© 2020 IJSRST | Volume 7 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST

Study of Security Threats and Authentication Protocols of RFID

Vijay Kumar Verma
M. Phil. Students, Department of Physics, B. R. A. Bihar University, Muzaffarpur-842001, Bihar, India

ABSTRACT

In this paper, we studied about security threats of RFID. RFID facilitates detection and identification of objects that are not easily detectable or distinguishable by using current sensor technologies.

Keywords: RFID, WSN, Radio Waves, Sensor.

I. INTRODUCTION

Radio frequency identification (RFID) uses electromagnetic field of radio frequency for automatic identification of objects with a unique ID number which is stored in the attached tag [1]. Both RFID and barcode systems have the same goal; identifying objects without human intervention. RFID systems have many continuing and emerging applications like access controls, tool management, supply chains, airline baggage management, livestock or inventory tracking and so on. It can also be used to distinguish between counterfeits and authentic products. The important security and operational problems such as cloning problem, tracing problem and scalability can be solved by RFID system with cheaper RFID tags for commercial application. Security can be CMOS technologies progressively efficient and the production costs decrease, which allows stronger security solutions on tags. More expensive tags with constraints power source, less memory, gate can be used for certain commercial application such as access controls systems and costly goods for security [1] [2].

II. SECURITY MODEL FOR RFID SYSTEM

This section describes a security model. The system consists of three components: a trusted server *S*, reader *R*, and tag *T*.

- Typically Tags have no its own power. It operates on electromagnetic field. These are wireless Trans ponders.
- The fields are generated by the transceiver that is the Reader. There exits two kind of broadcast challenges by responding the tags. These are unicast and multi-cast. Under the range of reader, these are addressed to all tags. But unicast challenges are addressed to particular tags.
- Server: The system has a trusted Server communicates with the reader and also reader communicated with the server. We consider that all honest tags *T* follow the protocol's requirements and system specifications. The parameters fixed are applied to the honest readers *R* and the trusted server *S*. Both Tag *T* and reader *R* interact by sending and receiving of data as an authentication transcript. We assume

the communication take place through secure channel. Since two parties involves in this communication, we can consider as two-party protocols.

III. SECURITY PROPERTIES AND ADVERSARY

This section describes the security properties and the adversary model. The protocol can be modeled in terms of the following four games with players the PPT adversary *A* against the honest tags *T* and the readers *R*. We have followed the Chatmon *e*t.al [3] protocol for this model.

- G_{auth} : Game for authentication
- G_{anon} : Game to achieve anonymity
- G_{trace} : Game for tracing
- G_{avail}: Game for availability

The game runs by the following steps.

- Initialization: In this phase the adversary A interacts with the tags and the readers in arbitrary manner.
- The knowledge of A will be examined. $Adv_G(A)$ denotes the score of A in game G . The adversary A that has no negligible advantage A to win the game G. Formally we can say

$$\mathbf{Adv_G(A) = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k_{\mu}, \mu > 0}$$

IV. PERFORMANCE ANALYSIS

We can evaluate the performance of the proposed protocol in term of its computation cost. Computation time for authentication can be evaluated in two phases verification and mutual authentication [7] [8] [9]. Consider the following notation to compute computation time.

- T_H : time requires to compute hash function.
- T_{add} : time requires for addition of points on Elliptic curve.
- T_{PK} : time require to compute private key.
- T_{PU} : time require to compute public key.
- T_{mul} : time for point multiplication.
- Te : Elliptic curve polynomial computation time.

Total computation time is $T = 11T_H + 4T_{add} + 6T_{mul} + 2T_e$

V. CONCLUSION

In this chapter, we have proposed an authentication protocol with provable security. It is resistant to insider attack, masquerade attack and provides mutual authentication. Security of the protocol relies on ECDLP. The protocol is also susceptible to forgery attacks. Since more expensive tags with constraints power source, less memory, gate can be used for certain commercial application such as access controls systems, the protocol is most suitable for implementation.

VI. REFERENCES

[1]. S. W. Wang, W. H. Chen, C. S. Ong, L. Liu and Y.W. Chuang, RFID application in hospitals: A case study on a demonstration RFID project in a taiwan hospital, system sciences, HICSS'06, Proceedings of the 39th Annual Hawaii International Conference 8 (2006).

[2]. R. Das, RFID forecasts, players & opportunities 2007–2017, Enterprise Networks & Servers, (March 2007).

[3]. C.F. Hernández, P.H. Ibargüengoytia-González, J.G. Hernández, J.A. Díaz, "Wireless Sensor Networks and Applications: a Survey", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, Pages 264 -273. March 2007.

[4]. Hasan Tahir, Syed Asim Ali Shah, "Wireless Sensor Networks– A Security Perspective", 12th IEEE International Multitopic Conference, Karachi, pp. 189-193, December 23-24, 2008.

[5]. Yee Wei Law, Paul J.M. Havinga, "How to secure a wireless sensor network", Published in Intelligent Sensors, Sensor Networks andInformation Processing 2005. IEEE pp 89-95.

[6]. L. Zhang and Z. Wang, Integration of RFID into wireless sensor networks: Architectures, opportunities and challenging problems. Proceedings of the 5th International Conference on Grid and Cooperative Computing Workshops (GCCW'06) (2006).