DESIGN AND IMPLEMENTATION OF A SECURITY LAYER FOR RFID SYSTEMS

V. Alarcon-Aquino, M. Dominguez-Jimenez, C. Ohms[1]

Department of Computing, Electronics, and Mechatronics
Universidad de las Américas Puebla
Cholula, Puebla, MEXICO
vicente.alarcon@udlap.mx

[1]Department of Information Technology and Electronics
Fachhochschule Kiel
Kiel, GERMANY

ABSTRACT

RFID (Radio Frequency Identification) is a technology whose employment will certainly grow in the following years. It is therefore necessary to consider the security issues that come out from the implementation of that type of systems. In this paper we present an approach to solve the security problems in RFID systems by designing a naive security layer based on authentication and encryption algorithms. The authentication mechanism is the mutual authentication based on a three-way handshaking model, which authenticates both the reader and the tag in the communication protocol. The cipher algorithm based on a symmetric-key cryptosystem is RC4 implemented in a proposed modification to the existing WEP protocol to make it more secure in terms of message privacy. The proposed approach is implemented using VHDL in FPGAs communicated through RF transceivers. The results show that the security layer is simple enough to be implemented in a low-price RFID tag.

KEY WORDS: *RFID, security layer, encryption, authentication, FPGA, WEP, RC4.*

1. INTRODUCTION

Automatic identification is a technology that has basically been around since the 1930s. It consists in obtaining information from an object, in order to identify it, in a fast and efficient way, without human intervention in the transference of information [1]. Bars code is one of the most popular automatic identification technologies used for many years in inventory control systems and supply chain management [2]. There is also another technology that appeared in recent years which identifies objects using radio frequency signals known as RFID (Radio Frequency Identification). In this technology, the information that identifies an object travels through the air in electromagnetic waves. Even though RFID seems to be new, it came out in the 50s but it was very expensive to implement [3].

RFID is a technology with a promising future so research in this kind of systems has had an exponential growth in the last years [3]. The most common application of RFID is good management in the supply chain that will cause the bars code to disappear. It has also been considered that RFID could be the key of the evolution of next generation networks, where ubiquitous is one of the most desired characteristics [2]. Since RFID is a technology whose employment will certainly grow significantly in the following years, there have been concerns about insecurities that come out from the implementation of that type of systems. RFID technology presents risks of unique privacy and security because people cannot be aware of the radiation used to read the tags, allowing any person with a reader to obtain data from tags that are in close vicinity [2]. Espionage problems can be presented with passive or active system attacks. When a passive attack is done, the information is only compiled and it is not altered; on the other hand, in an active attack the information integrity is altered [2]. It is therefore important to implement a security

layer that protects the information and prevents its undesired distribution, using schemes of information encryption and user authentication.

Recently, several published works present solutions to the aforementioned problems (see e.g., [1], [4], [5], [6], [7]). In [4] the author proposes a security scheme for RFID systems based on authentication and encryption algorithms. A mutual authentication protocol and an asymmetric cryptographic algorithm are proposed. The disadvantage of this approach is the implementation of the asymmetric algorithm because it requires complex hardware. In [1] the author presents RFID technology and its security and privacy issues. A series of possible solutions like hash functions, detections units and security agents is presented. These solutions are implemented in the reader avoiding the hardware limitations that tags have, with exception of the proposal based on the hash functions, which provides an authentication method in the system. In [5], [6], [7], the authors present an overview of the main security threats to RFID systems and possible solutions. In this paper, we propose an approach to solve the security problems in RFID networks by designing a naive security layer based on authentication and encryption algorithms. The authentication mechanism is the mutual authentication based on a three-way handshaking model in the communication protocol. The cipher algorithm is RC4 (Rivest Code 4) implemented in a proposed modification to the existing WEP (Wired Equivalent Privacy) protocol to make it more secure in terms of message privacy. Note that many new protocols like Wi-Fi Protected Access (WPA), WPA2, Robust Secure Networks (RSN) and 802.11i have been proposed to solve the vulnerabilities issues of the WEP protocol; nonetheless, despite their efficiency, these standards, and especially 802.11i, need hardware renew and reconsideration of security architecture [8], [9].

