Comments on an Improved RFID Security Protocol for ISO/IEC WD 29167-6

You Sung Kang, Dooho Choi, and Dong-Jo Park

With the rapid progress of RFID security technologies, the international standard group ISO/IEC JTC 1/SC 31 is developing a few security technologies for RFID systems. One of the initial proposals is ISO/IEC working draft (WD) 29167-6. Recently, Song and others stated that Protocol 1 of ISO/IEC WD 29167-6 is vulnerable to a malicious adversary. However, their analysis comes from a misunderstanding regarding a communication parameter called Handle. In this letter, we point out that an adversary cannot obtain any sensitive information from intervening in Protocol 1.

Keywords: RFID, authentication, RFID security.

I. Introduction

The use of RFID systems has become widespread in a range of applications. Much research on RFID security technology has been published in terms of software protocols and hardware design (see, for example, [1]-[3]). The international standard group ISO/IEC JTC 1/SC 31 is developing a few security technologies for RFID systems. One of the initial proposals is ISO/IEC working draft (WD) 29167-6.

ISO/IEC WD 29167-6 [4] describes security protocols and cryptographic operations as applicable for the ISO/IEC 18000-6 standard. ISO/IEC 18000-6 [5] defines parameters for air interface communications at an ultra-high frequency (UHF) band such as 860 MHz to 960 MHz. In particular, Type C of ISO/IEC 18000-6 is based on the EPCglobal UHF Generation-2 specification [6], which is a representative passive RFID technology. In 2011, ISO/IEC JTC 1/SC 31 withdrew the standardization activity for ISO/IEC WD 29167-6 and then requested new proposals for RFID security technology. At present, there are eight candidates that are in competition with each other. They each have one of the eight standard numbers ranging from ISO/IEC WD 29167-10 to ISO/IEC WD 29167-17. Among them, ISO/IEC WD 29167-14 [7] succeeds and includes Protocol 1 of ISO/IEC WD 29167-6 and main contents.

Recently, Song and others presented an analysis of the man-in-the-middle attack (hereafter, Song and others' analysis) against Protocol 1 of ISO/IEC WD 29167-6 [8]. However, Song and others' analysis comes from a misunderstanding regarding the role of *Handle*, a communication parameter. In this letter, we make clear the role of *Handle* on the basis of [4]. In addition, we disprove Song and others' claim that Protocol 1 is vulnerable to an adversary revealing sensitive data and injecting malicious data through an attack.

II. Review of Song and Others' Analysis

This section briefly reviews Song and others' analysis of Protocol 1. Figure 1 illustrates the operation procedures of Protocol 1. The operation procedures illustrated in Fig. 1, step (0) to step (13), are the same as those described in section II.B in [8]. To provide security services such as mutual authentication and data confidentiality, Protocol 1 assumes that a tag shares the same master key of 128 bits with a reader. They use the Advanced Encryption Standard (AES) algorithm to produce a session keystream. To generate the initial 128-bit session key, the AES engine takes a 128-bit initial vector as

Manuscript received Sept. 18, 2012; revised Oct. 23, 2012; accepted Oct. 30, 2012.

This work was supported by the IT R&D program of MKE/KEIT [Development of ultralight low-power RFID secure platform].

You Sung Kang (phone: +82 42 860 5960, youskang@etri.re.kr) is with the Software Research Laboratory, ETRI, Daejeon, Rep. of Korea, and also with the Department of Electrical Engineering, KAIST, Daejeon, Rep. of Korea.

Dooho Choi (corresponding author, dhchoi@etri.re.kr) is with the Software Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Dong-Jo Park (djpark@ee.kaist.ac.kr) is with the Department of Electrical Engineering, KAIST, Daejeon, Rep. of Korea.

http://dx.doi.org/10.4218/etrij.13.0212.0415

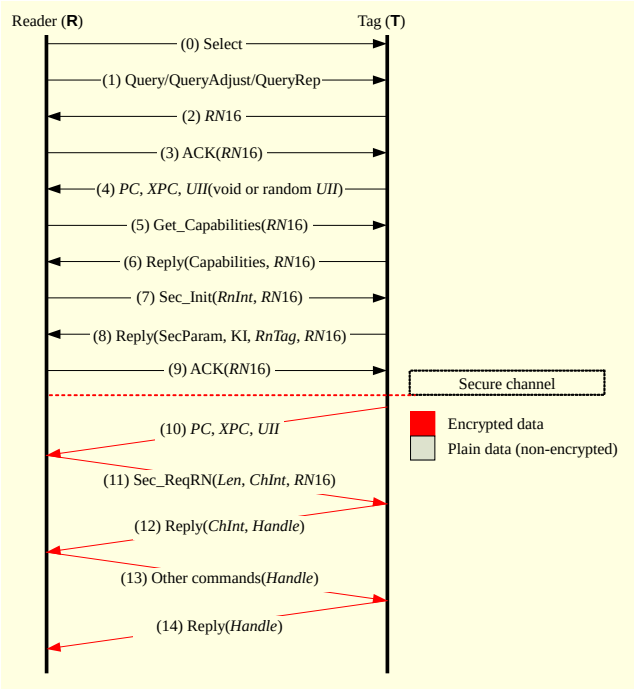

Fig. 1. Protocol 1: mutual authentication and secure communication in security mode.

input and the master key as key. Steps (7) and (8) are related to exchanging *RnInt* (a 64-bit random number of a reader) and *RnTag* (a 64-bit random number of a tag), which are combined into the 128-bit initial vector. For the next 128-bit session keystream in the same session, the AES engine takes the current session key as input, instead of the 128-bit initial vector. The encryption process operates in output feedback mode. That is, an exclusive-or (XOR) operation is performed between a plaintext and a session keystream in the same bit-length. After generating a session keystream, the encryption process is applied to all the payload data between the tag and the reader. In Fig. 1, the payload data after step (9) is the encrypted data with the session keystream.

