A SECURE METHOD FOR RFID WITH KEY TAG IN SUPPLY CHAIN MANAGEMENT

Hsieh-Hong Huang, Cheng-Yuan Ku, Department of Information Management,
National Chung Cheng University, 160 San-Hsing, Min-Hsiung, Chia-Yi 621, Taiwan, R.O.C.,
{chorist, cooperku}@mis.ccu.edu.tw

ABSTRACT

This paper proposed a secure method with key tag to prevent RFID tags from eavesdropping and also discuss other security issues about RFID systems. The proposed architecture provides a transparent to legacy system based on some cryptographic methods, such as triple-DES and Public Key Infrastructure (PKI). It could work compatibly with original item-identifier systems and material management systems in logistic network or supply chain environment, especially to high-tech or defense industry with high secrecy and confidentiality. We proposed to use symmetric cipher such as triple-DES to encrypt original EPC to be ciphertext with additional bits to store the information about the key, named "key tag", in RFID tags. Manufacturers attach on their products with the encrypted tags and ship them to the distribution center or other warehouses. Only authenticated users who are certificated by Certification Authority (CA) will get the key to decrypt the encrypted-tag to obtain the original EPC. And then query item information in Object Name Service (ONS) using Physical Markup Language (PML), the architecture proposed by Auto-ID Center, Massachusetts Institute of Technology (MIT). Transmitting tag codes in secure method prevents item information from malicious eavesdropping and ensures items security in supply chain management.

INTRODUCTION

In a supply chain, raw materials are procured, items are produced at factories, and then shipped to retailers or customers. Companies that transport a lot of items everyday need tools to track and locate them easily [8]. Information and communication technologies have been taken into account to reduce cost and improve quality of service [7]. A typical manufacturing or distributing process contains several phases in which items are handled and are to be identified. Automated identification reduced both the labor cost and errors in identification. Cause of the success of bar-code technology since 1974, automatic data capture technology has been a boon for productivity and bottom-line results. Although bar-code has many features such as low-cost, easy-to-make, and visual, there are limitations. For instance, the alignment with bar-code scanner, the location bar-code labeled, and the reading range limit its applications. A new auto data capture technology, RFID, comes to solve this problem. RFID technology has reach maturity both in ability and reliability [5]. In this study, we proposed a simple but feasible method using the key tag in RFID tag to protect items information.

With the advent of RFID technology, RFID-related security and privacy issues are raised [6]. There are several approaches, such as hash-luck, kill tag, faraday cage, active jamming, blocker tag, PRF-based private authentication etc. to prevent RFID tags from these privacy threats but there is no single approach could be completely satisfactory [2][3][4][10][11]. The limitation of pages does not allow us to survey all these works.

PROPOSED ARCHITECTURE

In this paper, we proposed to encrypt the original EPC and then pad extra codes to be identifier, named "key tag", to show the way where and how to get it decrypted. The key tag did not store the key but store the serial number of the key. There are several ways to encrypt the code, for example, Data Encryption Standard (DES), triple-DES, etc., depending on the tradeoff between strength and complexity [9]. Only those who have priority and certificated by CA have privilege to get the specific key. Next we discuss how it woks with 64-bit EPC and triple-DES, the most popular and widely used EPC and encryption scheme. We used a reserved 96-bit EPC segment to store the items information with 64-bit GITM-compatible EPC so that we will have the rest 32 bits for identification of keys. Those who get this encrypted code could use it as common use in supply chain environment, for instance, register the item, identified the item, and so on. The original 64-bit EPC will be encrypted into 64-bit ciphertext by triple-DES and extend to 96-bit EPC with necessary header and additional key tag. During the manufacture processing or distribution, all parties of the chain will only get a meaningless 96-bit EPC for identification. It is enough for users to track the product information but no more detailed data about the item. Using the key it could be decrypted into original 64-bit EPC and query the item information via PML and ONS on the Internet.

