Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

RASCP: Providing for a Secure Group Communication Plane Using RFID

ks[1], Dr. Somashekhar C Desai[2] and Chandramouli H[3]

[1] JJT University

Received: 6 December 2011 Accepted: 5 January 2012 Published: 15 January 2012

Abstract

Predominantly large distributed networks currently provide support for group oriented protocols and applications. Regardless of the type of distributed network there is a need to provide communication privacy and data integrity to the information exchange amongst the group members.This paper introduces a protocol named RFID Authentication based Secure Communication Plane (RASCP). RASCP adopts the commutative RSA algorithm to maintain data integrity. The proposed protocol not only eliminates the overheads resulting from key distribution and key compromise attacks but also provide for information security in the presence of colluded group members. Radio Frequency Identification (RFID) tags is used for group member identification. The RACP protocol is compared with the RFID extended Secure Lock (RSL) group communication protocol and its efficiency in terms of the computational complexity involved is discussed in this paper.

Index terms— RFID, RFID security, RFID authentication secure group communication, cryptography, commutative rsa, secure plane, computational cost, sieve of eratost

1 Introduction

FID systems and standards established by IEEE [1,2] are envisioned to be one of the most commonly used identification mechanisms in the near future [3]. A RFID authentication system primarily consists of a tag and a reader with a database to store the tag details. Tags available are of several types and classes [1] [2] but the research work presented here considers the most commonly available passive RFID tags of class 0. A lot of research is ongoing to provide security to the existing standards and the technology involved in manufacturing and Radio Frequency (RF) communication systems in place. Currently there exist several threats to the existing RFID deployments like Denial of Service Attacks, RFID Tag Cloning, RFID Tag Tracing, Eavesdropping, Replay Attacks Data Forging, Invading Privacy Information and Hot-listing to name a few [3][4] [5][6] [7][8] [9] [10]. More often than not researchers have focused on the eliminating the threats that currently exist in the RFID technology and methods towards improving it. In the research work presented here the use of the existing RFID technology for identification is adopted. The proposed protocol i.e. ?????????? assumes that the RFID communication module considered is secure and free of the above mentioned defects/attacks.

Communication provisioning is considered as the basic essentials of any network. The prevalent large scale distributed networks existent provide support for various business, personal, commerce, banking, military, intelligence applications and services. These networks are prone to varied kind of attacks and data compromise issues. To counter the issue of data compromise cryptography is commonly used. Cryptographic algorithms could be broadly classified into two types namely Symmetric and Asymmetric type. The ?????????? protocol proposed utilizes the asymmetric commutative RSA Algorithm to provide for security. These algorithms are discussed in detail in the future sections of this paper.

The remaining paper is organized as follows. Section II discusses the commutative RSA algorithm. The Sieve of Eratosthenes prime number generation algorithm is discussed in the next section. The fourth section of

the paper provides an in depth explanation of the proposed ??????????group communication scheme. The fifth section of the paper presents the RFID extended secure lock group communication scheme. The penultimate section of the paper discusses the experimental evaluation wherein the propose ?????????? and the ?????? are compared. The conclusion and the future work is discussed in the last section of the paper.

2 II.

3 Commutative rsa

A secure plane is realizable provided the data communicated over the plane is protected and cannot be colluded.

4 Prime number generation

Prime number generation functions and their application to the arena of cryptography have been extensively studied by researchers. The ???????? proposed in this paper utilizes the Sieve of Eratosthenes Algorithm [11]

5 IX. End For Each

Using the Encryption and Decryption Key Pair Computation algorithm all the group members ? ?? ? ?? compute the encryption and decryption key pairs which enable to construct the envisioned secure communication plane. The ?????????? discussed eliminates the security arising from key exchange [14], negating key compromise [15] external server maintenance for key management [16] proving the efficiency in creating a secure communication plane. Let us consider ?? users of the group ?? that need to communicate securely and the secure communication group ?? ? is defined as?? ? = {? 1 , ? 2 , ? 3 , ? ? . ? ?? }

Where ?? ? ?? and ?? ? ? ??