The rest of the paper is organized as follows. In Section 2, an overview of the RFID technology is introduced; In Section 3, we present the basic concepts of secure data networking as well as the privacy and security problems in the operation of RFID systems; In Section 4, the security layer designed for RFID systems is proposed, covering the air interface, the data frames, the authentication protocol and the encryption algorithm; Section 5 presents the hardware implementation of the proposed security layer using VHDL (*Very high speed integrated circuit Hardware Description Language)* in FPGAs (*Field-Programmable Gate Array*); experimental results are reported in Section 6. Finally, in Section 7, we present the conclusions drawn from previous sections

2. RFID TECHNOLOGY

In this section, we present an overview of the RFID technology. The first idea on RFID came out in 1948 with Harry Stockman who assured that the communication by reflected power could be viable [3]. An RFID system is always made up of three components (see Fig. 1): the *tag* is a transponder located on an object and holds the data that identifies it; the *reader* is a data capture device; and an *application* that processes all the information gathered by the reader [10]. RFID technology is based on the idea that an electronic circuit in a tag can be powered from a distance by a reader device which broadcasts energy to it using electromagnetic fields. When the tag is powered, it can exchange information with the reader through a physical principle known as backscatter modulation. In this process, a reader sends a signal to a tag, and the tag responds by reflecting part of this energy back to the reader.

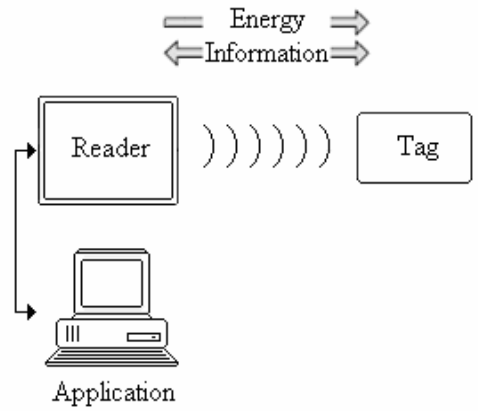

Figure 1. Components of an RFID system.

Data transfer from tags to readers must be done in a reliable way. A reliable communication depends on the coding technique and the modulation scheme of the transmissions. The coding technique in RFID systems must be selected in order to maintain the tags powered, as long as possible, not to consume too much bandwidth, and to detect collisions [1]. One solution is to use RZ (*Return-to-Zero*) coding on the forward channel and Manchester coding on the backward channel. Data coding determines the representation of each bit in a frame, meanwhile modulation determines how tags and readers communicate.

In RFID systems it is preferred to use FSK (*Frequency-Shift Keying*) and PSK (*Phase-Shift Keying*) because they maintain constant amplitude in the modulated signal, assuring maximum energy transfer from reader to tags. Since RFID systems generate and broadcast electromagnetic waves, they are classified as radio systems. They should not interfere or be interfered by other systems such as mobile telephony, radio and TV, among others. In order to solve interference problems with other licensed radio systems, RFID applications use the ISM (*Industrial, Scientific and Medical*) band which has been reserved for industrial, scientific and medical applications.

3. COMMUNICATION SYSTEMS SECURITY

In this section, a brief description of the security issues normally found in a communication systems security is described. Different components, resources and entities, turn a communication network into an easy target for attacks and illegal procedures. As a consequence, security is considered one of the most important operational aspects in networking. There are two primary classes of attacks in a communication system [11]:

- *Passive attack* – the data that is being transmitted from sender to receiver is being observed by the intruder. This type of attack threatens the confidentiality of information in transmission.

- Active attack – the intruder is able to observe and control the data transmitted. An active attack threatens the integrity and availability of information.

In order to confront these attacks, the security services have been established and they have the specific purpose of authenticate users and of maintaining the information as a secret [12]. The security services are implemented using security mechanisms such as user authentications mechanisms, to provide uniqueness identification; encryption mechanisms, to provide confidentiality; and data integrity mechanisms, to provide the authenticity of the source [13]. Usually encryption mechanisms apply for active tags. Since passive tags have short effective reading ranges, the risk of an intruder manipulating or eavesdropping the transmission is relatively low. Especially tags in the frequency band of 13.56 MHz

have ranges in the order of tens of centimeters [5] which means that an eavesdropper would have to come into very close proximity. Active tags, on the other hand, have ranges up to 100 meters, increasing the risk of manipulated or eavesdropped transmission significantly and, therefore, having a greater demand for security mechanisms. Fortunately, active tags also provide a more powerful energy source and, hence, permit the use of complex encryption hardware.

