A Study of Radio Frequency Identification Authentication Protocols

Researcher: Sidhartha Mishra

Faculty Mentor: Dr. Xiaowen Zhang

Computer Science Department

INTRODUCTION

- RFID (Radio Frequency Identification) technology has gained popularity in recent years due to the decreasing manufacturing cost of tags combined with its ease of communication - does not require line-of-sight scanning or physical contact
- Two major types of tags: passive and active – passive tags are more popular due to lower cost but have a shorter communication range and limited processing power
- A typical RFID infrastructure contains of RFID tags, readers, and backend server(s)
- Each RFID tag provides a unique identification number

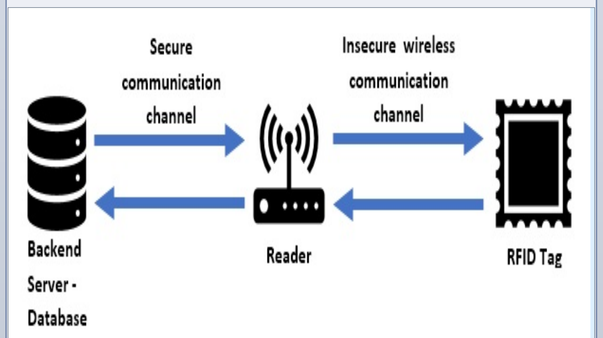

Figure 1: Diagram depicting a RFID ecosystem containing the backend server, reader, and tag

- The tags contain the identifying information corresponding to their corresponding object which is sent to the reader, which in turn is connected to the back-end server
- The connection between the reader(s) and the backend server is generally considered secure
- The communication between the tag(s) and the reader(s) takes place on a wireless channel which is considered insecure due to its susceptibility to various types of malicious attacks raising privacy and security concerns
- Tags have access to limited computational resources and therefore lightweight security solutions – Authentication Protocols – should be considered to provide adequate security
- In this research project, four lightweight protocols are simulated and studied with respect to their workings and security issues/ performance – two of these protocols rely on one-way hash functions while the other two make use of bitwise logic operations and/or matrix operations

PROTOCOLS

Protocol 1:

- This protocol was proposed by Muwanguzi and Biermann
- It is based on Hopper and Blum's HB protocol
- Requires minimal computation power and is therefore suitable for low-cost RFID tags
- Makes use of bitwise operations such as XOR and AND
- The protocols uses the idea of randomness in its computation involving authentication, combined with the reliance of one secret number on another, which makes it resistant to many types of malicious attacks including man-in-the-middle attacks, eavesdropping, spoofing, cloning, tracking, and unauthorized tag disabling
- Notation:
  - a: 32-bit Random Number on Reader side
  - b: 32-bit Random Number on Tag side
  - x / y: 64-bit secret key on Tag/Server side

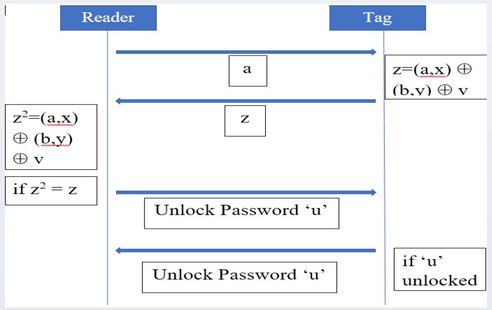

Figure 2: The protocol proposed by Muwanguzi and Biermann

Protocol 4:

- OHLCAP (enhanced): Originally proposed by Choi et al. Enhanced by Ha et al.
- Lightweight protocol utilizes one-way hash functions in combination with bitwise logic operations
- Any lightweight hash function may be used to implement this protocol and facilitate authentication
- Similar to LCAP the protocol aims for mutual authentication
- Freshness of the shared secret may not be guaranteed as the ID is not updated regularly and is therefore static, making the enhanced version fall short in comparison to the original LCAP protocol
- Notation:
  - N_R, N_T: Nonce generated by Reader and Tag, respectively
  - H: One-way hash function
  - H_L, H_R: Left and Right halves of computed hash values
  - ID,K: secret values shared with Tag and Reader

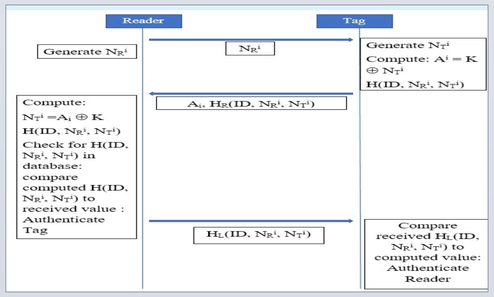

Figure 3: Enhanced OHLCAP protocol by Ha et al

SIMULATION PROGRAM

As part of this research project, a simulation program has been created to demonstrate the communication taking place in each of the protocols studied. The application has been programmed using the C# programming language and features a user-friendly Graphical User Interface (GUI) which can be run on a PC.