The secure communication plane consisting of ?? group members communicate data by using a series of encryption and decryption operations. The commutative nature of the ?????? algorithm adopted in the ?????????? ensures that the data communicated is encrypted at least once i.e. the original data is encrypted and then only communicated over the plane thereby securing the data. The presence of any colluded users within the group represented by ? ?? , on intercepting the data would not be unable to determine the level of encryptions and decryption procedures performed on the data prior to his interception. In the case if the user ? ?? ? ?? intercepts the data after the first encryption, ? ?? would not be able to recover the data as the encryption and the

6 XVI. End For

Using the Communication over Secure Plane Algorithm discussed above the ? ?????? is able to receive the data ?? sent by the user ? ???????? using ?? number of encryption and decryption functions. The algorithm also highlights the fact that the data ?? to be transmitted is not transmitted in the original form i.e. it is encrypted and transmitted there by securing the data.

The ??????????discussed utilizes the ???????? tags available with each group member ? ?? to construct the secure communication plane. The RFID tags are often used for identification and tracking. In ?????????? the RFID tags are used both for security provision and identification. As the ?????????? adopts multiple encryption and multiple decryptions to securely communicate data the overheads arising from this could be considered as a drawback of the ??????????. The ?????????? is evaluated with the Secure Lock secure group communication protocol in the subsequent section of this paper.

7 V.

Rfid extended secure lock group communication scheme (??????) The ?????? is a ???????? based extended Secure Lock protocol [17]. The ?????? protocol considers a central server and a set of group members defined as?? ?????? = {? 1 ?????? , ? 2 ?????? , ? 3 ?????? , ? ? . ? ?? ?????? }

The ?????? protocol incorporates an asymmetric cryptographic algorithm to provide security. Let the Year private and public of a group member ? ?? ?????? ? ?? ?????? be represented as (?? ?????? ?? , ?? ?????? ??) . The central server also known as the security server establishes a set of ?? = |?? ?????? | pair wise relatively prime numbers ?? 1 , ? . , ?? ?? from the ???????? tags possessed using the Sieve of Eratosthenes Prime number generation algorithm. These numbers are then assigned to group members ? ?? ?????? ? ?? ?????? and are assumed to be public in nature. To establish a secure plane of for communication using the ?????? the server computes the following based on the a randomly selected key represented as ?? ?????? Colluded group members on decryption cannot obtain the lock ?? ?????? selected by the server accurately hence providing for security.

The Chinese remainder theorem utilized by the server provides protection by securing the group membership and group size. The use of the Chinese remainder theorem and asymmetric cryptographic schemes render the ?????? group communication scheme inefficient and are not scalable.

8 VI.

9 Performance evaluation

This ?????????? secure communication mechanism proposed in this paper is compared with the ?????? protocol in terms of the computational costs incurred. The computational cost incurred is proportional to the execution time observed. The ??????????and the ?????? systems were developed using C#.Net on the Visual Studio 2010 Platform. The ???????? tags used were of type 0. The ???????? readers were integrated into the platform using VC++.Net. To evaluate the ?????????? and the ?????? secure group communication systems and to observe the computational costs the number of users in the group were varied from 5, 10, 20, 50, 70 and 100 users. The observations were monitored using log files maintained for every operation. The introduction of the ???????? tags into the ?????????? and ?????? can be considered as an overhead that exists in reading the tags and the average time observed in reading the RFID tags when the number of group members are varied from 5, 10,20,50,70 and 100 is as shown in Fig 1 **??** It could be observed that the average of the overheads observed reduces as the number of users increase proving that the induction of the ???????? based security systems are scalable in nature and do not affect the responsiveness of the systems. The average time taken to read a ???????? tags was found to be about 0.76ms. The ?????? secure group communication system adopts the RSA Algorithm with a key strength of 1024 [19] bits to incorporate secure transmissions amongst the group members. The ?????????? adopts the commutative RSA algorithm to construct a secure communication plane. The ?????? relies on a central server for key initialization, distribution using locks and the verifications is carried out by the group members. The experimental evaluation conducted considered the protocol initialization phase as the time taken to verify the group membership and derive the cryptographic keys. The computational overheads observed are as shown in Fig. **??**. It could be observed that the overheads are reduced by about 99.43% in the initialization phase in the ?????????? protocol. The ?????? considers a central server and the verification process of the group members. The overheads resulting from the group membership verification process for the ?????? scheme is as shown in Form the figures it is clear that the commutative RSA algorithm adopted in the ??????????is computationally less expensive when compared to the RSA cryptographic algorithm adopted in the ?????? group communication scheme ye providing security.

10 Operations

The experimental evaluation discussed in this paper prove that the proposed ?????????? group communication protocol introduced in this paper performs better than the existing ?????? scheme by reducing the computational overheads and yet providing security of the data transacted amongst the group members.