It is well known that the electromagnetic fields created by readers to get the information from tags allow any person with a reader to intercept that information. This allows obtaining the information stored in tags which causes privacy and security problems [1]. RFID must consider a protection scheme that allows the systems to defend from the following attacks [10]:

- Unauthorized reading of the information that a tag stores, with the purpose of duplicating or modifying it.

- Eavesdropping transmissions with the purpose of successfully obtaining information, and being able to take the identity of a tag.

Although other attack scenarios exist, besides the two mentioned before, these represent the most threatening and severe dangers to the security of a RFID system. Considering these types of attacks, the risks can directly be associated to organizations or people [2]. In an organization, commercial espionage risks can appear, causing the development and competitiveness between enterprises to be in danger. On the other hand, with the information obtained about our properties, offenders could track us and register our daily activities without our consent.

3.1 Authentication Algorithms

Before having access to a communication network, users must identify themselves and the system must identify its identity. This process is made through the identification, authentication and authorization of the entities that require communicating. User identification and authentication mechanisms in communication networks can be divided into entity authentication and mutual authentication systems [12]. In entity authentication systems, the identification and authentication is only one-way, and the entity authenticated is the one that initiates the communication. In mutual authentication systems, the identification and authentication is two-way, and both entities are authenticated. The handshaking model is preferable for mutual authentication.

3.2 Encryption Algorithms

The purpose of cryptography is to give confidentiality to the message that is transmitted and to guarantee the authenticity of the cryptogram and the entities that communicate [14]. The ciphering is made by applying mathematical techniques derived from a secret sequence of data called key, to the information. The application of these mathematical techniques is determined in the encryption algorithms. The encryption algorithms can be classified on the basis of the keys used, viz [14]:

- *Symmetric-key schemes* – the key used for encryption is the same for decryption. This key must be kept as a secret and it is known only by the entities that communicate.

- *Asymmetric-key schemes* – the key used for encryption is different for decryption. The encryption key is of public knowledge whereas the decryption key remains secret and it is only known by the entity that will receive the cryptogram.

Before analyzing encryption algorithms, it is necessary to know the perfect secrecy conditions established by Shannon in order to identify perfect ciphers [14]. These conditions are:

1. The secret key will be used only once.
2. The cryptanalyst has access only to the cryptogram.

The robustness of a cipher algorithm does not have to be the definitive element to establish its security, it is necessary to consider the usage of the algorithm and the protocols. Symmetric-key cryptosystems are based on simple operations that can be performed without having a deep background in mathematics and cryptology. The disadvantage of this system is that a key establishment stage must be carried out before any transmission [11]. Asymmetric-key cryptosystems in theory are more convenient than symmetric cryptography since it is not necessary to share a secret key. However, these systems require arithmetic operations that are difficult for small devices with limited processing power [11]. Cryptography in RFID systems shows a clear tendency towards symmetric-key algorithms [10] because the tags are limited in processing capabilities, complicating the design of asymmetric systems. Symmetric-key algorithms can be divided into block and stream ciphering mechanisms [14].

3.2.1 Stream ciphering mechanisms

The stream ciphering mechanism is shown in Fig. 2. It can be seen that in the transmitter, the bits of the plaintext M are combined, one at a time, with the bits of a pseudorandom stream S, generated from a secret key K, to get the ciphertext C. In the receiver, the bits of the ciphertext C are combined with the bits of the pseudorandom stream S, generated from the same secret key K, to get the plaintext M.

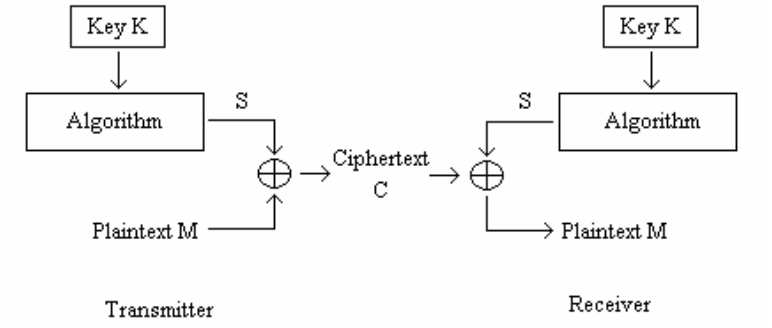

Figure 2. Stream ciphering mechanism.

