IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. 1 (Jan - Feb. 2015), PP 70-74
www.iosrjournals.org

RSA Algorithm as a Data Security Control Mechanism in RFID

Jonathan Sangoro[1]

Abstract: *With Radio Frequency Identification (RFID), new uses of identification and collection of data about tracking of items have been made possible; also, it is understandable that major interest is given to issues of information security and privacy. Lack of assurance regarding data security is one of the remaining obstacles for widespread usage of RFID (A. Juels and R. Pappu, 2004). RFID still can be done without security assurance if individuals do not have to worry about forsaking their privacy. Many issues related to data security and privacy within RFID systems is inherited through using already known technology and methods (Aljifri and Tyrewalla, 2004). However there are many new issues, especially regarding personal data security that need to be resolved and that is why I propose RSA algorithm to mitigate the data security challenges in RFID.*
Keywords: *RFID, Data security and RSA algorithm*.

I. Introduction

Radio Frequency Identification (RFID) has been in use for the last one and a half decades.

Currently, RFID systems are usually available in low, high, ultra-high, and microwave frequencies with passive, semi-passive (or semi-active) and active transponders or tags. Tags might be either Chipless, or contain a microchip with read only, or read and write memory. The component controlling communication in a RFID system is called a reader or interrogator, which can be stationary or portable depending on the application. In order for the tags to transmit their data, the tags must be in the reader's field or interrogation zone, and receive the necessary energy (in form of radio waves) from the reader.

Some of the key areas where RFID has been applied is; libraries, publishing, military, hospitals, asset management and livestock tracking.

Challenges to RFID technology

Although promising, RFID is not without its challenges, which arise from both a technological and usage point of view.

Security

Security is a key issue in RFID. People who use devices that carry personal information, such as credit card or other ID numbers, do not want others to access their accounts. These are significant security vulnerabilities in RFID and can lead to harm or losses.

Privacy

Another common concern with RFID is privacy. It is disconcerting for many people to have their movements or buying habits automatically tracked electronically. Many privacy groups are concerned about the ability to identify people as they walk through a store or shopping center via the tags embedded in their clothing and linked to them at the time of purchase.

Security Issues in RFID data communication

The communications between the components of RFID systems also suffer from security issues. Nevertheless, the level of vulnerability significantly differs from communication between the tag and the reader to communication between the reader and back-end system. Some of the security issues in the communication between the tag and the reader are listed below.

1. Eavesdropping.
   The communication between reader and tags via the air interface can be monitored by intercepting and decoding the radio signals. This is one of the most common threats to RFID systems. The eavesdropped information could for example be used to collect sensitive information about a person. It could also be used to perform a replay attack.
2. Replay Attack.
   The attacker can obtain and save all the exchanged messages between a tag and reader and either simulate the tag or the reader towards one another tag to access it's data.

3. Man-in-the-middle.
   A man-in-the-middle attack is a form of attack in which the adversary provokes or manipulates the communication between the reader and the tag, where manipulating the communication means relay, withhold, or insert messages.
4. Cloning Attack:
   The attacker reads the tag's information and copies it to another tag to impersonate the original tag. The backend server in this case cannot recognize the original tag from the fake one. This attack is typically a physical layer attack and that makes it hard to prevent.

Existing Solutions to Data Security

Kill Tag

By executing a special "kill" command on a tagged product, the RFID tag will be "killed" and can never be reactivated. This "kill" command may disconnect the antenna or short circuit fuse. This ensures that the tag cannot be detected any further, and thus protects the privacy of the individual who possesses the product.
But there are instances where a tag may need to be re-activated for examples when a customer returns a previously bought default item back to the store if the item is faulty, what happens then?

Faraday cage

An RFID tag can be shielded with a container made of metal mesh or foil, known as a "Faraday Cage". This foil lined container can block radio signals of certain frequencies and thus protect tagged products from being detected. However, this approach might not work in some situations. For example, it is difficult to wrap foil-lined containers around tags used in clothing for pets and people, or the goods in the supermarkets cannot all have their tags wrapped in a faraday cage for obvious reasons, it would be too expensive.

Active Jamming

Active jamming of RF signals refers to the use of a device that actively broadcasts radio signals in order to disrupt the operation of any nearby RFID readers. This physical means of shielding may disrupt nearby RFID systems. But if the jamming signal is too strong, there is a risk of disruption to all nearby RFID systems.

"RSA" Selective Blocker Tag

A blocker tag is a passive RFID device that uses a sophisticated algorithm to simulate many ordinary RFID tags simultaneously. It provides an endless series of responses to RFID readers through the use of two antennas to reflect back two bits simultaneously, thereby preventing other tags from being read, performing a kind of passive jamming.
However, this approach gives individuals a lot of control. In addition, a blocker tag may be used maliciously to circumvent RFID reader protocols by simulating multiple tag identifiers.

