International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

Provably Lightweight Rfid Mutual Authentication Protocol

N.Swetha

ABSTARCT:

Simplest-Lightweight Authentication Protocol (SLAP) is one of the modern mutual authentication protocols for light-weight RFID environment. However, server impersonation attack may be launched at the aforementioned protocol. The essential motive of this paper is to comprehensively verify the safety susceptible factor of SLAP. This paper additionally proposes an alternative mutual authentication protocol which set up to be cozy and available for mild-weight RFID environment. The proposed protocol is examined by a security protocol verifier, AVISPA, and benchmarked in opposition to the particular SLAP. The results show that the proposed protocol has the comparable functionality with SLAP in stopping appeared assaults and concurrently receives rid of the stated security weakness on SLAP.

INTRODUCTION:

Radio-frequency identification (RFID) is a Wi-Fi verbal exchange used to interchange statistics the usage of radio wave. A regular RFID gadget accommodates of one or greater readers that have the potential to communicate within slim tiers with many tags [1], [2] as shown in Figure 1. An RFID tag may be related on numerous entities together with product, character, or animal for the motive of identity. The primary benefit of using RFID is that a few tags may be observed from several meters away and even past the road of sight of the reader. RFID has advanced in numerous new paperwork and programs. For instance, the battery powered active RFID gadgets have been used for automatic toll series on motorways due to the fact the early 80s. In addition, RFID tags are really may be packed into a totally reasonably-priced and small form appropriate for software program on single-product packages because of the technological advances in miniaturization. Hence, maximum of the cutting-edge successful hypermarkets are the usage of the RFID machine and tags to permit consistent with object monitoring of goods from the manufacturer to the give up-man or woman [3].Nevertheless, like some different conversation structures, RFID systems are

prone to certainly one of a kind form of assaults such as eavesdropping, replay attack, man-in-the-center attack, and denial of service (Do's) attack. Besides, the information obtained from a valid tag may be without issues used to impersonate the tag. As an effect, the reader will now not capable of verify whether or not it communicates with a legitimate or fake tag [4]. This form of attack is known as impersonation assault it really is preventable by manner of appealing a relaxed authentication mechanism. In 2004, Ohkubo et al. [5] proposed an RFID protocol based totally on hash-chains to prevent eavesdropping. However, this protocol is prone to replay attacks which can be installation after unsuccessful authentication. Henrico et al. [6] proposed an easy scheme counting on one way hash-capabilities primarily based totally on Ohkubo et al. [5] scheme to prevent the eavesdropping, message interception, spoofing, and replay assaults. Unfortunately, this protocol is liable to the tracing assault. In 2005, Demetrious [7] supplied a protocol that gives comfy and authenticated tag reader transactions to save you in opposition to trendy attacks in conjunction with impersonation, replay, and cloning. However, this protocol is vulnerable to the tracing assault for the cause that tag ID remains regular in some unspecified time in the future of the identification session of the tag. Alternatively, Lou et al. [8] proposed any other RFID scheme based mostly on Ohkubo et al. [5]. The electricity of the Lou's protocol is that encrypted information site visitors are supported the various parties without the use of cryptographic ciphering algorithms but, Lou's protocol is susceptible in opposition to replay assault. In 2008, Gaskell et al. [9] proposed a light-weight RFID mutual authentication protocol called Simplest-Lightweight Authentication Protocol (SLAP). The protocol can face up to well-known assaults and does no longer demand complex computational approaches. Compared to the previous protocols, SLAP is considered because the maximum secure RFID authentication protocol it is appropriate for light-weight RFID environment. However, as demonstrated via the use of Amgun and C¸ agleam [10], server impersonation assault can be completed closer to SLAP. The demonstration indicates the opportunity of impersonation attacks which breaks the synchronization between the server and the tag while not having to understand the inner

state of the tag. In addressing the problem, Amgun and C¸ agleam [10] has proposed a revised SLAP which nearly just like the specific paintings through clearly reordering the content material of the authentication message (from server to tag). Notwithstanding a completely compact implementation, either SLAP or revised SLAP reveals partial of the name of the game (based on the range of tag to be had within the machine) to help the server in locating the corresponding thriller. Such an attempt can pave a way for an attacker to lay to the tag to expose components of the secret, at most its first area [9]. Although it's far hard to perform, revealing at this issue may want to supply better possibility on one of kind threats inclusive of sample analysis and brute-pressure (guessing) to infer the entire mystery. For that purpose, an opportunity mutual authentication protocol, similarly referred to as PLAP, is proposed which particularly keeps the confidentiality of the name of the sport.

