Data Security On RFID Information Using Word Auto Key Encryption Algorithm

Robbi Rahimi*, Syamsuddin Lubis2, N Nurmalini2, Haida Dafitri3
1Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia
2Department of Informatics, AMIK Intel Com Global Indo, Kisaran, Indonesia
3Department of Informatics, Universitas Harapan Medan, Medan, Indonesia

*usurobbi85@zoho.com

Abstract. RFID technology is a technology that is commonly used, one of the problems that exist in RFID is the information contained in RFID Tags are not encrypted and easily read by others. Word Auto Key Encryption (WAKE) is one of the cryptographic algorithms that can be used to secure data on RFID Tag. Experiments resulted in the process of reading and writing encrypted data on RFID Tags can be done well and data more secure than before.

1. Introduction

Development of communications technology in the digital age is currently vulnerable to security attack [1], [2]. One way to secure data is to change the data into another form that cannot be known by others [3], encryption using cryptography is one of solution that can be used.

Data on Radio Frequency Identification (RFID)[4], [5] are in the form of text and this can be read by transponders remotely without having direct contact [6], the data on the RFID label is generally not encrypted and can be read or modified by irresponsible parties, thus action can cause deprivation to the owner. Securing data on RFID by using a cryptography algorithm is chosen because it takes time for irresponsible parties to read and if data on RFID modified with plain text it will not be read by transponders due to different data (Non Encryption), Word Auto Key Encryption (WAKE) algorithm [7] is used on RFID data security.

Security testing on RFID is perform by using RFID Card, RFID Reader and Arduino as experiment material, RFID Card contains encrypted text using WAKE algorithm. An experiment is done to prove that data on RFID is safe and cannot be easily read when data encrypted using WAKE algorithm.

2. Methodology

2.1 Cryptography

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, sender/recipient authentication, and data authentication so messages or documents are secure and unreadable by unauthorized parties [3], [8]–[12]. General purpose cryptography [3], [9]:

A. Confidentiality
   Ensure that data or information can only be accessed by certain parties only.

B. Authentication
   the sender and the recipient of the message know that the message came from the actual party.
C. Integrity
   This issue relates to the assurance that the data or messages sent are not modified to the recipient.

D. Nonrepudiation
   Nonrepudiation prevents both senders and receivers from denying that they have sent or received a message / information. If a message is sent, the recipient can prove that the message was indeed sent by the sender listed. Conversely, if a message is received, the sender can prove that the message has been received by the intended party.

E. Access Control
   Limit data sources only to specific people.

F. Availability
   Required all information on a computer system and must be available to all parties entitled to such information.

The six aspects of data security, four of them can be overcome by using cryptography that is confidentiality, integrity, authentication, and nonrepudiation.

2.2 Word Auto Key Encryption

Word Auto Key Encryption (WAKE) is a stream cipher algorithm that works using 128 bit keys and a 256 x 32 bit table [7], [13]. The WAKE algorithm uses XOR, AND, OR and Shift Right operations in the encryption and decryption process. The main process of WAKE algorithm such as [7]:

a. Formation of S-Box table.

b. Key generation.

c. Encryption and Decryption.

The core of the WAKE algorithm exists in the process of forming the S-Box table and the key generation. The S-Box table of the WAKE algorithm is flexible and different for each round.

Program listing of the WAKE algorithm used for the encryption and decryption process [7].

a. Wake Encryption

```
strPlain = pcEnkripsi
X = ""
For N = 1 To Len(strPlain)
   X = X & FormatS(FDecToBiner(Asc(Mid(strPlain, N, 1))), "0", 8)
Next N
X1 = "": X2 = "": cHasil = ""
For N = 1 To Len(X) Step 8
   X1 = Mid(strKunciBiner, (N Mod 32), 8)
   X2 = FOpBiner("XOR", Mid(X, N, 8), X1, 8)
   cHasil = cHasil & Chr(FBinerToDec(X2))
Next N
strCipher = cHasil
```