RSA Algorithm

Introduction

Rivest Shamir Aldeman (RSA) algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors which are Prime numbers. The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key. This makes the RSA algorithm a very popular choice in data encryption.

The Algorithm

First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it. It must be 512 bits at least i.e. numbers greater than 10^{154}. We then generate the encryption key e which must be co-prime to the number m = φ (n) = (p - 1) (q - 1). We then create the decryption key d such that de mod m = 1. We now have both the public and private keys.

Encryption

We let y = E(x) be the encryption function where x is an integer and y is the encrypted form of x
$y = x^e \bmod n$

Decryption

We let X = D(y) be the decryption function where y is an encrypted integer and X is the decrypted form of y

$X = y^d \bmod n$

Simple Example

a. We start by selecting primes p = 3 and q = 11.
b. n = p q = 33
2. m = (p - 1)(q - 1) = (2)(10) = 20.
3. Try e = 3
4. gcd (3; 20) = 1
5. $\Rightarrow$ e is co-prime to n
6. Find d such that $1 \equiv de \bmod m$
7. $\Rightarrow 1 = Km + de$
8. Using the extended Euclid Algorithm we see that 1 = -1(20) + 7(3)
9. $\Rightarrow d = 7$
10. Now let's say that we want to encrypt the number x = 9:
11. We use the Encryption function $y = x^e \bmod n$

a. $= 9^3 \bmod 33$
b. $= 729 \bmod 33 \equiv 3$

12. $\Rightarrow y = 3$
13. To decrypt y we use the function $X = y^d \bmod n$

$X = 3^7 \bmod 33$

$X = 2187 \bmod 33 \equiv 9$

$\Rightarrow X = 9 = x \Rightarrow$ It Works!

Example of RSA algorithm

Example 1

Let U = 5 and V = 11. This gives R a value of 55, and:

Phi (55) = (5 - 1) * (11 - 1) = 4 * 10 = 40.

Now, we need to find numbers to fit the equation:

P * Q = 1 (mod 40).

Let P=7

7 * Q = 1 (mod 40).

What would that make Q? If we rewrite this equation to get rid of the unfamiliar modulus arithmetic, we have:

7 * Q = K * 40 + 1, where K can be any number.

The first value for Q that works is 23:

7 * 23 = 161 = 4 * 40 + 1.

So we have 7 for P, our public key, and 23 for Q, our private key.
To make our cipher work, you may recall that the values we use for T must be less than R, and also relatively prime to R. We also don't want to use 1 for T, because 1 raised to any power whatsoever is going to remain 1.

Table 1. conversion table

2	3	4	6	7	8	9	12	13	14	16	17	1
A	B	C	D	E	F	G	H	I	J	K	L	M
19	21	23	24	26	27	28	29	31	32	34	36	37
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
38	39	41	42	43	46	47	48	49	51	52	53	
Sp	0	1	2	3	4	5	6	7	8	9	*	

The password we will encrypt is "VENIO"

V	E	N	I	O
31	7	19	13	21

Table 2. Conversion table

To encode it, we simply need to raise each number to the power of P modulo R.

V: 31^7 (mod 55) = 27512614111 (mod 55) = 26
E: 7^7 (mod 55) = 823543 (mod 55) = 28
N: 19^7 (mod 55) = 893871739 (mod 55) = 24
I: 13^7 (mod 55) = 62748517 (mod 55) = 7
O: 21^7 (mod 55) = 1801088541 (mod 55) = 21

So, our encrypted message is 26, 28, 24, 7, 21 -- or "RTQEO" in our personalized character set.
When the message "RTQEO" arrives on the other end of our insecure phone line, we can decrypt it simply by repeating the process -- this time using Q, our private key, in place of P.

R: 26^23 (mod 55) = 350257144982200575261531309080576 (mod 55) = 31
T: 28^23 (mod 55) = 19259043800372760688541191131627 52 (mod 55) = 7
Q: 24^23 (mod 55) = 55572324035428505185378394701824 (mod 55) = 19
E: 7^23 (mod 55) = 27368747340080916343 (mod 55) = 13
O: 21^23 (mod 55) = 25765808751082182919290758696 61 (mod 55) = 21

The result is 31, 7, 19, 13, 21 -- or "VENIO", our original message.

Proposed Solution

The solution which I propose is an RSA password generated query to improve data security in RFID and ensure that data cannot be accessed by any random reader or attacker that is transmitting radio signal. This also prevents hacking, modification and eavesdropping of data stored in tags by malicious individuals who know that as long as they have readers which transmit radio frequency they can always intercept data or prompt data from tags even if the data stored in those tags is not intended for them. They then use this private data for the own malicious intentions, blackmail or advantage by selling it to the highest competitor.

