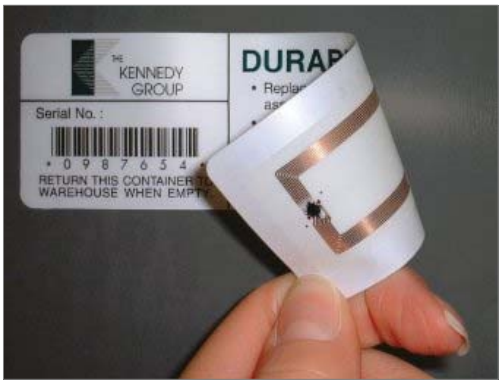
Project Description:

RFID Tags

Application Scenario



A passive RFID tag consists of a tiny chip combined with an antenna, but without an autonomous power supply. The tag receives its energy from a reading device and is powered only when spoken to. A typical application for such a chip is for identification purposes: A reading device sends a query and the chip responds by sending its ID, thus confirming that the tag is close by. A sample application would be that of an electronic product code: Instead of scanning the bar code of one product at a time, a reader could read the serial numbers of a whole bunch of products at once. This increases efficiency both in the supply chain and upon supermarket check-out.

Apart from giving rise to privacy concerns, this simple approach is far from secure though. A suitable radio device can record the ID and replay it when desired. This is critical for applications where correct identification is important. As a working example, think of a pharmacy that checks whether the medicine that is received from a supplier is authentic or whether it deals with a cheap placebo. Given a non-cryptographic solution, it would be easy to equip the counterfeit medicine with tags that reply by sending the IDs recorded from authentic packages.

Thus, we need a cryptographically secure authentication solution for RFID tags. However, such tags do not have enough capacity to run standard cryptographic components like AES or SHA-2. Instead, they have to rely on so-called *light-weight* authentication protocols which use much less gates and also very little energy. Your task is to look at some protocols in the literature and choose one that is suitable for a medicine anti-forgery application.
Hint: Pay attention to Replay-Attacks, and to Distance-bounding protocols for avoiding those.

Project Definition

Design, evaluate and document an RFID solution that addresses the issues presented by the scenario outlined above. Issues that *must* be addressed are:

- Risk analysis: What assets are at stake?
- Threat model: What assumptions do you make about the attacker(s), and what threats is your system supposed to protect against?
- Comparison: Examine a number of possible solutions with respect to the resources consumed. Important parameters in this investigation are the running time of the algorithms, the memory footprint of its implementation, power consumption and any special requirements on the processor hardware imposed by the proposed solution. The evaluation should consider as many of these parameters as possible.
- Security: Make sure that your system protects against the security issues raised in the threat model, and clearly document the threats that you do not protect against.