Information Security Group

Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium

---

Proposal 2010-03: Reducing RFID-Readers Load

[http://sites.uclouvain.be/security/internship.html]

Level: Bachelor or Master thesis.

Keywords: Security, Authentication, RFID, TMTO, Meet-in-the-Middle, Traceability attack, Complexity.

Requirements: The student candidate for this thesis should have a very good background in C and not be afraid by mathematical formulas. Ability to read scientific papers in English.

Theory: 

Practice: 

Abstract:

Often presented as the new technological revolution, radio frequency identification (RFID) allows us to identify objects or subjects with neither physical nor visual contact. We merely need to place a transponder on or in the object and query it remotely using a reader. Even though it has only been a few months since it has started to be covered by the media, this technology is fundamentally not new. It was used during the Second World

War by the Royal Air Force to distinguish allied aircrafts from enemy aircrafts. It has also been used for many years in applications as diverse as: motorway tolls, ski lifts, identification of livestock and pets, automobile ignition keys, etc. Thus, there exists a whole range of RFID technologies that have very different purposes and characteristics.

The boom that RFID enjoys today rests on the ability to develop very small and cheap transponders called ``electronic tags''. These tags only offer weak computation and storage capacities. They are passive, that is to say, they do not have their own battery, but take their power from the reader's electromagnetic field, which in turn implies that their communication distance is relatively short, i.e., a few meters in the best case. When they are outside the reader's field, the electronic tags are inert, incapable of carrying out any sort of calculation or communication. However, their low cost and their small size, sometimes less than a square millimeter, gives them undeniable advantages that could be exploited in innumerable domains, for example supply chains, passports, public transportation fare collection, pet identification, access control (eg the UCL's access card), car ignition keys, tagged books in libraries, etc.

The biggest challenge for RFID technology is to provide benefits without threatening the privacy of consumers. Among these threats is the malicious traceability of the tag's holder by an adversary. Authentication protocols executed between a tag and a reader should be immune to such an attack, but this implies a cost in terms of computation when symmetric-key cryptography only is available on the tag.

The goal of this project is to analyse and compare the solutions already suggested [1], [2], [3] and to demonstrate their efficiency by the means of an implementation.

Further readings:

- [1] http://www.cs.berkeley.edu/~daw/papers/librfid-ccs04.pdf
- [2] http://lasecwww.epfl.ch/~gavoine/download/papers/AvoineO-2005-persec.pdf
- [3] http://eprint.iacr.org/2009/092.pdf

Links towards these papers are available from http://www.avoine.net/rfid/

Contact
Information Security Group
UCL / INGI / GSI
Place Saint Barbe, 2
Building Réaumur