Information Security Group

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

---

Proposal 2010-01: Practical Cryptanalysis of Pseudo-Random Number Generators in RFID

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

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

Keywords: RFID, Practical Attacks on PRNG.

Requirements: Good skills in implementing. Ability to learn how to play with RFID devices. Knowledge in statistics would be valuable.

Theory: 
Practice:

Abstract:

Randomness is the keystone of any cryptographic system. Generating randomness is yet far from being an easy task, especially with low-cost devices as RFID passive tags. Indeed, on one hand few logic gates can be ``wasted'' just for generating randomness; on the other hand passive RFID tags have no battery - hence no clock - and must so trust in some way the reader that feeds them. Most current pseudo-random number generators

(PRNG) implemented on RFID tags definitely suffer from poor designs. For example, the PRNG implemented on Mifare Classic RFID tags - 1 billion of such tags have been sold since 1995 - is re-initialized each time the tag enters the field of a reader. Consequently an adversary can easily drive the PRNG of a Mifare Classic tag just by measuring the time between the tag is powered and the PRNG is called.

The goal of this project is to analyze in practice PRNGs implemented on tags available in our everyday lives, e.g., tags for building access control, public transportation, ski lift, biometric passport, etc. The analysis will depends on whether or not the specifications of the PRNG are known. When they are not known, which is the most usual case, the RFID tag is considered as a black box and two approaches are required: (1) Determining whether the PRNG can be influenced by some external events; (2) Determining whether the PRNG output is biased. Guidelines and tools provided by the US National Institute of Standards and Technology (See random_number.html) might be useful for this work. The expected aim of this project is to eventually break some RFID solutions in practice.

Depending of the profile of the student, this topic can be tackled from different approaches, either practical or theoretical. For example, it is expected to analyze the PRNG as a black box, but students familiar with reverse engineering techniques may wish apply their knowledge against some PRNGs. Whatever the approach, the student will be required to implement tests, which requires skills in programming. Choice of the language is let to the discretion of the candidate.

Further readings: Candidates for this thesis should have a look at the articles [KoningHG-2008-cardis] and [GarciaKMRVW-2008-esorics]. They should also visit the NIST's web page random_number.html.

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

Gildas Avoine
gildas.avoine@uclouvain.be
