SECURE MUTUAL AUTHENTICATION PROTOCOL VIA RFID SYSTEM

Mr. Rajan Bhalani[1], Assit. Prof. Mr. Mohit Patel[2]
[1]Student, Swaminarayan College of Engineering & Technology, Kalol

ABSTRACT: ***The blueprint of ultra-lightweight authentication protocols is very important to the pervasive deployment of low-cost RFIDs. This paper examines the security of a new ultra-lightweight RFID authentication protocols SASI. SASI, a newly recommended ultra-lightweight RFID protocol with enhanced used security than earlier implemented protocols i.e. LMAP, M2AP, and EMAP [10, 7, 3]. A proposed idea is given for its improvements. Since RFID tags are pervasive and at times even insensible to the human user, all modern RFID protocols are planned to battle tracking so that the position confidentiality of the human RFID user is not dishonored. An additional design measure for RFIDs is the squat computational attempt essential for tags, in view that the majority of tags are passive devices that originate power from an RFID reader's transmitted signals. Along this element, a class of ultra lightweight RFID authentication protocols have been planned that use only the most basic bitwise and arithmetic procedures like OR, XOR, addition, simple rotation, bit rotation etc. The rest of paper is organized as follows. In section 2 a brief introduction to the technology is presented. In section 3 we have analyzed some RFID protocol and SASI is discussed in detail. Existing problem is discussed in next section. Our proposed idea is explained in section 5. Steps in our algorithm along with complexity are given in section 6. Finally we conclude in section 7, along with future directions.***

Keywords: RFID, IDS, SASI, XOR, HASH, TAG, DB, L2MAP

I. INTRODUCTION & CONCEPTS

An authentication protocol enables a sender to throw messages to a receiver through an unsafe and unprotected communication station in such a way that the receiver can be persuaded that the messages are without a doubt coming from the intended sender and the messages have not been changed or modified by any intruder or adversary meeting in the center of the communication station. Radio Frequency Identification is an elegant and sophisticated, yet modest and highly unfailing technology that uses radio waves to individually recognize an individual, or an article and object without any physical contact with the same. There are two apparatuses to any RFID system: a transponder frequently called a "tag", & an interrogator that is called a "reader". Tags are typically attached to the objects or items. Each tag carries a sole identification number (serial), which is planned and programmed at the time of manufacturing and engineering process to guarantee that the article carries a distinguishing uniqueness and description. Normally, when the tag passes through or senses a radio signal from the reader, the tag recognizes itself to the reader. RFID tags are very trivial and tiny microchips involving of a small processor, a little bit memory, radio transmitter and an antenna coil. The size of memory and processing powers differs from a few characters or bytes to some kilobytes. The tag's data is communicated and transmitted to the reader as a unique radio frequency through the antenna coil [18, 19, 20]. Their use has become more common in daily life especially in vehicular toll payment systems on highways and motorways. The technology needs to be more secure.

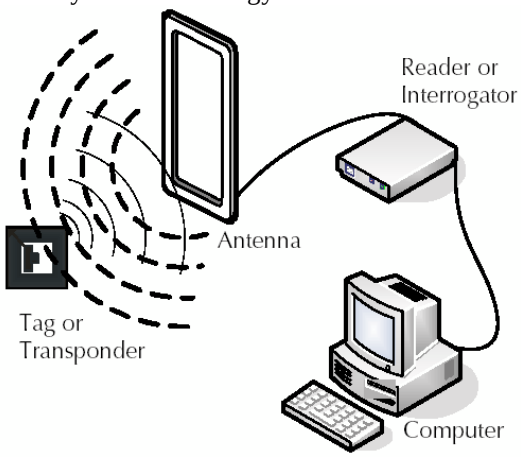


Fig 2.1: Working diagram of an RFID System

II. RELATED WORK & EXISTING PROTOCOLS:

The RFID authentication protocol encompasses three entities- a tag, a reader and a backend server. The frequency or station between the reader and the backend server is expected to be protected and safe, but the frequency between the tag and the reader is vulnerable to all the imaginable and probable attacks. During the authentication phase, the reader attempts to authenticate the tag through the support of the backend server, where the server preserves a top- secret database of tag-related information and data.

LMAP and M2AP include only simple and modest bitwise operations like bitwise AND, bitwise XOR, bitwise OR, and addition modulus

2 (+). The random number generator is solitary required and essentials on the reader side. We will only describe SASI because LMAP & M2AP both are same to SASI. SASI is a very fresh ultra-lightweight RFID protocol, planned and claimed to be more secure and safe than previous such classes of protocols.