3.2.2 Block ciphering mechanisms

In block ciphering mechanisms, the plaintext is encrypted grouping the symbols in blocks of two or more elements [15]. The main characteristics of block ciphering mechanisms are:

- The encryption of each symbol depends on the adjacent ones.
- The encryption of a group of symbols is always done by the same way.
- Two equal messages, encrypted under the same key, will produce the same ciphertext.
- It is not necessary to decrypt a complete message in order to get a piece of the plaintext.

The disadvantage that presents block ciphering, in comparison with stream ciphering, consists in the manipulation of long arrays of bits and high processing capabilities. Block ciphering has very little application in RFID systems [10].

4. PROPOSED SECURITY LAYER

In this section we describe the proposed security layer for solving the security problems in RFID systems. This proposal covers the air interface, the data frame, the authentication protocol and the encryption algorithm.

4.1 Air interface

RFID systems are radio systems that work in frequencies within unlicensed bands. Unfortunately, at the present time, a general consensus on the operation of this technology does not exist since each manufacturer designs proprietary systems. The work reported in this paper proposes the operation of RFID technology in the band of 13.56MHz in order to comply with the national regulations existing in the United States and Japan [10]. The operation mode chosen is half-duplex using FSK modulation. This mode is chosen because the active tags used in this proposal are always connected to their own power source, allowing them to have enough energy to process data.

4.2 Data frame

Information is transferred between tags and the reader using data frames of 120 bits (see Fig. 3), of which 80 correspond to the payload of transmission and 40 to control traffic. Each frame has a 4 bits sequence to determine the header of the frame, SOF (*Start Of Frame*) and other to determine the trailer, EOF (*End Of Frame*). The SOF sequence is specified by bits “1101” whereas the EOF sequence is specified by bits “1011”. The length of these fields was determined in order to limit the control traffic and increase the transmission efficiency. There is a 32 bits field of CRC (*Cyclic Redundancy Check*) to provide error detection in message transmissions. The CRC-32 is defined by the polynomial $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ [10].

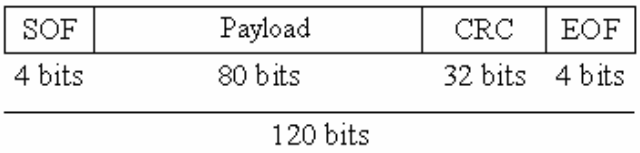

Figure 3. Data frame.

4.3 Authentication protocol

The authentication scheme chosen in the security layer is the mutual authentication based on a three-way handshaking model [12] which is an implementation of a *Simple Authentication and Security Layer (SASL)* protocol as specified in RFC 2222 [16]. In this approach, none of the communicants will receive any secret information during the authentication process. This peer-to-peer authentication service provides the calling entity with a high assurance that the connection has been established with the addressed peer entity. By this way, the first attack in RFID systems, unauthorized reading of the information stored in tags, can be neutralized. Furthermore, tag tracking is prevented since the tag would not respond at all to a query sent out by a reader that does not know the secret key.

The authentication protocol is shown in Fig. 4 and Fig. 5. Reader A has a data base of all the private keys from each user K_X. When the reader tries to establish a communication with tag B, it sends its identification number ID_A and a private session key K_S, both encrypted under the secret key K_B, together with a random number r_1 encrypted under the session key. Only entity B is able to decipher the message to obtain K_S and ID_A, which tells B that the source of the message is A. With the decryption of this message, the key establishment stage is completed and both A and B are in possession of the session key. Next B obtains the random number r_1 by decipherment using K_S. Tag B takes r1 and sends it back with another random number r_2, both ciphered under K_S, to establish a mutual authentication. The appearance of r_1 in the message authenticates B to A. Finally, A authenticates itself by sending back the random number r_2. If all the steps are successfully carried out, the mutual confidence is sufficient to

enable communication, encrypted under K_S. In this way, tag B identifies itself by sending ID_B which is the information that the reader provides to the application.

