Society for Science and Education
United Kingdom

TNC Transactions on Networks and Communications

Volume 2, Issue 5
ISSN: 2054 - 7420

Security issues in RFID Middleware Systems: Proposed EPC implementation for network layer attacks

Arif Sari
School of Applied Sciences, Department of Management Information Systems, European University of Lefke, Lefke, Cyprus;
asari@ieee.org

ABSTRACT

Recently, Radio Frequency Identification (RFID) technology becomes very popular. Especially low-cost RFID tags are widely used in supply chain management. Due to lack of security considerations in simple RFID technology, performance optimization becomes quite important rather than securing the data transmitted over RFID media. Since security holes shown variety in RFID systems, this paper classifies the attacks that occurs in different layer of RFID models. The security enhanced EPC RFID middleware systems that are widely used in organizations and their vulnerabilities against Network Layer attacks are investigated in this research to clarify the actual impact of network layer attacks in RFID systems. This paper investigates the RFID middleware attacks and impact of possible integration of EPCglobal architecture to mitigate such attacks on RFID systems.

Keywords: RFID Security, RFID attacks, classification, EPCglobal middleware systems, network layer attacks.

1 Introduction

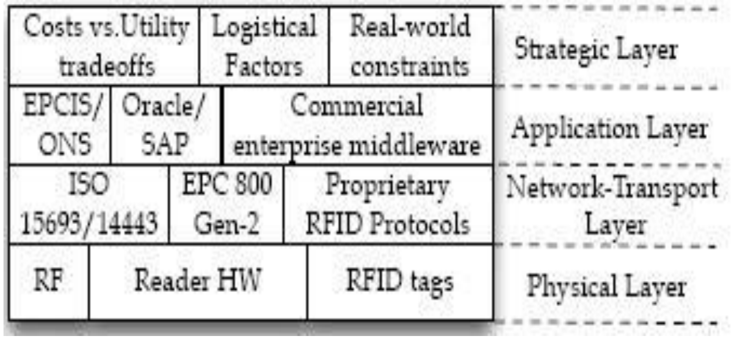
Radio-Frequency Identification (RFID) tags become quite popular since organizations are highly spending in implementing security measures to protect their information assets [1]. The RFID is used to describe a system that transmits the identity of an object or a person wirelessly using radio waves [2]. The simplest types of RFID tags are devices that are quite passive, and have no internal power source. This technology is currently used in security access control systems and can therefore be implemented in enhancing internet security within an organization [3]. This is because RFID has long been as an electronic key to control who has access to office building or areas within an organization. Through the automatic data collection, RFID technology can achieve greater visibility and product velocity across supply chains, more efficient inventory management, easier product tracking and monitoring, reduced product counterfeiting. However providing security such a big network is quite difficult and since the design and implementation of RFID systems are addressed the performance optimization, security issues creates a great challenge for the RFID systems. This paper addresses this problem by analyzing RFID network that uses security enhanced middleware systems and under Network layer attacks. In RFID systems, varieties of attacks are available. In the following sections, different types of attacks are also discussed briefly. As it is also well known that because of the lack of security considerations, the new middleware must be addressed in order to define the security problems and solutions. For that reason, ALE and EPC Global

DOI: 10.14738/tnc.25.431
Publication Date: 11th September 2014
URL: http://dx.doi.org/10.14738/tnc.25.431

Network is also discussed that major concepts of RFID middleware systems in the methodology section where Network-Transport Layer attacks impacts are also discussed.

2 Classification of RFID layers

The RFID systems can be classified into different segments in terms of layers. The Figure 1 below illustrates the RFID communication layers.



Costs vs.Utility tradeoffs	Logistical Factors	Real-world constraints	Strategic Layer
EPCIS/ ONS	Oracle/ SAP	Commercial enterprise middleware	Application Layer
ISO 15693/14443	EPC 800 Gen-2	Proprietary RFID Protocols	Network-Transport Layer
RF	Reader HW	RFID tags	Physical Layer

Figure 1: RFID Communication Layers

Due to scope of this study, all of the layers presented on the Figure 1 above are discussed briefly while each and every layer can be investigated separately.

The first layer in the communication protocol is Physical Layer. The physical layer is the combination of physical interface, radio signals and RFID devices. Since the nature wireless communication environment of RFID systems that leads lack of resilience against physical manipulation, the attackers simply disable RFID tags through relay attacks. The Network layer or Transport Layer is the second layer of the RFID communication system that includes all kind of attacks which are related the way that data are transferred between the entities of an RFID network the attacks that are based on the way the RFID systems communicate and the way that data are transferred between the entities of an RFID network components.

The third layer is called Application layer which includes all kind of attacks that target information related to applications and the binging between users and RFID tags.

The Strategic layer includes organizational data coverage area and covers competitive espionage, social engineering, privacy and targeted security threats.

3 Classıficatıon of RFID attacks

As it is discussed briefly in the previous section, RFID layers are classified into different layers and each of these layers has its own characteristics. The RFID attacks are classified based on the characteristics of these layers. The Figure 2 below illustrates the classification of RFID attacks.