Since the communication and transmission between the reader and the backend server is expected to be protected, SASI considers the reader and server as one object. Each tag

Tj has a 96-bit static identification number IDj and for a specific session i pre-shares with the reader a 96- bit pseudonym IDSi and two top-secret keys Key1i, Key2i both of 96 bits. Each tag retains and maintains two entries, every of the form (IDSi,Key1i,Key2i), where one corresponds to old information used in the most fresh completed protocol conference, while the other corresponds to the stored values or information that are to be used in the succeeding protocol session.
A tag is not likely to accomplish any computations except for straightforward and basic bitwise logical or arithmetic procedures like XOR, simple OR, subtraction (-), addition (+), and bit rotation (<<). The SASI protocol comprises of the

- Tag identification phase,
- Mutual authentication phase and
- Updating phase.

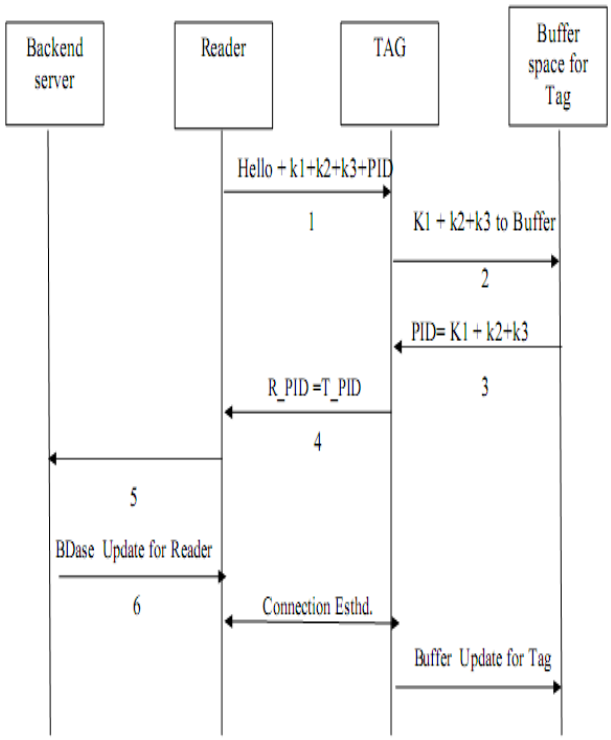
TAG IDENTIFICATION:

1. The reader R directs a hello message to the tag T
2. T sets the alias IDS to the value of IDS next from its database. It also sets Key1 and Key2 to correspondingly the values of K1next and K2next. It then directs IDS to reader R.
3. R checks if there exists an entry IDSi in its database that equals the received IDS. If no match occurs, it resends the hello message to tag T and delays for an IDS message.
4. On receiving a 2nd hello message, tag T now sets the alias IDS to the value of IDSold from its local database, and consistently Key1 and Key2, both keys are set equal to Key1old and Key2old (keys used in previous session) respectively.
5. Once reader R finds an entry IDSi in its database that is equal to the expected IDS value, it continues to the next steps with IDSi and equivalent Key1i, Key2i from the local record entry.

MUTUAL AUTHENTICATION:
1. Reader R arbitrarily produces two random numbers i.e. n1, n2, and continues to calculate the values A, B,
Key1 ˆ, Key2 ˆ, C, involving OR, XOR, bit rotation and addition.
2. The concatenation of A||B||C is then directed to tag T.
3. Tag T computes the random numbers n1, n2 and values Key1 ˆ, Key2 ˆ from the acknowledged concatenation statement i.e. A||B||C. It then computes C ˆ from the values of Key1, Key2, Key1 ˆand Key2 ˆ through the OR, XOR and simple addition procedures, as shown in figure 3.1.
4. If the computed C ˆ equals the received C, then tag T calculates D using OR, XOR, and addition (+) procedures and functions.
5. This calculated D is directed to reader R, and tag T now continues to the next Updating period or stage.
6. Reader R computes D ˆ and checks if it
matches the received D. If so, reader R continues to the next and final Updating stage.

UPDATING:
1. Reader R modernizes and updates its database entry for (IDSi, Key1i, Key2i), while tag T updates its database entry for(IDSold,Key1old, Key2old), (IDSnext, Key1next, Key2next). The whole scenario is shown in Fig 3.1 below.

Fig 3.1: Working diagram of SASI Protocol [3, 5]



At the finishing point of the protocol, both the reader R and the tag T have successfully and positively authenticated each other, and additionally have updated their stored database entries in groundwork for the next & subsequent protocol session. Since these updates are functions of the recently computed and exchanged Key1 ˆ, Key2 ˆ, and they have confirmed the received C, D against their own calculated C ˆ, D ˆ which are functions of Key1 ˆ, Key2 ˆ, then both the reader R and tag T are also guaranteed that they have the same Key1 ˆ, Key2 values and are in synchrony, thus avoiding and preventing de-synchronization attacks.

