

SSN Project Proposal

Stamatis Maritsas
Kenneth van Rijsbergen
Yadvir Singh

Abstract

Today RFID tags are used in many places where a user has to be authenticated. The scope of this research project is to create a secure Android mobile application that is going to be used to access usernames and passwords stored in a card based on RFID technology making the user's life easier.

1 Research question

How can we securely store/access sensitive data on a RFID card using an Android mobile application?

Our research is going to include the following steps:

1. Investigate RFID implementation, Android SDK and available encryption/decryption mechanisms that we could implement.
2. Review what is the most secure solution on how the sensitive data are going to be stored/accessed on the RFID card (symmetric/asymmetric cryptography?)
3. Dive into Android SDK, start the development of the mobile application and set up the test environment.
4. Run specific tests to verify the functionality of the whole application and drawing conclusions, which indicate how close we finally got comparing to our initial goal.

2 Related work

Nowadays, we have more and more applications that are based on RFID implementation but the big question that arises is "How secure is this mechanism?". Although, it is safe to say that this technology has matured enough to be used in toll-gate payment systems, automobile security, casino management, animal tracking etc., it would not be wise to say that RFIDs are secure enough when it comes down to financial transactions or using ID documents embedded with RFID chips unless better safeguards are implemented to ensure foolproof security. [?]

The paper by Ortiz Jr. stated that there are a number of security issues that arise with the use of RFID. They can for example be used to send malicious data to a back end server. SRI Internationals Neumann stated further that terrorist could copy cards that give access to RFID-based airport luggage-scanning systems. There is also a possibility that hackers "could record data from an RFID chip that is on an inexpensive product and upload the data to a chip that is on an expensive product, thereby getting the latter for a lower price" says Lukas Grunwald, a consultant with DN-Systems Enterprise Solution. [?]

3 Planning

Week	Work
1	Start by looking at RFID implementation, deciding how data are going to be structured, looking at Android SDK and investigate encryptions methods and libraries. Also, we are going to decide how the design of the application is going to be.
2	Start the development of a prototype application in an incremental approach. Phase 1 of 2nd week: Test the writing/reading procedure on the card using plaintext. Phase 2 of 2nd week: Implement encryption/decryption.
3	Finalize the software application and run complete tests on the whole functionality.
4	Writing the report, making conclusions, start writing down our test results and preparing the presentation.

4 Hardware

We intended to use an Android smartphone with NFC in combination with blank RFID cards.

5 Ethical issues

Due to the use of sensitive data (usernames and passwords) we have to make sure that the software is going to be as secured as possible. The encryption method that we are going to use has to be recommended as secured by the informatics community.

In addition, the libraries that we are going to use for the encryption must be well-defined and properly tested to make sure that is a correct implementation of the cryptosystem.

Finally, we have to make sure that in the implementation there will be no vulnerabilities except from the encryption mechanism.