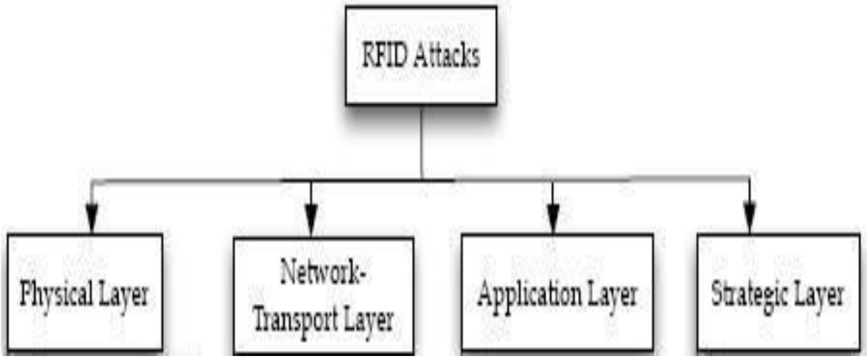


Figure 2: Classification of RFID Attacks

In the literature, varieties of researches have also been stated different classifications of possible threats and risks in RFID networks ([4], [5], [6], [7]).

The detailed classification of business intelligence risks have stated by the author [30]. The researcher [4,7] have proven that the privacy issues of RFID systems cannot be solved through separate studies or separate consideration of layers.

Since this research focuses RFID middleware systems that contains EPC global network, Network-Transport layer must be investigated specifically.

In EPC global architecture, the message that transmitted is secured in the middleware and protected through specific system [8]. This allows companies and organizations to implement and carry out a secure data transmission. In the next section, the EPC global middleware and Network-Transport layer attack is discussed.

4 Proposed Methodology

The RFID Middleware systems contain EPCglobal network architecture. The Figure 3 below illustrates the EPCglobal Network architecture. The EPCglobal Network consists of the ID System (EPC Tags and Readers) EPC Middleware, Electronic Product Code (EPC), Object Name Services (ONS) and EPS Information Services (EPICS) [2]. The EPC sits on the tags and it is a number that is designed to uniquely identify an individual object in the supply chain process. The role of RFID middleware is to handle data interchange between the various systems within the architecture. The diagram below shows an EPCglobal Network Architecture [9].

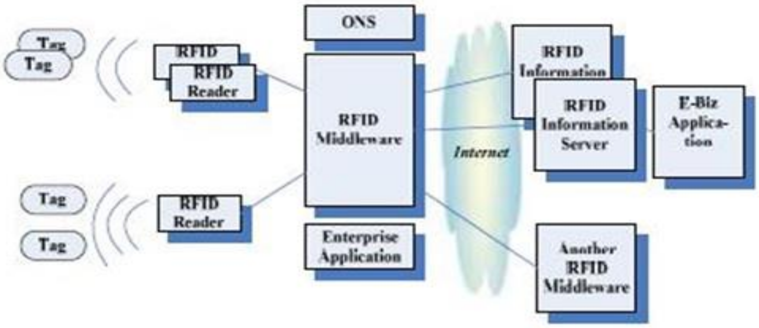


Figure 3: EPCGloblal Network Architecture

All implementation of EPC middleware system belongs to Network-Transport layer, and this layer includes all the attacks that are based on the way the RFID systems communicate and the way that data are transferred between the entities of an RFID network (tags, readers). This section describes the network layer attacks that affect the network transport layer and it's affect on the EPC Global Network architecture and possible solutions to cope with these attacks.

The Secure enhanced middleware system can be achieved through secure middleware system architecture, identification and authentication and transport data protection. This goal has achieved since the proposed mechanism already have the middleware. The classification of attacks shown on the Figure 4 below illustrates that the Network-Transport Layer attacks are categorized under 3 categories which are; Tag attacks, Reader Attacks and Network Protocol Attacks. The Tag attacks are divided into two categories such as Cloning and Spoofing. Cloning is replication of legitimate RFID tags as fake ones that does not require extraordinary financial support and easy to implement through writable and reprogrammable tags. Spoofing is similar to cloning since it's not required to have physical RFID tag, but allows adversary to gain same privileges electronically.

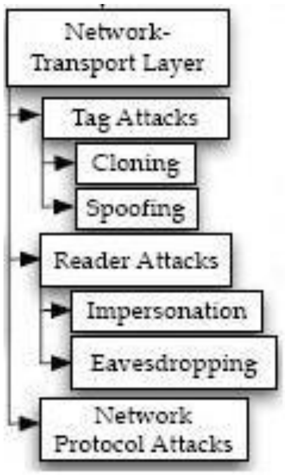


Figure 4: Network Transport Layer Attack Classification

The next category is Reader attacks that fall into 2 different sections such as impersonation and eavesdropping attacks. The Impersonation attacks may occur when the RFID system has unauthenticated communication line and adversary counterfeits the legitimate reader. Eavesdropping attacks sniff the communication between legitimate RFID tags and readers and collect the information. The collected information is used to perform more sophisticated attacks in the future.