III. EXISTING PROBLEM IN SASI:

Since RFID tags are transportable and very small, attached to diverse objects and are often oblivious to the human user, confidentiality is a major fear in the strategy, design and usage of RFIDs. Definitely, these tags are ordinarily embedded in personal devices carried around an individual wherever he is, e.g. credit cards, e- passports, personal digital assistants (PDAs), BREW devices & Bluetooth devices etc. “So an RFID tag can be traced, it means the human user’s whereabouts can be tracked. It can subsequently be claimed that one of the important and vital human rights of an individual is that his position or actions and activities should not be perceptible”. Thus, designers of RFID protocols want to guarantee that RFID tags cannot be followed and traced, so that location

secrecy of the human RFID user can be safeguarded and protected Raphael C.-W. Phan, Member, IEEE have statistically proved in his article that SASI can not attain intractability even under a passive attack. The flaw he abuse is that the public messages i.e. C and D are each a function of the same unknown secret keys Key1, Key2, Key1 ˆ, Key2 ˆ, and the static identifier ID is only contained in D; thus by further exploiting the bit interaction between the operators, OR and XOR. & XOR and canceling out the secrets Key1, Key2, Key1 ˆ, Key2 ˆ, he showed that C and D in combination outflows at least one bit of information about the static identifier ID of a tag. intractability grounded on the statement that the pseudonym IDS is updated every session as a function of random numbers, and hence any two pseudonyms are probable to look arbitrary and thus be unlikable." The problem is

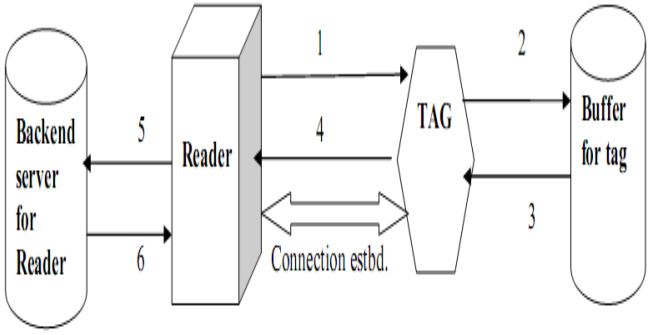


Fig 5.1: Proposed Solution

discussed in this paper but still no efficient and precise solution is proposed.

IV. PROPOSED SOLUTION

After a deep study of different lightweight RFID authentication protocols, we conclude that previou lightweight RFID authentication protocols i.e. LMAP, M2AP & EMAP are not traceable but they are not so much secure. So our idea for improvement is to combine these lightweight RFID authentication protocols. In SASI the server maintains a separate secret database for the secret keys & a separate database for the unique key of the tag. SASI is costly in database maintenance on server side. Moreover server's maintenance and scalability are ignored in the given paper. To make it more efficient hash functions are to be implemented on tag side. Although hashing requires strong mathematical calculation but combined with simple operations as is SASI, it works fine. Implementation of hashing limprove bandwidth capacity as server will not keep the secret key database for the tags, and hence there is no requirement of exhaustive search operations. Furthermore if server/reader replies are kept only for short time security may be improved i.e. traceability in the since that older information are unavailable to try. To achieve this goal system current date is XORed with the key, and then a hash function is applied at server side. After sending the request the same hash is applied to extract the secret key, as explained below. This is only an enhanced proposed idea, still required a lot of study of different lightweight RFID authentication protocols. Our future work is to do some mathematical calculations and will propose a new lightweight RFID authentication protocol.

V. ALGORTHM & PROTOCOL

Our proposed algorithm executes faster due to hashing because hashing requires low processor speed. The flow diagram of our proposed scheme is given in Fig 6.1

