Cryptanalysis of ultralightweight RFID authentication protocol

Umar Mujahid, M.Najam-ul-islam, Jameel Ahmed, Usman Mujahid

Radio frequency identification (RFID) technology is one of the most emerging technologies in the field of pervasive systems, which provides the automatic identification of the object with non-line of sight capability. RFID is much better than its contending identification scheme (Bar code) in terms of efficiency and functional haste. Although it offers many advantages over other identification schemes but there are also allied security apprehensions, so to make the system secure in a cost effective manner we use ultralightweight authentication protocols. In this letter, a desynchornization attack has been presented on recently published ultralightweight authentication protocol RAPP (RFID authentication protocol with permutation). Then an advanced version of RAPP has also been proposed to combat against the desynchronization attack.

Introduction: Radio frequency identification (RFID) is becoming very eminent identification scheme because of its enriched features and low cost. But their extensive deployment also sustains some security risks and practical attacks on the system. As the tag transmits its identity to reader on wireless channel, which is open for all malicious adversaries, so they can easily perform various attacks such as passive or active attacks, cloning and tracking etc. An effective and supple approach to assure the privacy and security is to adopt authentication protocols. To make the system cost effective, several lightweight and ultralightweight authentication protocols have already been proposed.

P. Peris-Lopez, J. C. Hernandez-Castro et.al [5],[6] proposed LMAP (Lightweight mutual authentication protocol) and EMAP (An efficient mutual authentication protocol) for low cost RFID tags, where only 250-300 logic gates have been devoted for the security-related errands. The protocol was divided into four steps: tag identification, mutual identification, pseudonym updating and key updating. But Tieyan Li and Guilin Wang [7] analysed the security vulnerabilities in LMAP and EMAP. They have also identified two effective attacks namely, desynchronization and full disclosure attacks against LMAP. First attack broke the synchronization between reader and tag while the second attack disclosed all the secrets stored on a tag. Then Hung-Yu Chien, [3] proposed a new ultralightweight RFID authentication protocol that provides strong authentication and strong integrity (SASI) protection of its transmission and of updated data. A new function ROT(X, Y) had been incorporated in the protocol for overall security enhancement of the system. But in 2011, Hung-Min Sun, Wei-Chih Ting [4] performed cryptanalysis of SASI protocol and found two desynchronization attacks to break the protocol. Then in 2012, Yun Tian, Gongliang chen et.al [1] proposed a new ultralightweight RFID authentication protocol with permutation (RAPP). In RAPP, tag involves only three operations: bitwise XOR, left rotation and permutation. The presence of the effective operations in the protocol made the computational complexity and cost of the tags low.

In this letter, a cryptanalysis of RAPP has been performed; a desynchronization attack [2] has been presented first and then a novel solution has been proposed to combat against this desynchronized attack.

RAPP Scheme: RAPP involves three characters: Tag, reader and backend database. In RAPP, the channel between reader and backend database was assumed to be secure since both reader and backend database can use general cryptographic algorithms or may be connected via optical fiber. But on the other hand, the channel between the tag and reader is wireless and susceptible to possible attacks. Each tag has an L-bit unique secret identifier ID, and other four elements {IDS, K_1, K_2, K_3}. These four elements will be updated after completion of the protocol by using following set of equations:

$$IDS^{new} = Per(IDS^{old}, n_1 \oplus n_2) \oplus K_1^{old} \oplus K_2^{old} \oplus K_3^{old}$$

$$K_1^{new} = Per(K_1^{old}, n_1) \oplus K_2^{old}$$

$$K_2^{new} = Per(K_2^{old}, n_2) \oplus K_1^{old}$$

$$K_3^{new} = Per(K_3^{old}, n_1 \oplus n_2) \oplus IDS^{old}$$

Here permutation operation has been used in all equations, which can be computed as follows:

Let X=1010011 & Y=0101101

Per (X, Y) =0001111

The permutation can be computed by considering the two pointers P_1 and P_2 as index values for their corresponding strings of X and Y. In our example, first entry in string Y is 0 so, first entry of the string X has been moved to the last position in the third string. Now, as second entry of string Y is 1 so, put the second entry at the first place of the third string. The process will be repeated till the last entry of both X and Y strings. RAPP contains three rounds: tag identification, mutual authentication and pseudonym pupation. Firstly, reader transmits a 'Hello' message to tag and tag will reply with its IDS. Now, reader will lookup this IDS in the backend database, if IDS matches with the entry of the database then reader will transmit A and B messages comprises of random number 'n_1'towards tag (If IDS didn't match with the database entry, then reader will ask tag to send its old IDS and compare this IDS^{old} with its entry). The tag can deduce the random number 'n_1' through message A, and make sure whether the reader is endorsed by confirming the precision of message B:

$$A = Per(K_2, K_1) \oplus n_1 \quad (1)$$

$$B = Per(K_1 \oplus K_2, Rot(n_1, n_1) \oplus Per(n_1, K_1) \quad (2)$$

Then in the next step if the tag found the reader a valid one, it will send a message 'C' towards reader. After receiving message 'C' the reader will compare it with the local 'C' to authenticate the tag:

$$C = Per(n_1 \oplus K_1, n_1 \oplus K_3) \oplus ID \quad (3)$$

If the reader found the tag a valid one, it will generate another random number n_2, and conceal this random number in the message 'D'. The reader will compute and send message (D and E) to tag. The tag will deduce the random number n_2 from 'D' and make sure that n_2 is not being tampered by checking the precision of message 'E':

$$D = Per(K_3, K_2) \oplus n_2 \quad (4)$$

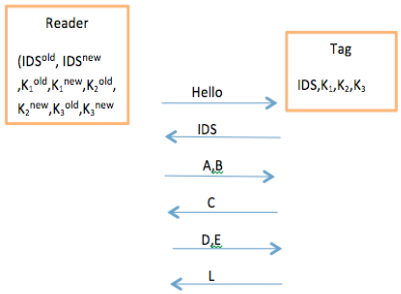
$$E = Per(K_3, Rot(n_2, n_2)) \oplus Per(n_1, K_3 \oplus K_2) \quad (5)$$

After authenticating successfully, the reader and tag will update their pseudonyms as discussed earlier.