b. Wake Decryption

```
strCipher = pcDekripsi
X = ""
For N = 1 To Len(strCipher)
   X = X & FormatS(FDecToBiner(Asc(Mid(strCipher, N, 1))), "0", 8)
Next N
X1 = "": X2 = "": cHasil = ""
For N = 1 To Len(X) Step 8
   X1 = Mid(strKunciBiner, (N Mod 32), 8)
   X2 = FOpBiner("XOR", Mid(X, N, 8), X1, 8)
   cHasil = cHasil & Chr(FBinerToDec(X2))
Next N
strPlain = cHasil
```

c. Key Generation

```
X = ""
For N = 1 To Len(pcKunci)
\[ X = X \& \text{FormatS(FDecToBiner(Asc(Mid(pcKunci, N, 1))), "0", 8)} \]

Next N

\[ A(0) = \text{Mid}(X, 1, 32) \]
\[ B(0) = \text{Mid}(X, 33, 32) \]
\[ C(0) = \text{Mid}(X, 65, 32) \]
\[ D(0) = \text{Mid}(X, 97, 32) \]

For N = 1 To pnPutaran
  \[ A(N) = \text{FungsiM}(A(N - 1), D(N - 1)) \]
  \[ B(N) = \text{FungsiM}(B(N - 1), A(N)) \]
  \[ C(N) = \text{FungsiM}(C(N - 1), B(N)) \]
  \[ D(N) = \text{FungsiM}(D(N - 1), C(N)) \]
Next N

\[ \text{strKunciBiner} = D(N - 1) \]

2.3 *Radio Frequency Identification*

Radio Frequency Identification (RFID)\[4\] is an object identification method by utilizing radio waves. The identification process is done by RFID Reader and RFID Transponder (RFID tag). The system works by placing RFID tags on an object or object to be identified. Each RFID tag has a unique identification number (ID number), so no RFID tags have the same ID number \[4\], \[14\]. RFID technology can be used to describe a system capable of transmitting identity data from an object wirelessly using radio waves\[14\].

Generally RFID system consists of 4 components\[15\]–\[17\], such as:

a. Tags
   Tags are devices that store information for object identification. RFID tags are often also referred to as transponders.

b. Antenna
   A device used to transmit radio frequency signals between RFID readers and RFID tags.

c. RFID Reader
   It is a device compatible with RFID tags that will communicate wirelessly with tags.

d. Application Software
   An application on a workstation or PC that can read data from tags through RFID reader. Both the RFID tag and reader are equipped with an antenna so that it can receive and emit electromagnetic waves

RFID reader is a connection between the application software with the antenna that will radiate radio waves to RFID tags \[14\]. Radio waves emitted by the antenna operate in the surrounding space. Consequently data can move wirelessly to RFID tags that are located adjacent to the antenna. In this research used RFID reader RC522 as reader/writer and using tags with Mifare S50 RFID card / Contactless card 13.56 Mhz HF.

*Figure 1. RFID Reader RC522*
Security system application architecture for RFID [15], [18], [19] that can be used there are 4 (four) types:

a. Fixed Code System
   This system is the simplest and most used system. Fixed code stored in the RFID tag is read and compared to the code stored in the database. This system does not allow copying of RFID tags. This simple system has the lowest security level.

b. Rolling Code System
   Operates in the same way as the Fixed Code system, but the secret code in the RFID tag is only valid for a certain period of time. RFID readers on this system must have the ability to write RFID tags. The RFID tags used must be programmed multiple times. This system provides better security, but that should be considered is the secret code synchronization process.

c. Password Protection System
   Simple authentication systems can be provided by RFID systems with password protection. Confidential data on RFID tags will only be transmitted after the RFID reader sends the appropriate password data to prove the validity of the RFID reader. The length of the password can vary between several minutes to several years depending on the length of the password. For security systems with multiple users and with different passwords, the limitations of total communication time are very long, because RFID readers should expect passwords from the available databases.

