Peer Review – Survey on Passive RFID Tag Cryptography for Non-Specialists

Summary

This paper explains the cryptography mechanism and challenges of passive RFID tags. In this paper, the reader will be introduced to the principles and security concepts of passive RFID tags. Using Avoine's adversary model, this paper also discusses the security measure against tracking passive RFID tags.

This paper is recommended for a reader that is interested in the cryptography of RFID but does not possess extensive literature background in this field.

Strength

- This paper discusses RFID security in a manner that is understandable for a person new to this field.
- Good uses of metaphor in explaining the mechanism of RFID protocol.
- This paper utilizes many sources to support its content.

Weakness

- Despite being claimed to be a starting point regarding RFID, this paper requires more elaborated information regarding the basic RFID mechanism, such as how RFID memory is structured, what it contains, and how the basic authentication protocol of RFID actually works.
- The use of RFID technology seems not to be relevant as a background.
- The paper lacks an elaborated and explicit explanation of the impracticality of certain RFID categories.
- It is hard to make a correlation between the third and fifth cryptography protocols in preventing the adversary introduced (Avoine) reach its goal.

- This paper needs to be more clear in stating the advantages and disadvantages of each cryptography protocol.
- The related work of the paper does not explain the uniqueness or urgency of the paper compared to other papers in the same field.
- The Evaluation section of this paper does not discuss the evaluation of the paper, but rather the evaluation of discussed cryptography protocols. The content of this section can be combined with the explanation of the discussed cryptography protocols itself to add more context.

Comments

- Keywords are missing.
- As an explanatory, this paper is too dense and feels more like a summary.
- In subsection III.A: In pointing out the usage of RFID technology, the enumeration of the paragraph seems too much.
- In subsection III.B: The categorization of RFID needs more structured paragraphs.
- In III.C.2: Explain briefly the definition of backscatter modulation around the part where it is applied.
- After the headline of section IV: The paragraph is too long and can be divided into two separate paragraphs
- In subsection IV.A: Capabilities of RFID protocol can be made into bullet points to improve readability
- In subsection V.E: Maybe introduce the name of RFID tags since the beginning of the explanation to avoid confusion
- In VII: Mention the author of the paper in citation 28.