Desynchronization attack on RAPP: In this attack, foe (*f*) will break the synchronization of tag and reader by misleading both tag and reader to update their communal values to different values. In the first step foe, *f* will eavesdrop the normal RAPP protocol session between the tag and reader. The *f* will store these exchanged messages (IDS, A, B and C) and will block D and E messages to prevent the tag from updating its pseudonyms. But reader will update its pseudonyms as reader already got the C message from the tag. Now, foe will wait until an authentic reader initiates a new protocol session with this tag. In this session reader sends $A^{\wedge} = Per(K_2, K_1) \oplus n_1^{\wedge}$ and $B^{\wedge} = Per(K_1 \oplus K_2, Rot(n_1^{\wedge}, n_1^{\wedge}) \oplus Per(n_1^{\wedge}, K_1)$ to tag. In return tag will send $C^{\wedge} = Per(n_1^{\wedge} \oplus K_1, n_1^{\wedge} \oplus K_3) \oplus ID$ towards reader. The reader will send $D^{\wedge} = Per(K_3, K_2) \oplus n_2^{\wedge}$ and $E^{\wedge} = Per(K_3, Rot(n_2^{\wedge}, n_2^{\wedge})) \oplus Per(n_1^{\wedge}, K_3 \oplus K_2)$ but again *f* will block $D^{\wedge}$ and $E^{\wedge}$ so, that the tag may not be able to update its pseudonyms. Here $n_1^{\wedge}$ and $n_2^{\wedge}$ are two random numbers which are different from n_1 and n_2.

Finally '*f* 'will send the Hello message to tag by impersonating as a valid reader. Tag will transmit its IDS towards reader (*f*) and *f* will then replay the previously captured message (A&B). Tag will extract $n_1$from A, verify B and send C to reader (i.e. *f*). Reader will then again replay the captured messages D and E towards tag. Tag will then update its pseudonyms according to n_1 and n_2. Now, if the legitimate reader starts its protocol with the victimized tag, it will not authenticate the valid tag because of different stored values of pseudonyms.

Modified RAPP: The proposed modified version of RFID authentication protocol with permutation (RAPP) will combat against the Desynchronization attack by adding a acknowledgement message from the tag. The modified RAPP is as follows:



$A= Per (K_2, K_1) \oplus n_1$; $B=Per (K_1 \oplus K_2, Rot (n_1, n1)) \oplus Per (n_1, K1)$; $C=Per (n_1 \oplus K_1, n_1 \oplus K_3) \oplus ID$

$D=Per (K_3, K_2) \oplus n_2$; $E=Per (K_3, Rot (n_2, n2)) \oplus Per (n_1, K_3 \oplus K_2)$;

$L=Per (n_1 \oplus n_2, Rot (n_2, n1)) \oplus ID^*$

Fig. 1 Advanced RAPP

In advanced RAPP, the basic operation of the mutual authentication is same as in RAPP, but a new 'L' message has been assimilated in the protocol for acknowledgement purpose. The "L" message will inform the reader that tag has successfully updated its pseudonyms. If reader didn't receive "L" message from tag, then it will go to step one and send the hello message again to the same tag, which will reply with its IDS. Reader will compare this IDS with IDS^{old} of the same tag, if entries didn't coincide then reader will not update its pseudonyms, as desynchronization attack has been hurled between the tag and reader. So, desynchronization attack will not affect the Advanced RAPP ultralightweight protocol.

Conclusion:

In this letter, a Desynchronization attack on RAPP, a new ultralightweight authentication protocol has been presented. Then advanced version of RAPP has been proposed, which comprises of an acknowledgment methodology to combat against Desynchronization attack.

Authors: Umar Mujahid[1,2], Muhammad Najam-ul-islam[1], Jameel Ahmed[2], Usman Mujahid[3]
Bahria University, Islamabad[1], HITEC University, Taxila[2], Air University, Islamabad[3]

References:

[1] Yun Tian, Gongliang chen et.al," A new ultralightweight RFID Authentication protocol with permutation" IEEE Communication Letters, Vol. 16.No, 5,May 2012

[2] Nasour Bagheri, Masoumeh Safkhani et.al, " Cryptanalysis of RAPP, an RFID Authentication Protocol" Cryptology ePrint Archive: Report 2012/702

[3] Hung-Yu Chien," SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity" IEEE Transactions on dependable and secure computing, vol 4, no. 4, October-December-2007

[4] Hung-Min Sun, Wei-Chih Ting et.al," On the Security of Chien's Ultralightweight RFID Authentication Protocol" IEEE Transactions on dependable and secure computing, vol. 8, no. 2, March-April 2011

[5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and A. Ribagorda, "LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags," in Proc. 2006 Workshop RFID Security.

[6] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro," EMAP: An Efficient Mutual-Authentication Protocol for Low-cost RFID Tags" Springer Link, Volume 4277, 2006, pp 352-36.

[7] Tieyan Li and Guilin Wang," Security Analysis of family of Ultra-Lightweight RFID Authentication Protocols", Journal of Software, Vol. 3, No. 3, MARCH 2008.