Pervasive Integrity Checking with Coupled Objects

Paul Couderc, Michel Banâtre, and Fabien Allard

INRIA Rennes, Campus Universitaire de Beaulieu, 35042 Rennes Cecex France
{paul.couderc,banatre,fallard}@inria.fr
http://www.inria.fr/recherche/equipes/aces.fr.html

Abstract. Integrity checking is important in many activities such as. While the computing and telecommunication worlds commonly use digital integrity checking, many activities from the real world do not beneficiate from automatic mechanisms for ensuring integrity. We propose the concept of coupled objects where groups of physical objects are tagged with RFID chips enabling pervasive and autonomous integrity checking.

Keywords: Pervasive computing, security, integrity, RFID.

Checking for integrity of a set of objects is often needed in various activities, both in the real world and in the information society. The basic principle is to verify that a set of objects, parts, components, people remain same along some activity or process, or remains consistent against a given property (such as a part count).

In the real world, it is a common step in logistic: objects to be transported are usually checked by the sender (for their conformance to the recipient expectation), and at arrival by the recipient. When a school get a group of children to a museum, people responsible for the children will regularly check that no one is missing. Yet another common example is to check for our personal belongings when leaving a place, to avoid lost. While important, these verification are tedious, vulnerable to human errors, and often forgotten.

Because of these vulnerabilities, problems arise: E-commerce clients sometimes receive incomplete packages, valuable and important objects (notebook computers, passports etc.) get lost in airports, planes, trains, hotels, etc. with sometimes dramatic consequences.

While there are very few automatic solutions to improve the situation in the real world, integrity checking in the computing world is a basic and widely used mechanism: magnetic and optical storage devices, network communications are all using checksums and error checking code to detect information corruption, to name a few. The emergence of Ubiquitous computing and the rapid penetration of RFID devices enables similar integrity checking solutions to work for physical objects. However, RFID raises serious concerns regarding privacy. In a world where many personal objects are electronically identified, the activities of individuals could be traceable in a similar, though much more comprehensive, way to googling someone today on the Internet.

P. Sénac, M. Ott, and A. Seneviratne (Eds.): MobiQuitous 2010, LNICST 73, pp. 305–307, 2012.

An important cause of this issue is that RFID systems are usually based on the concept of global identification, associated directory services or tracking databases. However, technically RFID are just small memory devices that can be addressed by near-field communication, and although identification has been the main application target, these devices provide support for alternative mechanisms.

We developped such an alternative approach for pervasive integrity checking, called *coupled objects*, which does not rely on global identifification. We briefly present the principle on the simple application that addresses a common problem when travelling: it is unfortunately easy to forget something. For example, security procedures in airports require that your personal effects are checked separately from you by X-rays. Forgetting one of your items, or mistakenly exchanging a similar item with someone else occurs frequently. Solutions have been proposed for this problem, based on active tags attached to the items that are monitored by an owner tag. This is impractical for several reasons: active tags are expensive, they require batteries (and hence regular maintenance), radio emissions may be restricted by regulations (on planes for example), and temporarily separating an item from its owner would require the alarm to be disabled.

1 Autonomous Integrity Checking for a Set of Physical Objects

Coupled objects enables another solution using RFID tags attached to the items. It is possible to write in the memory of the tags the data required to check the integrity of the group of items. We compute a signature from the identifiers of all the items using a hashing function. An important aspect is that the identifiers associated with each item can be regenerated regularly (eg for each trip): they are only used for a locally computed integrity check, not for identification. The values could be written in the tags at, for example, the airport check-in, the train station, or even when leaving home. Then, at relevant points after the area in which people are vulnerable to item loss or exchange, we deploy checking gates (such as the exit of the security check in airports, or the exit gate of a plane or a train). These gates would ensure the integrity of groups of items crossing them, warning people in the case of a missing item or the presence of someone elses item.

This solution is a distributed system where only local properties are checked in order to ensure a global goal. In fact, it uses a principle similar to the transmission of a file in independent fragments over a packet network, where integrity is verified by checking sequence number coherency or checksums, except that here the data are carried by physical fragments. Such a solution is interesting because while providing a security service, it avoids the privacy concerns of many other RFID approaches. Specifically, tracking of individuals is not easy, since the tags content may change often for the same person and same set of objects. Further, the system is not based on identification, ensuring greater privacy.

Another interesting aspect is that checkpoints and association points are autonomous and only carry local processing. The system is therefore not dependent on a remote information system. This has important benefits in terms of extensibility, reliability and deployment costs.

2 Perspectives and Conclusion

We presented the principles of an approach enabling the design of pervasive integrity checking solution for many applications. The strong points of this solution are its independence of any remote information system support or network support, and user's privacy respect as it is anonymous and does not relies on global identifiers. It differs from many RFID systems where the concept of identification is central and related to database supported information systems. The approach also differs from some personal security systems based on PAN and active monitoring [3]. Coupled objects is in the line of the idea of RFID used to store in a distributed way group information over a set of physical artifacts, due to Bohn and Mattern [1], and *SmartBox* [2], where abstractions are proposed to determine common high level properties (such as completeness) of groups of physical artifacts using RFID infrastructures.

The approach we presented has benefits in various potential application where privacy and/or autonomy is a concern. Yet there are still challenges to overcome. In some applications where many tags have to be read at once on mobile objects, the performance of current hardware with respect to inventory read reliability and speed can be an issue. Another issue is security: the tags used in any RFID security solution should resist to tag cloning attacks or tag destruction attempt. This typically involve tag level cryptography logic, which require more execution cycles, more power, and more time to be read. Other perspectives are other application scenarios, we are in particular examining green-IT solutions for waste recycling using coupled objects to ensure the quality of the returned materials. Finally, we are also developing the mapping of complex data structures such as tree on a set of memory-limited tags considered as fragments.

References

1. Bohn, J., Mattern, F.: Super-distributed rfid tag infrastructures. In: Markopoulos, P., Eggen, B., Aarts, E., Crowley, J.L. (eds.) EUSAI 2004. LNCS, vol. 3295, pp. 1–12. Springer, Heidelberg (2004)
2. Floerkemeier, C., Lampe, M., Schoch, T.: The smart box concept for ubiquitous computing environments. In: Proceedings of sOc 2003 (Smart Objects Conference), Grenoble, pp. 118–121 (May 2003)
3. Kraemer, R.: The bluetooth briefcase: Intelligent luggage for increased security (2004), `http://www-rnks.informatik.tu-cottbus.de/content/unrestricted/teachings/2004/`