Figure 1: RFID system

PROVABLY LIGHTWEIGHT AUTHENTICATION PROTOCOL (PLAP)

PLAP is first of all designed to conquer safety weaknesses of SLAP, primarily appearing authentication without revealing any part of the name of the game and on the equal time capable to save you the server impersonation attack which causes de-synchronization among the tag and the server as addressed in revised SLAP [10]. PLAP makes use of hash characteristic, exclu sive OR (XOR) operation, and pseudorandom number generator (PRNG) in acting the authentication. Figure 2 illustrates the overall authentication steps in PLAP. PLAP includes two levels, which can be the initialization phase and the authentication section as defined in the following subsections

RELATED WORK:

The early tries of ultralightweight cryptography seemed inside the Ultralightweight Mutual Authentication Protocol (UMAP) circle of relatives. It consisted of the Lightweight Mutual Authentication Protocol (LMAP) [3], Minimalist Mutual- Authentication Protocol (M2AP) [4], and the Efficient t Mutual Authentication Protocol (EMAP) [5]. The principal operations in those protocols are the XOR, AND, OR and addition. These protocols have been validated to be liable to desynchronization and full disclosure assaults [6–11]. The Strong Authentication and Strong Integrity (SASI) protocol [12] was proposed as an opportunity to triumph over those weaknesses. It added the rotation operation to the bitwise operations used inside the UMAP family. The protocol emerge as investigated very well and severa papers gave positive attacks that led to de-synchronization [13-14]. More importantly, a full disclosure attack with excessive chance of fulfillment through eavesdropping on 217 protocol runs became furnished in [15]. A positive evaluation of SASI in [16] supplied the desynchronization, ID disclosure, and full mystery values disclosure assaults. The Gossamer protocol furnished improvements to overcome the vulnerabilities of its predecessors. It however become proven, however, that the de-synchronization trouble come to be no longer solved. Active assaults that would bring about desynchronization are positive in [17-18]. One protocol that received attention is the RFID authentication protocol with permutation (RAPP) [19]. This protocol extended the operations utilized in SASI via adding the permutation operation. The reason in the back of the permutation operation is to hide any bit relationships that cease end result from bitwise operation. Similar to its predecessors, diverse attacks seemed and confirmed its inherent weaknesses. Desynchronization assaults with an less expensive probability of success are given in [20-21]. Moreover, an in depth assessment in [22] gave the stairs to run a whole disclosure attack the use of 230 tag queries. This variety of queries changed into relatively decreased proper down to 192 tag queries in an stepped forward entire disclosure attack in [23]. A specific analysis of these preceding assaults is given in [24]. One latest protocol is the Succinct and Lightweight Authentication Protocol (SLAP) [25]. In this protocol, an ultralightweight operation, called conversion, is used as the idea for

cryptographic operations. The authors present an extensive security evaluation and declare that the protocol is proof towards de-synchronization, replay, and tracing assaults. SLAP modified into accompanied through using an high-quality more recent protocol called the pseudo-Kasami code based totally Mutual Authentication Protocol (KMAP) [26] that avoids the usage of smooth bitwise operations and, as a substitute, makes use of a primitive operation that complements the diffusion residences to make the secrets and techniques irreversible. In the analysis component, it's far claimed that the protocol resists all varieties of attacks. The art work in [27] furnished an evaluation of SLAP and KMAP and supplied a generalized case of a de-synchronization attack that applies to each protocols. The attack indicates that the de-synchronization attack continues to be viable regardless of the truth that the tag and the reader preserve copies of the vintage and new mystery values. As a general commentary, maximum of the protocols which might be based totally on lightweight operations have been shown to be susceptible to attacks because of the inherent weaknesses of their cryptographic operations. The paintings in [28] discusses the everyday mistakes that seem inside the layout of protocols and gives pointers to be observed in order to layout and evaluate the validity of mutual authentication protocols. Recently, Gao et al. [2] presented an analysis of the RAPP protocol and proven a de-synchronization attack with the useful resource of tampering with the exchanged message. As a option to the vulnerability, the authors proposed a brand new protocol referred to as LPCP. This protocol is a lightweight protocol (the authors name it approximate ultra-lightweight) that uses the CRC function together with the operations defined for the RAPP protocol. The authors demonstrated the protocol the usage of the Simple Promela Interpreter and claimed that the LPCP protocol provides confidentiality and is immune to desynchronization, tracing, replay, and full disclosure assaults. The paintings in [29] supplied a de-synchronization assault with the resource of impersonating a legitimate reader the use of eavesdropped messages from in advance durations. We in addition analyze the protocol and gift attacks with a fulfillment possibility same to one

