



Information Security Group

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

- [Home](#)
- [People](#)
- [Research](#)
- [Publications](#)
- [Press](#)
- [Industry](#)
- [Our Labs](#)
- [RFID Lounge](#)

Proposal 2010-02: RFID Toolbox Reloaded

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

Level: Master thesis. Can also be adapted for a Bachelor thesis.

Keywords: RFID, security, programming, electronic devices.

Requirements: Excellent skills in programming. Ability to learn how to drive RFID devices. Geek-oriented project.

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 goal of this project is to provide a toolbox of easy-to-use programs that enable the read of the usual applications, like Mifare cards, pet identification tags, etc. A first step has been done in 2009/2010 with a first successful Master thesis on this topic. The goal is now to pursue this work and go further in the analysis of RFID systems, e.g. fingerprinting of the tags, collisions on the nonces, fuzzing, ... and to generate an automatic or semi-automatic report of the analysis. This project will use RFID devices like the [OpenPCD reader](#), the [Proxmark](#) sniffer, and the [DemoTag](#). The choice of the language to develop this toolbox is part of the project.

The funny part of this project is that the students will be able during this project to read their own passport, the ID of their pet, their ski pass, etc. They will have to provide super-clean code, well documented, portable, and easy to use.

Further readings: Candidates for this thesis should have a look at the website [Yoki](#), [RFIDiot](#), [LibNFC](#), and [OpenPCD](#).

Contact
Information Security Group
[UCL](#) / [INGI](#) / [GSI](#)
Place Saint Barbe, 2
Building Réaumur
B-1348 Louvain-la-Neuve
Belgium