The network protocol attacks are the last category that covers the back-end systems and networking infrastructures that communicates with RFID systems. The variety of attacks can be classified and investigated specifically under the Network Protocol attacks since it covers network infrastructure and databases. The operating systems, communication protocols or any other entrusted node especially in wide networks may be used by an adversary to compromise the system.

The cloning and spoofing can be simply prevented in 21st century's technology. A researcher have proposed a specific intrusion detection mechanism against cloning attacks that with the false alarm rates from %2.52 to %8.4 which seems quite successful [10]. The RFID Middleware system encrypts the message through the middleware that prevents passive eavesdropping attacks rather than storing less information on RFID tags. This system will force users to retrieve requested information from the back-end databases that may lead another information leakage and requires further investigation on Network Protocol attacks. The proposed RFID middleware system uses digital signature encryption functions such as X.509 certificate for authentication or private key [9]. In addition to this, EPCglobal Architecture Application Level Events (ALE) layer uses differentiated access control policies that secure not only the entire transmission media but the message itself at the each intermediary checkpoint. This prevents eavesdropping [3]. In addition to this specific feature, there are other proposed encryption mechanisms proposed by the researchers that can be implemented on RFID middleware systems for to enhance security such as hash-lock [11], randomized hash-lock [12] and chained hashes [13].

5 Conclusion

There are several tasks involved in incorporating RFID in protecting variety of attacks in or outside of the organization. In this study, possible network layer attacks are discussed with EPCglobal network architecture by considering the point of attack based on the RFID layers. However each and every category should to be investigated separately for better understanding of each attack and its countermeasures. The main aim of this empirical investigation was to expose and highlight the network layer attacks on RFID layers. The use of middleware contains encryption mechanisms in its nature so it ensures confidentiality and integrity of the information transmitted over the internet. The study can be expanded by examining also other types of threats and give a better overview of the problem by discussing possible countermeasures in each category of RFID attacks in the future.

REFERENCES

[1]. Kindberg et al. (2002), “People, Places, and Things: Web Presence of the Real World,” ACM Mobile Works & Applications J., pp. 365-376.

[2]. Whiting, R. (2004). “RFID growth poses a data management challenge,” Computing, pp. 29-30. Publisher: VNU Business Publications, UK.

[3]. Finkelzeller, K. (2003). The RFID Handbook, 2nd ed., John Wiley & Sons.

[4]. Garfinkel, S., Juels, A., and Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. IEEE Security & Privacy, 3(3), 34-43.

[5]. [5] Ayoade, J. (2007). Privacy and RFID Systems, Roadmap for solving security and privacy concerns in RFID systems. Computer Law & Security Report 23, 555-561.

[6]. Karygiannis, A., Phillips, T., and Tsibertzopoulos, A. (2006). RFID security: A taxonomy of risk. In Proceedings of the 1st International Conference on Communications and Networking in China (ChinaCom'06), October 2006, Beijing, China (pp. 1-7). IEEE Press.

[7]. Avoine, G. & Oechslin, P. (2005). RFID traceability: a multilayer problem. In A.S. Patrick, M. Yung (Eds.), Financial Cryptography and Data Security, 9th International C, FS 2005, Roseau, The Commonwealth of Dominica, Lecture Notes in Computer Science, Security and Cryptology, vol. 3570, (pp.125-140). Berlin, Heidelberg: Springer-Verlag. doi:10.1007/b137875.

[8]. Sari, A. (2010). RFID Security Models use of Security Enhanced RFID Middleware Systems for Enhancing Organizational Data Security. 6th ArchEng International Symposium of European University of Lefke, Vol 6.

[9]. Jieun, S. and Kim, T. (2005). Security Enhanced RFID Middleware System. Retrieved from *http://www.waset.org/journals/waset/v10/v10-16.pdf*

[10]. Mirowski, L. , Hartnett, J. (2007). Deckard: A system to detect change of RFID tag ownership. International Journal of Computer Science and Network Security, 7(7):89 -98.

[11]. Weis, S.A. (2003) Security and privacy in Radio-Frequency Identi_cation devices. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

[12]. Weis, S., Sarma, S., Rivest, R., and Engels, D. (2003). Security and privacy aspects of low-cost Radio Frequency Identi_cation systems. In D. Hutter, G. M�uller, W. Stephan, M. Ullmann (Eds.), Security in Pervasive Computing, Proceedings of the 1st International Conference in Security in Pervasive Computing, Boppard, Germany, March 12-14, 2003, Lecture Notes in Computer Science, vol. 2802, (pp. 201- 212). Berlin, Heidelberg: Springer Verlag. doi:10.1007/b95124.

[13]. Ohkubo, M., Suzuki, K., and Kinoshita, S. (2003). Cryptographic approach to privacyfriendly" tags. In Proceedings of RFID Privacy Workshop, MIT, MA, USA.