d. Combination System Rolling Code with Password
   It is an aggregated system with a revamped secret code facility and password to protect secret codes stored in RFID tags. The critical issue of this system is the timing of communication and password synchronization. With this system will provide a high level of security.

Weaknesses in the fixed code system that the data stored in the text and must be compared in the database, to overcome the weakness of fixed code system can be done with the encryption before to write in RFID Tag and the key used is Serial Number in RFID Tags that would not be possible same all over RFID Tag.

3. Results and Discussion

The mechanism of data security on RFID Tag consists of writing and reading process on RFID Tags, all communication process is done by using Arduino UNO as communication between RFID Reader, RFID Tag and computer as host, see figure 3 below for thus communication.
The above mechanism describes the information security process in RFID Tag, where the process of writing and reading is done on the host.

An experiment of data security on RFID is accomplished by determining plaintext, key and number of key rotation (S-Box), as previously explained under the formation of key and S-Box is very dynamic.

\[
\text{Plaintext} = \text{SCITEPRESS}
\]

\[
\text{Key} = 000009002E4EA2CB
\]

\[
\text{Rotation} = 3
\]

In addition the above key is obtained from the RFID Tag serial number by adding 4 digits 0000 before "09002E4EA2CB" so that the key is equal to 2 bytes. The result of the plaintext encryption process is as follows:

\[
\text{Plaintext: } \text{SCITEPRESS}'
\]

| ASCII from 'S' | ASCII from 'C' | ASCII from 'I' | ASCII from 'T' | ASCII from 'E' | ASCII from 'P' | ASCII from 'R' | ASCII from 'E' | ASCII from 'S' |
|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| 53             | 43             | 49             | 54             | 45             | 50             | 52             | 45             | 53             |

\[
\text{Plaintext (hexadecimal)} = 53434954455052455353
\]

\[
\text{Key in hexadecimal} = 2B1C125A
\]

\[
\text{Ciphertext} = \text{Plaintext XOR Key}
\]

\[
\begin{align*}
53 \text{ XOR } 2B &= 78 = \text{'x'} \\
43 \text{ XOR } 1C &= 5F = \text{'}
\end{align*}
\]

\[
\begin{align*}
49 \text{ XOR } 12 &= 5B = \text{'}
\end{align*}
\]

\[
\begin{align*}
54 \text{ XOR } 5A &= 0E = \text{'}
\end{align*}
\]

\[
\begin{align*}
45 \text{ XOR } 2B &= 6E = \text{'}
\end{align*}
\]

\[
\begin{align*}
50 \text{ XOR } 1C &= 4C = \text{'}
\end{align*}
\]

\[
\begin{align*}
52 \text{ XOR } 12 &= 40 = \text{'}
\end{align*}
\]

\[
\begin{align*}
45 \text{ XOR } 5A &= 1F = \text{'}
\end{align*}
\]

\[
\begin{align*}
53 \text{ XOR } 2B &= 78 = \text{'x'}
\end{align*}
\]

\[
\begin{align*}
53 \text{ XOR } 1C &= 4F = \text{'O'}
\end{align*}
\]

\[
\text{Ciphertext} = x_{__}nL@_xO
\]

The next test is ready with same plaintext and key but with different rotation number, S-Box rotation is used 6 rounds to get the result below.

Key generation from s-box process

\[
\text{Key} = \text{A3D23A2A}
\]

\[
\text{Cipher text} = \text{Plaintext XOR Key}
\]

\[
\begin{align*}
53 \text{ XOR } A3 &= F0 = \text{'}
\end{align*}
\]

\[
\begin{align*}
43 \text{ XOR } D2 &= 91 = \text{'}
\end{align*}
\]

\[
\begin{align*}
49 \text{ XOR } 3A &= 73 = \text{'}
\end{align*}
\]
54 XOR 2A = 7E = ‘~’  
45 XOR A3 = E6 = ‘œ’  
50 XOR D2 = 82 = ‘,’  
52 XOR 3A = 68 = ‘h’  
45 XOR 2A = 6F = ‘o’  
53 XOR A3 = F0 = ‘ð’  
53 XOR D2 = 81 = ‘’

Cipher text = ð’s~æ’hoð