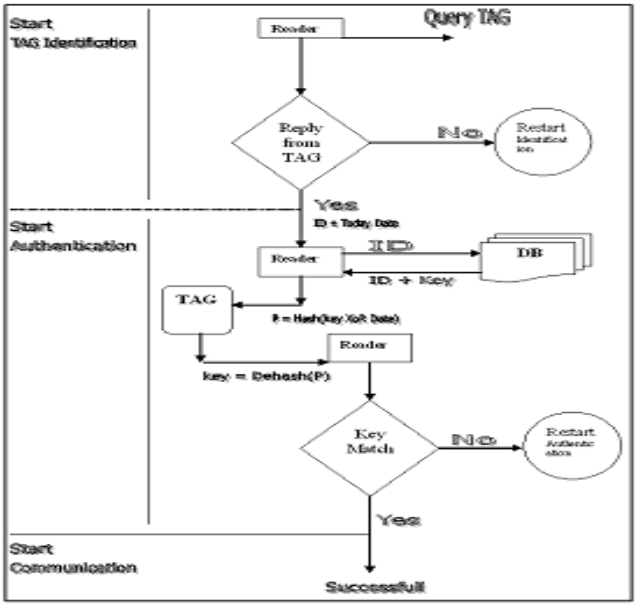


Fig 6.1: Flow diagram

The date variable will make the system more secure as it will help in washing out of old information after some specific duration. The problem with the tag is that it is having very low speed processor and only a few bits of memory. It will take much time in computing bit rotation, XoR, OR, concatenation and dealing with random numbers. The running time of our proposed algorithm and protocol is the sum of running times of all statements and function. We can calculate its complexity and can easily conclude that the algorithm runs in linear time i.e. O(n2)

$$T(n) = C_1 n + C_2 + C_3 \sum t_k + C_4 + C_5$$

Using equation $\sum_{j=2}^{n} j = \frac{n(n+1)}{2} - 1$ we can calculate

$T(n) = a(n) + b$ in best case while

$T(n) = a(n^2) + b(n) + c$ in worst case. If the database is not so large then we can achieve our goal in linear time. So it is unlikely that a worst case will occur and will result in quadratic running time. The cost C_2, C_3 and C_5 are constant times that are negligible in hashing. In case if the ID was matched in 1st try then C_3 will be zero and hence total running time will be O(n). In worst case the algorithms runs in $a(x^2) + b(x) + c$ i.e. quadratic running time. The solution to quadratic running time is $O(n^2)$.

VI. CONCLUSION & FUTURE WORK

In general terms, RFID is a means of recognizing an individual or entity using a radio frequency transmission. The technology and knowledge can be used to recognize, track, sort or sse a wide variety of things. Communication takes place between a reader (interrogator) and a transponder (Silicon Chip connected to an antenna) frequently called a tag. Tags can either be active (if powered by own battery) or passive (when powered by the reader field or signals). The attack on SASI is a passive one. Passive attacks are achievable in practice since they only necessitate only eavesdropping, which is a typical hazard or threat in RFID setting where physical wireless communication station or channel is open to parties within communication and transmission. Excitingly, the earlier ultra-lightweight RFID protocols like LMAP, M2AP and EMAP by Peris-Lopez et al, do not parade and show the above mentioned properties that he exploited for his attack on SASI. The chief motive and reason is "because any and planned with healthier security should not necessarily be taken for granted to be more safe, protected and secure than older versions, but even against attacks considered by both old and new designs, e.g. in this case, intractability. Our future work is to do some mathematical calculations and will propose a new lightweight RFID authentication protocol.

REFERENCES

[1] Journal of Software, Vol. 3, No. 3, Academy Publisher, pp. 1-10,

[2] O'Connor, Mary, "Philips Demos Polymer HF Tags.", RFID Journal. 1, 52 (2006)

[3] Karl Hanser Verlag, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification", 2003

[4] Sample, A.P.; Yeager, D.J.; Powledge, P.S.; Mamishev, A.V.; Smith, J.R, "Design of an RFID Based Battery Free Programmable Sensing Platform", IEEE Transactions on Instrumentation and Measurement , vol.57, no.11, pp.2608"2615, Nov. 2008

[5] E. Kosta, M. Meints, M. Hensen and M. Gasson, "An Analysis of Security and Privacy Issues Relating to RFID Enabled ePassports," Proceedings of IFIP-SEC'07, IFIP International Federation for Information Processing, Vol. 232, Springer Boston, pp. 467-472, 2007.

[6] T. Li, G. Wang and R.H. Deng, "Security Analysis on a Family of Ultra-Lightweight RFID Authentication Protocols,"

[7] R.I. Paise and S. Vaudenay, "Mutual Authentication in RFID," Proceedings of AsiaCCS '08, ACM, pp. 292-299, 2008.

[8] S. Vaudenay, "RFID Privacy based on Public-Key Cryptography," Proceedings of ICISC '06, LNCS 4296, Springer, pp. 1–6, 2006.

[9] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[10] Harald Vogt, "Efficient Object Identification with Passive RFID Tags", Springer-Verlag Berlin Heidelberg 2002

[11] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "RFID PRIVACY ISSUES AND TECHNICAL CHALLENGES", September 2005/Vol. 48, No. 9 COMMUNICATIONS OF THE ACM

[12] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels, "RFID Systems and Security and Privacy Implications", Springer-Verlag Berlin Heidelberg 2003