CONCLUSIONS The low-cost RFID systems are some typical resourceconstraint devices and their computation and storage

resources are very finite. Therefore some lightweight authentication protocols are developed to satisfy the particular scenario of lowcost RFID systems. Our protocol uses CRC function, which is simpler and needs less computation and storage resources than Hash function, to encrypt all sessions transferred between tag and reader. This ensures the confidentiality and privacy of RFID systems. Meanwhile, our protocol utilizes pseudorandom numbers to randomize all session messages between reader and tag so as to ensure their freshness. The secret keys of last successful authentication are reserved in backend server so as to resist against de-synchronized attack. The secrecy of RFID systems is updated in time for assuring forward security. So our protocol can impede eavesdropping. It can effectively prevent tracing attack, replay attack, and de-synchronized attack. It only uses pseudorandom number generator and CRC function. CRC function is simple and it consumes less computation and memory resources than Hash functions. EPCglobal Class-1 Gen-2 tags provide such on-chip function. So our protocol is feasible to lowcost FRID systems with EPCglobal Class-1 Gen-2 tags.

REFERENCES

[1]Prosanta Gope, Tzonelih Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," computers & security, 55, pp.271–280, 2015.

[2] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications," Proc. of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. Lectures Notes in Computer Science, vo1.2523, pp.454-469, 2003.

[3]M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain Based Forward Secure Privacy Protection Scheme for Low-cost RFID," Proc. of the 2004 Symposium on Cryptography and formation Security, pp.719-724, 2004.

[4]Yong Ki Lee, Ingrid Verbauwhede. "Secure and Low-cost RFID Authentication Protocols," Proc. of the 2nd IEEE Workshop on Adaptive Wireless Networks, pp.1-5, 2005.

[5]J.-S.Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication

protocol using a secret value," Computer Communication, 34, pp. 391-397, 2011.

[6]Seyed Mohammad Alavi, Behzad Abdolmaleki, and Karim Baghery, "Vulnerabilities and Improvements on HRAP+, a Hash-Based RFID Authentication Protocol," ACSIJ Advances in Computer Science: an International Journal, 6(12) , pp.51-56, 2014.

[7]Cho Jung-Sik, Jeong Young-Sik, and Sang Oh-Park, "Consideration on the Brute-force Attack Cost and Retrieval Cost: A Hash-based Radio-frequency Identification (RFID) Tag Mutual Authentication Protocol," Computers and Mathematics with Applications. 8, pp.1-8, 2012.

[8]Kim, H., "Desynchronization Attack on Hash-based RFID Mutual Authentication Protocol," Journal of Security Engineering, 9(4), pp.357-365, 2012.

[9]Noureddine Chikouche, Foudil Cherif, "A Secure Code-Based Authentication Scheme for RFID Systems," International Journal of Computer Network and Information Security, 9, pp.1-9, 2015.

AUTHOR'S PROFILE:

N Swetha, Asst professor in Narsimha reddy engineering college.

Education: B.tech (ECE) at Nigama engineering college, Karimanagar

M.tech(EMBEDDED SYSTEMS) Narsimha reddy engineering college, Hyderabad

Research Interest: (In EMBEDDED SYSTEMS and IMAGE PROCESSING)