11 VII.

12 Conclusion and future work

RFID devices are universally used for the purpose of identifications. Many researchers have focused on improving the security of RFID systems in place. This paper introduces a RFID Authentication based Secure Communication Plane (??????????) felicitating secure transmissions amongst group members. The ?????????? protocol adopts the commutative RSA algorithm to preserve the integrity of the data transacted over the communication plane. The RFID tags are used for the purpose of identification and for protocol initialization. The proposed ??????????scheme is compared with the ?????? secure group communication scheme. The ?????????? scheme proposed overcomes the drawbacks arising from key distribution, key compromise and external trusted server requirements, yet providing security in the presence of even colluded users. The experimental study conducted proves the efficiency of the proposed ?????????? over the ?????? group communication scheme. The future of the work presented here is to compare the RASCP scheme with other secure group communication schemes using RFID tags. [1] [2] [3]

[1] © 2012 Global Journals Inc. (US)Global Journal of Computer Science and Technology

[2] © 2012 Global Journals Inc. (US)

[3] RASCP: Providing for a secure group communication plane using RFID

1 

Figure 1: Figure 1 :

?????????_?? ???????? and ?????????_?? ???????? are computed using the following
?????????_?? ???????? = ???????????_?? ?? ???????? ? × ???????????_?? ?? ???????? ??
?????????_?? ???????? = ???????????_?? ?? ???????? ? 1?
× ???????????_?? ?? ???????
From the above equations it is clear that
?????????_?? ?? ?????????_?? ?? ???????? = ?????????_?? ?? ???????? for ?? and ?? . The encryptio
of ?? and ?? represented as
(?????????_?? ?? (?????????_?? ?? ???????? , ?????????_?? ?? ?????

is to be obtained.

obtained by randomly selecting numbers such that it is
a co prime of The decryption key pair of ?? and ?? is represented by
(?????????_?? ?? (?????????_?? ?? ???????? , ?????????_?? ?? ???????? , ?????????_?? ?? ???????
following equation
?????????_?? ????????
= (?????????_?? ????????) ?1 ??????(?????????_?? ????????)
The commutative RSA decryption operation on
the encrypted data ?? is defined
?????? ?? = ?? ?????????? _?? ???????? ??????(?????????_?? ????????)
a) Commutative proof RSA Algorithm
The commutative property of the RSA algorithm
adopted in ?????????? can be proved if data ?? encrypted by
?? and then encrypted by ?? provides the same resultant
if the encryption is performed by ?? followed by the
encryption performed by ?? i.e.
?????? ?? (?????? ?? ?????? ?? ? ?? ?????????? _?? ?? ???????? ??????(?????????_?? ?? ??) ??) ? ??

? ?????? ?? ? ?? ?????????? _?? ?? ???????? ??????(?????????_?? ??

???????? ? = ?? ??????????? _?? ?? ???????? × ?????????? _?? ?? ???????? ? ??????(?????????_?? ??
As ?????????? ?? ?? that ???????? = ?????????_?? ??

???????? ? = ?? ??????????? _?? ?? ???????? × ?????????? _?? ?? ???????? ? ??????(?????????_?? ??
And hence
?????? ?? (?????? ?? ??
)
?
??????
??
(??????
??

Figure 2:

RASCP: Providing for a secure group communication plane using RFID ?? , used to obtain the parameters ??????????_?? ?? ???????? and ??????????_?? ?? ???????? using the

2012 Sieve of Eratosthenes Prime number generation algorithm. Each member of the group contributes towards the construction of the commutative RSA sets

Year ??????????_?? and ??????????_?? defined as ??????????_?? = in ?? ?????? = {2,3,4, ? ?

68 Algorithm 1: Sieve of Eratosthenes Prime number generation algorithm Input: User RFID based Numbe

Volume XII Issue XVI Version I (D D D D)

E

is ??????????? ?? ? ?? VIII

is ????????

????,?????????

?? ??????????

? ??

?? ?

??

[Note: ?????? = ?? ?????????? (??????, ?? ?????? , ?? ??????) VII. While (?????? 2 > ?? ??????) VIII. ?? = Set of all indexes of ?? ???????? ? ?? ?????? ? ?? ???????? = ?? Let us consider a set of users who would like to communicate securely represented by a set defined as ?? = {? 1 , ? 2 , ? 3 , ? ? . ? ?? } Group Member Set ?? = {ð ?"°ð ?"° ?? , ð ?"°ð ?"° ?? , ð ?"°ð ?"° ?? , ? ? . ð ?"°ð ?"° ?? } II.Group RFID Tag Associated with each Group Member ð ?"°ð ?"° ?? , ?? ?? and its data ????????]