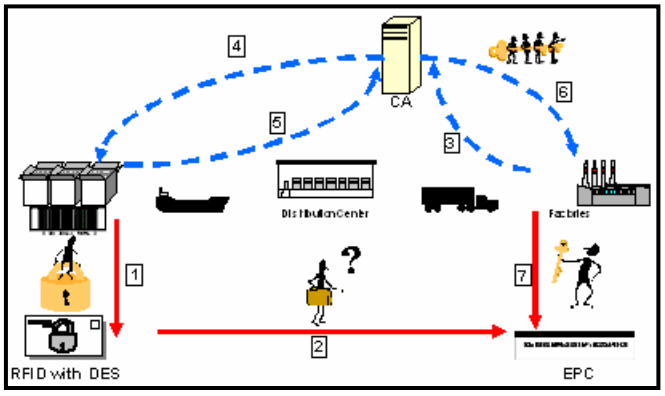

Figure 1 System Architecture

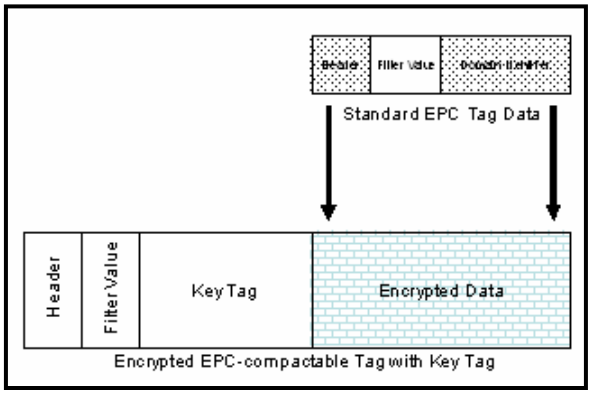

Figure 2 Tag Encoding

Here is an example to show how the architecture works. When an item was made in the factory, a 64-bit EPC was assigned to it. The EPC was assigned by the coding rule defined by EAN/UCC and Auto-ID

center [1]. Those who want to know what the EPC means could send a PML query to the ONS and get the product information in common. Then we encrypted the original EPC into ciphertext using triple-DES for privacy or security reason (Step 1). It becomes a valid 96-bit EPC code that combine encrypted-EPC with additional 32-bit, header, manufacturer-identifier and key tag (Step 2). Only supply chain members could ask manufacturers for the key to decrypt the code. They should have been authorized via CA to show the key tag to get the key to encrypted-EPC (Step 3, 4, 5, 6, 7).

DISCUSSION AND CONCLUSION

This paper presents a novel method that using the encryption methods with key tag to protect RFID security. The process can be divided into two parts. One is encryption, which is using triple-DES or other encryption to encrypt original EPC and padding its key tag without any computational function on tags. Then the tags would be as cheap as possible. The other is mutual authentication between producer and product holder. The encryption and certificate authorization technologies are adopted because they are mature. Although the proposed method requires an infrastructure of CA and KDC, it is simple and easily implemented.

ACKNOWLEDGEMENTS

This research was supported by the National Science Council of the Republic of China under grants NSC93-2218-E-194-016.

SELECTED REFERENCES

[1] Brock, D. L., Integrating the Electronic Product Code (EPC) and the Global Trade Number (GTIN), Auto-ID Center, November 1, 2001

[2] Juels, A., Rivest, R. L., and Szydlo, M., "The blocker tag: selective blocking of RFID tags for consumer privacy", *Proceedings of the 10th ACM conference on Computer and communication security*, October 27-30, 2003

[3] Molnar, D. and Wager, D., "Privacy and Security in Library RFID - Issues, Practices, and Architectures", *Proceedings of the 11th ACM Conference on Computer and Communication Security*, October 25-29, 2004

[4] Rivest, R., Sarma, S., Garfinkel, S., and Weis, Stephen, Privacy and Security in Radio-Frequency Identification Systems, MIT Laboratory for Computer Science, March 2003

[5] Schwirn, M., RFID Comes of Age in Manufacturing and Supply-Chain Applications, SRIC-BI SCAN: D04-2460, SRI Consulting Business Intelligence, February 2004

[6] Schwirn, M., Beyond the Supply-Chain: RFID in the value Chain, SRIC-BI SCAN: D04-2462, SRI Consulting Business Intelligence, March 2004