Ciphertext result then written to RFID Tag using arduino as the medium. Based on the above two test results obtained different ciphertext when the number of key rotation with S-Box function made 3 rounds and 6 round, ciphertext results can be decrypted using the same step where the key and the number of key rounds should be same, reading of information (ciphertext) on RFID Tag with RFID Reader will activate the decryption process automatically to know data in RFID Tag were true.

4. Conclusion

Data security on RFID Tags by using WAKE algorithm can be done well, the data available on RFID Tag will also be difficult to read by unauthorized if doesn’t not know the algorithm, key and key rotation count. Improvisation from this research can be developed chip or RFID Tag which have component of cryptography which by default can be read and written by system and easy in synchronization.

REFERENCES

[1] H. Nurdiyanto, R. Rahim, and N. Wulan, “Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement,” J. Phys. Conf. Ser., vol. 930, no. 1, p. 012005, Dec. 2017.
[2] H. Arrosida and M. E. Echsony, “The Design of Optimal PID Control Method for Quadcopter Movement Control,” Int. J. Artif. Intell. Res., vol. 2, no. 1, p. 1, Feb. 2018.
[3] R. Rahim, “Man-in-the-middle-attack prevention using interlock protocol method,” ARPN J. Eng. Appl. Sci., vol. 12, no. 22, pp. 6483–6487, 2017.
[4] R. Want, “An introduction to RFID technology,” IEEE Pervasive Computing, vol. 5, no. 1. pp. 25–33, 2006.
[5] Iswanto, O. Wahyunggoro, and A. I. Cahyadi, “3D object modeling using data fusion from laser sensor on quadrotor,” in AIP Conference Proceedings, 2016, vol. 1755.
[6] A. Randall, “RFID Can Be Hacked: Here’s How, & What You Can Do To Stay Safe,” 2017. [Online]. Available: http://www.makeuseof.com/tag/rfid-hacked-stay-safe/. [Accessed: 03-Sep-2017].
[7] L. Legito and R. Rahim, “SMS Encryption Using Word Auto Key Encryption,” Int. J. Recent Trends Eng. Res., vol. 3, no. 1, pp. 251–256, 2017.
[8] S. Manna and S. Dutta, “A Stream Cipher based Bit-Level Symmetric Key Cryptographic Technique using Chen Prime Number,” Int. J. Comput. Appl., vol. 107, no. 12, pp. 975–8887, 2014.
[9] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, “Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression,” World Trans. Eng. Technol. Educ., vol. 15, no. 3, pp. 292–297, 2017.
[10] R. Rahim and A. Ikhwan, “Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher,” *Int. J. Sci. Res. Sci. Technol.*, vol. 2, no. 6, pp. 71–78, 2016.

[11] R. Rahim, “128 Bit Hash of Variable Length in Short Message Service Security,” *Int. J. Secur. Its Appl.*, vol. 11, no. 1, pp. 45–58, Jan. 2017.

[12] H. Wandani, M. Budiman, and A. Sharif, “Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem,” *Alkhawarizmi*, 2012.

[13] H. Gultom, “Penyandian Email Menggunakan Algoritma Kriptografi WAKE( Word Auto Key Encryption),” *Pelita Inform. Budi Darma*, vol. 4, no. 1, pp. 107–111, 2013.

[14] M. Kaur, M. Sandhu, N. Mohan, and P. S. Sandhu, “RFID Technology Principles, Advantages, Limitations &amp; Its Applications,” *Int. J. Comput. Electr. Eng.*, vol. 3, no. 1, pp. 1793–8163, 2011.

[15] A. N. Nambiar, “RFID technology: a review of its applications,” *Proc. World Congr. Eng. Comput. Sci.*, vol. 2, pp. 20–22, 2009.

[16] S. Garrido Azevedo and H. Carvalho, “Contribution of RFID technology to better management of fashion supply chains,” *Int. J. Retail Distrib. Manag.*, vol. 40, no. 2, pp. 128–156, 2012.

[17] C. M. Roberts, “Radio frequency identification (RFID),” *Computers and Security*, vol. 25, no. 1, pp. 18–26, 2006.

[18] S. Spiekermann and S. Evdokimov, “Critical RFID privacy-enhancing technologies,” *IEEE Secur. Priv.*, vol. 7, no. 2, pp. 56–62, 2009.

[19] H. Knospe and H. Pohl, “RFID security,” *Inf. Secur. Tech. Rep.*, vol. 9, no. 4, pp. 39–50, 2004.