Figure 3:

Figure 4:

[44th Hawaii International Conference (2011)] *44th Hawaii International Conference*, Jan. 2011. p. .

[Paillard ()] 'A FULLY DISTRIBUTED PRIME NUMBERS GENERATION USING THE WHEEL SIEVE'. Gabriel Paillard . *Parallel and Distributed Computing and Networks*, 2005. p. .

[Gries and Misra ()] 'A linear sieve algorithm for finding prime numbers'. D Gries , J Misra . *Communications of the ACM* 1978. 21 (12) p. .

[Zou et al. ()] 'A New Scheme for Anonymous Secure Group Communication'. Xukai Zou , Mingrui Qi , Yan Sui . *System Sciences (HICSS)*, 2011.

[Bruhadeshwar and Kulkarni ()] 'Balancing Revocation and Storage Trade-Offs in Secure Group Communication'. Bezawada Bruhadeshwar , Sandeep S Kulkarni . *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING* JANUARY-FEBRUARY 2011. 8 (1) p. .

[Huang et al. (2010)] 'Hardware implementation of RFID mutual authentication protocol'. Y J Huang , C C Yuan , M K Chen , W C Lin , H C Teng . *IEEE Trans. Ind. Electron* May 2010. 57 (5) p. .

[Board ()] 'IEEE Standard for Smart Transducer Interface for Sensors and Actuators-Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats'. Ieee-Sa Standards Board . *IEEE Std* 1451. IEEE Instrumentation and Measurement Society. p. .

[Victor et al. (2007)] *Improving Satellite Multicast Security Scalability by Reducing Rekeying Requirements*, P Victor , HubenkoJr , A Richard , Rusty O Raines , Barry E Baldwin , Robert F Mullins , Michael R Mills , Grimaila . July/August 2007. p. .

[Arjen and Lenstra] 'Key length. Handbook of Information Security'. K Arjen , Lenstra . *Chief, Hossein Bidgoli*, p. .

[Juels (2004)] 'Minimalist Cryptography for Low-Cost RFID Tags'. A Juels . *Proc. Fourth Int'l Conf. Security in Comm. Networks (SCN '04)*, (Fourth Int'l Conf. Security in Comm. Networks (SCN '04)) Sept. 2004.

[Karst and Wicker ()] *On the Rekeying Load in Group Key Distributions Using Cover-Free Families*, Nathaniel Karst , Stephen B Wicker . 2011. IEEE.

[Crandall and Pomerance ()] *Prime Numbers: a computational perspective*, R Crandall , C Pomerance . 2001. Springer Verlag.

[Molnar and Wagner (2004)] 'Privacy and Security in Library RFID: Issues, Practices, and Architectures'. D Molnar , D Wagner . *Proc. 11th ACM Conf. Computer and Comm. Security (CCS '04)*, (11th ACM Conf. Computer and Comm. Security (CCS '04)) Oct. 2004.

[Lee and Kim (2006)] 'Privacy Threats and Issues in Mobile RFID'. H Lee , J Kim . *Proc. First Int'l Conf. Availability, Reliability and Security (ARES '06)*, (First Int'l Conf. Availability, Reliability and Security (ARES '06)) Apr. 2006.

[Juels (2005)] *RFID Security and Privacy: A Research Survey*, A Juels . Sept. 2005. (manuscript, RSA Laboratories)

[Alomair et al. ()] 'Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification'. Basel Alomair , Andrew Clark , Jorge Cuellar , Radha Poovendran . *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS* AUGUST 2012. 23 (8) p. .

[Chiou and Chen (1989)] 'Secure broadcasting using the Secure Lock'. G H Chiou , W Chen . *IEEE Transactions on Software Engineering* Aug. 1989. 15 (8) p. .

[Weis (2003)] 'Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems'. S Weis . *Proc. First Int'l Conf. Security in Pervasive Computing (SPC '03)*, (First Int'l Conf. Security in Pervasive Computing (SPC '03)) Mar. 2003.

[Weis (2003)] 'Security and Privacy in Radio-Frequency Identification Devices'. S Weis . *Mass. Inst. of Technology (MIT)* May 2003. (master's thesis)

[Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (T *Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats" ISO/IEC/IEEE21451-7*, (First edition 2011-12-15)