Proving Co-Location by Context Comparison

Review

The author has given a nice explanation on the requirement of proving co-location. Sometimes we have to do some private and confidential operations to a device which requires manual intervention to preserve user’s privacy by ensuring that the user himself is involved in the task. Payment in a shop or unlocking a laptop are considered to be such applications. Therefore for the manual operation the user has to be in proximity with the device. But sometimes it is not possible or the user may be reluctant to do the manual tasks repetitively. It is not possible to unlock a car manually when the car owner is carrying pizzas in both hands or a laptop owner may not want to provide a password to unlock his laptop everytime he moves close in. So the goal is to minimise and if possible nullify user activity and still provide the same level of privacy. To do this at least we have to ensure that the device and the user are close and the activity happening is known to the user. This way we can ensure that somebody else cannot just unlock a car when the owner is not nearby. That is why a scheme has to be proposed that proves co-location of the user and the device. The author has explained all these requirements briefly and in an organized manner.

The above discussed scenario has been named as Zero Interaction Authentication (ZIA) and the author explained the scheme well with a diagram. But it could be described a bit more according to the original paper. There are a few points which could have been taken care of-

- Whether the session key is used only once or multiple times or what basically the encryption scheme is doing when the user goes out of range etc.
- The ZIA scheme is described in the context of locking and unlocking of a device. It would be nice if the author describes it in the context of payments using NFC devices.

The author has discussed the problems of Distance Bounding Protocols to prove co-location. It is true that in those protocols there are certain parameters which can be forged. As a solution, the author is proposing context tag based solutions. He has shown that Ambient Audio is one of the strongest form of context information as audio signals in the surroundings are not harmonic and almost impossible to match if two communicating parties are not in vicinity. It is hard to forge audio signals.

Ambient Light is a bit problematic to use because in the same location, light intensity can change with the orientation of the device. So light cannot be relied upon.

The author has stated a weakness about GPS that a user has to wait for a few seconds or move fast to refresh the GPS location. GPS responds faster than mobile objects than static ones. Here a question arises,

- What is the purpose of refreshing GPS location when the user is static or his location has not been changed. This can be elaborated a bit.
- The author has said about having device acceleration as a context tag and to prove co-location, the devices has to be shaken in one hand as they both will give similar data.
• It would be nice if one practical application can be given when two devices are shaken in one hand for generating context tags.

The author has taken a good step to enhance the Blueproximity software by pairing the communicating devices together. A secure communication channel would obviously stop the Ghost & Leech approach to play into the system. But one thing the author may consider,

• A situation can be such that an adversary comes closer to a car when the owner is far away. Within a threshold distance their co-location can be established by context data. Now if the adversary manages to have fake bluetooth id same as the the owner’s device and the authentication scheme does not pair both of them together then the adversary is appearing as the owner. The author can think about how to tackle this scenario.

The author may also think some of these points to include:

• A brief idea of how RFID and NFC based schemes differ. In Introduction the author has written that,

  “RFID consists of readers and tags and works in a challenge-response manner to provide contactless authentication. NFC is a promising standard based on RFID enabling short-range communication (<=10cm) and contactless transactions between two handsets.”

From this description it is unclear that how these two schemes differ from each other while both provides contactless communication between between two parties. The author can include their separate application areas in two-three sentences.

• The enhancement on Blueproximity can be written step by step. If so then it would be nice to read.

• The author may consider a situation like a person uses his NFC enabled phone to unlock his car. It is a problem if somebody has stolen the phone and uses it to open the car. Same can happen in NFC phone based payment scheme. So while thinking of co-locating devices in some cases it may be essential to co-locate the user and a device. These scenarios may be taken care of.

The paper is in a good shape. It is well written and would become closer to completion if the above discussed points are considered. Some sentence constructions seem to be inappropriate and they are pointed out in the paper.