Information Security Group

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

- Home
- People
- Research
- Publications
- Press
- Industry
- Our Labs
- RFID Lounge

Proposal 2010-05: Decoding Information Obtained from a Chip

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

Level: Bachelor thesis.

Keywords: Security, Information theory, Constrained environments, Practical cryptanalysis.

Requirements: The student should like challenging tasks as decrypting data by hand using tips. This requires him to be rigorous, tidy, and patient.

Theory:	●●●●○
Practice:	●●○○○

Abstract:

Information stored in restricted environments e.g. contactless chips is sometimes not directly intelligible after reading, although it is usually not encrypted. This can be due to compression of the data, encoding in non-standard formats, unknown offset, ... Retrieving the useful information is not an easy task due to the small quantity of available data. Tips or tricks are usually needed to succeed, e.g. trying to find some dates, times, UID, names, etc. in the analyzed data. Corroborating the obtained information is

sometimes fruitful; for example, if the analyzed contactless chip is used for the application X, perhaps analyzing the content of the website that describes X may help to guess the content of the chip. Also, performing a differential comparison of the data obtained from several devices can reveal some patterns. The goal of this project is to develop a tool whose aim is to retrieve the untelligible information in data extracted from a chip.

Further readings: As an example, interested candidates should read the article entitled "Lire son Passe Navigo en un clin d'oeil" published in the magazine MISC, Number 48, March/April 2010.

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

Last update: Thu, 04 Mar 2010 23:59:00 +0100