According to Song and others' analysis, an adversary intercepts and replaces the transmitted data in steps (11) through (13). The adversary replaces a message field for the tag's *Handle* with a random string of the adversary in step (12). As a result of the intervention, a tag and a reader may fail to share *Handle* while they successfully authenticate each other. Refer to section III in [8] for the intervention scenario presented by Song and others.

III. Understanding of Handle

In the passive UHF RFID system, tags located within the communication range of a reader can receive all access commands from the reader. According to [6], *Handle* is generated by a tag and backscattered to a reader. The reader then uses *Handle* in subsequent commands and the tag uses *Handle* in subsequent replies. The value of *Handle* is fixed for the entire duration of a tag access operation. Tags check whether the received *Handle* is the same as the *Handle* backscattered by them, and only a tag with the same *Handle* executes the access command. The other tags ignore the command and do not reply to the command. That is, the role of *Handle* is similar to a session ID between a tag and a reader. In addition, [6] describes that a reader shall not use *Handle* for cover-coding purposes. The cover-coding defined in [6] is a bit-wise XOR between a password and a message to generate a 16-bit ciphertext. It implies that *Handle* must not be used as a secret key. In other words, *Handle* is not a security parameter, but a kind of session ID indicating a specified tag.

The reason why *Handle* is XORed with a session key in Protocol 1 is for implementation convenience in the physical layer. Once a tag and a reader establish a session key, they apply XOR to all of the input/output payload messages including *Handle*. From a tag's perspective, it can recognize *Handle* after XORing a payload message, so it has no difficulty communicating with a reader. On the other hand, it is more complex for a tag to partially apply XOR to payload messages because it must parse each field of input/output payload messages. According to [4], a tag does not need to check the length of each field at the physical layer. If *Handle* is excluded from XOR operation even after establishing a security channel, a tag must check the length of each field to find the position of *Handle*. The design idea of [4] makes the physical layer simple to implement. XORing *Handle* with a session key has nothing to do with the security effect.

IV. Comment on Effects of Song and Others' Analysis

In this section, we review Song and others' analysis in terms of the attack effect. In [8], Song and others stated that the mutual authentication between a reader (hereafter, **R**) and a tag (hereafter, **T**) finishes successfully, but, in fact, they fail to share the same *Handle*. It is a misunderstanding to conclude that *Handle* contributes to the mutual authentication of **R** and **T**, as *Handle* has nothing to do with the authentication function. In fact, the data contributing to a mutual authentication is *RN*16 and *ChInt* at step (11) and step (12), respectively (see section II.B in [8] for more details). According to Song and others' analysis, an adversary (hereafter, **A**) can intercept and replace the air interface messages and intervene in tag authentication. However, after intervening in Protocol 1, **A** cannot send any data independently of a legitimate reader because it does not know the session key. For the same reason, **A** cannot reveal any sensitive information. Furthermore, Song and others'

analysis is not an authentication of a third party because **A**'s intervention is performed only if the legitimate tag exists in the authentication procedure.

For example, assume that **A** intervenes in communication in the supply chain management using passive RFID tags. A legitimate reader can authenticate legitimate tags and conceal the sensitive data even though Song and others' analysis is applied to the process. On the other hand, **A** neither can forge another legitimate tag for itself nor obtain any information from intercepting. As a result, Song and others' analysis is not a security threat in terms of attack effect.

V. Conclusion

We analyzed the attack effect of Song and others' analysis on Protocol 1 of ISO/IEC WD 29167-6. Our analysis shows that Song and others' analysis is not a security threat in terms of attack effect. We also explained that *Handle* is not a security parameter, but a kind of session ID. We hope that our analysis and explanation help the RFID industry make a better decision for the security technology.

References

[1] D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," *Proc. ACM-CCS*, 2004, pp. 210-219.

[2] H. Sun and W. Ting, "A Gen2-Based RFID Authentication Protocol for Security and Privacy," *IEEE Trans. Mobile Computing*, vol. 8, no. 8, Aug. 2009, pp. 1052-1062.

[3] H.-B. Kang et al., "High Security FeRAM-Based EPC C1G2 UHF (860 MHz-960 MHz) Passive RFID Tag Chip," *ETRI J.*, vol. 30, no. 6, Dec. 2008, pp. 826-832.

[4] ISO/IEC WD 29167-6, *Information Technology – Automatic Identification and Data Capture Techniques – Part 6: Air Interface for Security Services and File Management for RFID at 860-960 MHz*, International Organization for Standardization, Aug. 2010.

[5] ISO/IEC 18000-6, *Information technology – Radio Frequency Identification for Item Management – Part 6: Parameters for Air Interface Communication at 860 MHz to 960 MHz*, 2nd ed., International Organization for Standardization, Dec. 2010.

[6] EPCglobal Specification for RFID Air Interface, *Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, Version 1.0.9*, GS1 EPCglobal, Jan. 2005.

[7] ISO/IEC WD 29167-14, *Information Technology – Automatic Identification and Data Capture Techniques – Part 14: Air Interface for Security Services Crypto Suite AES-OFB*, International Organization for Standardization, Oct. 2011.

[8] B. Song, J.Y. Hwang, and K.-A. Shim, "Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6," *IEEE Commun. Lett.*, vol. 15, no. 12, Dec. 2011, pp. 1375-1377.