This improvement can be done by adding a script of code to the middleware or software that enables communication or flow or data between the different components that make up and RFID system (tags, readers and database).

Finally, this also solves the problem of multiple collision of data from different tags as only the tags with the verified and authenticated password will be allowed to transmit it's data while the rest of the tags will be locked out.

How it works

Data security is enhanced by ensuring that the reader and the tag must first have RSA algorithm encoded in the source code. This will ensure that before data transmission occurs, the reader will query the tag to send it's password, the tag will then send it's password in ciphertext back to the reader for authentication and verification. The reader then uses the private key in it's possession to decrypt the ciphertext password back to plaintext and quickly matches it to the password of that particular tag which is stored in the database. If the password is correct then the corresponding requested data by the reader is transmitted in ciphertext form. Once the reader receives this data, it quickly uses the private key in its possession to decode the data ciphertext to plaintext.

Data Security requirements shall be incorporated in the reader such that if the tag sends its correct encrypted password (in ciphertext) which is verified and authenticated then data transmission is allowed to proceed from tag to reader and vice-versa, but if the password sent by the tag is wrong , further communication between the tag and reader is blocked forthwith. The advantage is also cemented in the fact that RSA algorithm is based on factorization of two large prime numbers which cannot be easily broken down or determined if one does not have a private key.

II. Conclusion And Recommendation

While the use of RFID technology is increasing across a range of different industries, the associated security and privacy issues need to be carefully addressed.

This paper recommends the use of public key encryption, RSA algorithm in particular is a robust approach to mitigating the data security issues in RFID. This is due to the fact that RSA algorithm is based on use of public and private keys which are used to encrypt data from plaintext to ciphertext and again decrypt the ciphertext back to plaintext. This is the main reason for recommending RSA algorithm as a suitable mechanism for mitigating data security in RFID applications. This is because an attacker who does not possess the correct private key can never decrypt the correct password since the key he/she posses will decrypt the data, yes, but it will be the wrong password and communication terminated henceforth.

This is a low cost technique of enhancing data security since no new equipment requires to be bought but only a small script of code is added to the original software to append the RSA algorithm to the code for data security enhancement.

References

[1]. A.Juels and R. Pappu, (2003), "Squealing euros: Privacy protection in RFID-enabled banknotes", In proceedings of Financial Cryptography – FC'03, LNCS, volume 2742, Springer-Verlag, pages 103-121.
[2]. Tanenbaum, D. Wetherall "Computer Networks"2011.
[3]. AES page available via http://www.nist.gov/CryptoToolkit

[4]. Artz, Matthew (2003). City library adopts controversial RFID chips. Retrieved October 10, 2003, from http://www.berkeleydaily.org/article.cfm?issue=10-10-3&storyID=17547

[5]. Auto-ID Center, (2002), "860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0", Technical Report MIT-AUTOID-TR-007, November.
[6]. Booth-Thomas, Cathy (2003, October 20). The see-it-all chips. Time, 162 (15), 12-17
[7]. Chachra, Vinod (2003). Experiences in implementing RFID solutions in a multi-vendor
[8]. environment. IFLA Conference, Berlin, August, 2003. Retrieved August 15, 2003, from
[9]. http://www.ifla.org/IV/ifla69/paper/132e-chachra.pdf
[10]. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
[11]. EPC Radio-Frequency Identity Protocols Generation 2 Identity Tag (Class 1):Protocol for Communications at 860 MHz-960 MHz. EPC Global Hardware Action Group (HAG), EPC Identity Tag (Class 1) Generation 2, Last-call Working Draft Version 1.0.2, 2003-11-24.
[12]. FIPS 180-2. Secure Hash Standard, http://csrc.nist.gov/publications/, 2002
[13]. H. Aljifri, and N. Tyrewalla, (2004), "Security model for Intra-Domain Mobility Management Protocol", Int. J. of Mobile Communications, Vol. 2, No.2, pp. 157 – 170.
[14]. Hecht, Jeff (2004). Casino chips to carry RFID tags. New Scientist. Retrieved September 02, 2004, from http://www.newscientist.com/news/news.jsp?id=ns99994542
[15]. Holmström, J., Ketokivi, K., Hameri, A.-P. (2009b), "Bridging Practice and Theory: A Design Science Approach", Decision Sciences, Vol. 40 No. 1, pp. 65-87.
[16]. Juels, A., Weis, S.A. (2005). Authenticating Pervasive Devices with Human Protocols.
[17]. Advances in Cryptology – Crypto '05. Lecture Notes in Computer Science. Volume 3621. Pages 293-308.
[18]. W. Küchlin, "Public key encryption," ACM SIGSAM Bulletin, August 1987, pp. 69-73.