfortable regimes of dictated access control.