A proposal for experimental validation of a framework for use privacy for RFID

Monday 31st August, 2009

1 Description of the scenario

RFID and NFC are the *de-facto* technology for storing small amount of data on devices that can be read without physical contact. It is expected that everyday objects will be tagged with small components which are used to carry information to identify the object. For example, the government industry plans to use RFID tags for the management of post-sale services. Obviously, it is expected that encryption is used for storing information on the tag so that only legitimate users can access the stored data. Encryption though does not solve all problems and we are interested in privacy issues associated with RFID tags. Specifically, RFID tags can be read by anyone and the string stored on a tag, even though it is a ciphertext, can be used to trace the tag and, in the case the tag is attached to a personal object, to trace the owner of the tag.

We thus envision a system in which the environment helps in alleviating this problem: as tags move in the environment they are read by special devices called the *randomizers* which provide the following service: every time a randomizer reads a tag carrying a ciphertext, the ciphertext is re-randomized; that is, a new ciphertext carrying the same cleartext is computed. The randomization procedure gives the security guarantee that an adversary he cannot decide whether two tags he has seen are two different tags or it is just the same tag that has been re-randomized. See [1] for technical details.

2 The Experiments

The security guaranteed by the proofs does not cover the case in which the same RFID is read by one or two adversaries between two consecutive re-randomization. Indeed in this case the two adversaries can certainly trace the RFID tag.

The aim of the experiment is to understand how often this happen under reasonable mobility models and as function of the ratio of adversaries and randomizers and thus formulate suggestions on the number of randomizers to use as a function of the expected number of adversaries present in the network.

2.1 Setup

In our experiments we will consider a finite 2D plane and we defined

1. how tags, randomizers and adversaries move;
2. how we measure the success of the adversaries.

We fix the position of the randomizers. The position will be chosen depending on the mobility model applied to the tags so to maximize the probability of interaction between tags and randomizers. Also the adversaries will receive fixed positions. They will not know where randomizers are located nor will be able to follow users (in which case they could trace a user even if RFID tag were not present).

2.1.1 Mobility Model for Tags

Tags are the only moving parties. We will use different mobility models to gain an understanding of the level of privacy provided by the different scenario. Such synthetic models attempt to realistically represent the behaviours of mobile nodes (MNs) without the use of observations coming from real life systems.

For our experiments we upper bound the speed of the users so that a tag stays within the operational range of a randomizer for enough time to be re-randomized.

We have chosen to analyze the following models (see [2] for a survey).

1. *Random Walk Mobility Model*: A simple mobility model based on random directions and speeds; it is a widely used model to represent purely random movements of the entities of a system in various disciplines from physics to meteorology. With the addition of pauses between changes in direction or speed we will talk of Random Waypoint Mobility Model. Even if this model is not realistic to model the behaviour of a moving user, we use this and the following two models as a benchmark.

2. *Random Direction Mobility Model*: A model that forces MNs to travel to the edge of the simulation area before changing direction and speed. This model has been created to promote a semi-constant number of neighbors throughout the simulation.

3. *A Boundless Simulation Area Mobility Model*: In this model it exists a relationship between the previous and the current direction of travel and velocity of an MN. Also when an MN reaches one side of the simulation area, it continue traveling and reappear on the opposite side of the simulation area. This technique creates a torus-shaped simulation area allowing MNs to travel unobstructed.

4. *Nomadic Community Mobility Model*: This model represents groups of MNs that collectively move from one point to another. Consider, for example, a class of students touring an art museum. In this model each MN uses an entity mobility model to roam around a given reference point. When the reference point changes, all MNs in the group travel to the new area defined by the reference point.

5. *Pursue Mobility Model*: The model attempts to represent MNs tracking a particular target. For example, this model could represent police officers attempting to catch an escaped criminal.

2.1.2 Measuring Adversary Success

In our experiment we will look at two different measures on how to quantify the breach of security.

1. Trace Measure: This is a 0/1 measure. The adversary wins if it manages to trace the tag at least one time. Meaning that the tag is traced twice by the adversary between two consecutive randomization.

2. Path Measure: This is a more accurate measure as we look at the percentage of the path played by a tag that the adversary manages to trace. The adversary wins if this percentage is more than a fixed threshold.

References

[1] Carlo Blundo and Angelo De Caro and Giuseppe Persiano, 2009, Untraceable Tags based on Mild Assumptions, Accepted Paper in the 2nd SETOP International Workshop on Autonomous and Spontaneous Security (**SETOP 2009**)

[2] Tracy Camp and Jeff Boleng and Vanessa Davies, 2002. *A Survey of Mobility Models for Ad Hoc Network Research*, Wireless Communications & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, Volume 2, pages 483–502.