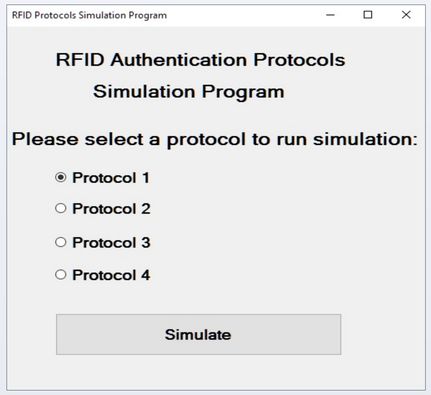

Figure 4: Screenshot of the RFID Authentication Protocol Simulation Program

This program contains two separate parts : server and client. The server side of the application corresponds to the reader in the RFID ecosystem, whereas the client corresponds to the tag.

The program utilizes socket programming to implement the server and client programs. Socket programming allows for communication between the two entities in order to simulate the exchange of messages/information between the reader and the tag.

- Server/ Reader program:
  - Allocates a dedicated port on the local machine for communication with client/tag program
  - Runs in an infinite loop until closed by the user
  - Accepts connection from client/tag and executes the code corresponding to the chosen protocol
  - The Server/Reader program utilizes the SHA1 hash function to implement the hash based protocols

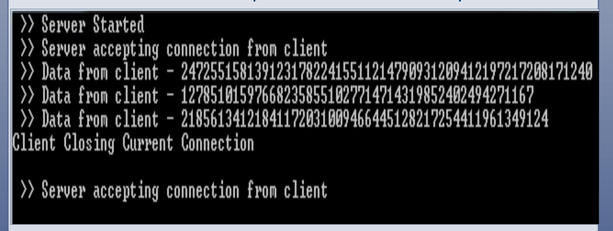

Figure 5: Screenshot of the Server/Reader program

- Client/Tag program:
  - Establishes connection with Server/Reader
  - Sends identifier to Server/Reader program to denote the chosen protocol then runs the code for the corresponding protocol
  - Performs a run-through of communication needed for authentication according to the respective protocol

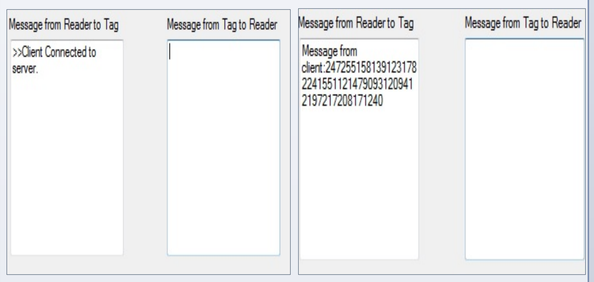

Figure 4: Screenshots of the RFID Authentication Protocol Simulation – Client/Tag program

CONCLUSION

Each of the RFID Authentication Protocols studied in this research project have their strengths and weaknesses. Some of these strengths and weaknesses have been discussed and outlined based on literature review. In order to determine the ideal choice of protocol for a given application, one must consider these pros and cons in relevance to the level of security required by the specific application and any applicable technical limitations for which it is planning to be used. As a note of further study, the simulation program created for this research project may be implemented as a web application so that it can be accessed via the Internet.

MAIN REFERENCES

[1]R. Mahmood and W. Al-Hamdani, 'Is RFID Technology Secure and Private?', in *InfoSecCD Information Security Curriculum Development*, 2011, pp. 42-49.

[2]R. Aggarwal and M. Das, 'RFID Security in the Context of "Internet of Things"', in *SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things*, 2012, pp. 51-56.

[3]S. Karthikeyan and M. Nesterenko, 'RFID Security without Extensive Cryptography', in *CCS Computer and Communications Security*, 2005, pp. 63-67.

[4]M. Muwanguzi and E. Biermann, 'Integrated Security Framework for Low Cost RFID Tags', in *SAICSIT '10 Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*, 2010, pp. 201-208.

[5] X. Zhang, Q. Gao, and M. Saad, 'Looking at a class of RFID APs through GNY logic', in *International Journal of Security and Networks,* Vol. 5, 2010, pp. 135-146.