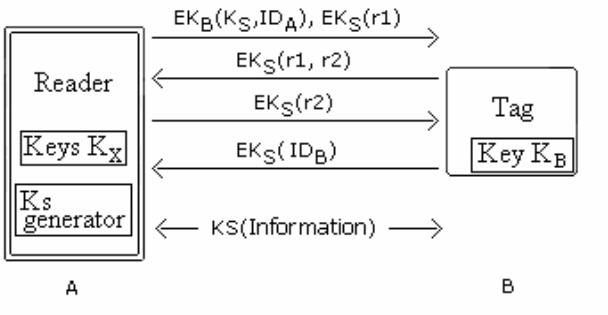

Figure 4 Proposed authentication protocol.

The information exchanged by the tag and the reader is embedded into the data frame shown in Fig. 3. Fig. 5 provides a more detailed view of the information exchange. Note that the second and third step of the authentication process leaves unused bits (indicated by X). For an example of the process, see Section 6 and Tables 1-4.

First step:

SOF	K_s	ID_A	r_1	CRC	EOF
4 bits	64 bits	8 bits	8 bits	32 bits	4 bits

Second step:

SOF	r_1	r_2	X	CRC	EOF
4 bits	8 bits	8 bits	64 bits	32 bits	4 bits

Third step:

SOF	r_2	X	CRC	EOF
4 bits	8 bits	72 bits	32 bits	4 bits

Fourth step:

SOF	ID_B	CRC	EOF
4 bits	80 bits	32 bits	4 bits

Figure 5 Detailed view of the authentication protocol.

4.4 Encryption algorithm

The architecture and limited hardware resources of RFID tags suggest the use of symmetric-key encryption methods, especially stream ciphering. The algorithm chosen to implement encryption in the system is RC4, that is, one of the most used stream ciphers [17]. This algorithm is chosen because it is simple, fast and easy to implement. By this way, the second attack in RFID systems, eavesdropping transmissions with the purpose of successfully obtaining information, can be neutralized. Note that the

implementation of RC4 requires only memory, adders and registers and, therefore, it is possible to adopt the algorithm in a low-price RFID tag.

The RC4 algorithm was designed by Ron Rivest in 1987 and was kept as a secret until 1997 when an anonymous description was published on the web [17]. Many cryptanalysts assure that using RC4 lead to insecure cryptosystems but, in practice, it has been demonstrated that those cryptosystems have an acceptable security level. This algorithm generates a pseudorandom stream of bits called keystream. In the encryption process, it is combined with the plaintext using XOR, and in the decryption it is combined with the ciphertext. The keystream is generated from a permutation of all 256 possible bytes. This permutation is initialized with a variable length key which in our proposal fits to 64 bits,using the KSA (*Key-Scheduling Algorithm*) algorithm. Once the permutation is done, the stream is generated using the PRGA (*Pseudo-Random Generation Algorithm*) algorithm [17]. The KSA algorithm which is used to initialize the permutation in an array S, is described as follows.

1) Array S is initialized with the identity permutation.
for i from 0 to 255
S[i]=i

2) Array S processed 256 times.
for i from 0 to 255
j=(j+S[i]+key[I mod key_length]) mod 256
swap(S[i],S[j])

The PRGA algorithm generates one byte from the keystream so it must be executed as many times as needed in order to get a stream within the desired length. The steps of the algorithm are:

1) Each execution increments counter i, and the new value of counter j is computed by adding the current value of j with the value of S indexed by i.

$$i := (i + 1) \bmod 256$$
$$j := (j + S[i]) \bmod 256$$

2) The values of S indexed by i and j are swapped.

swap (S[i],S[jj])

3) The output generated corresponds to the value of S indexed by (S[i]+S[j]).

$$output\ S[(S[i] + S[j]) \bmod 256]$$

One of the advantages of using RC4, instead of other stream ciphers, is its software implementation because it requires only byte-length manipulations. In the hardware implementation, it requires only memory modules, byte-length adders and registers [17]. One of the vulnerabilities of the RC4 algorithm consists in the fact that the keystream generator is slightly biased in favor of certain sequences of bytes [17]. RC4 does not take a separate nonce alongside the key. Such a nonce is a requirement for security so that encrypting the same message twice produces a different ciphertext each time. A secure solution to this that works for any secure cipher is to concatenate the key and a nonce. By this way, a 64 bit-length dynamic key K_K is generated from an 40 bit-length static key K and a 24 bit-length initialization vector IV, as it is shown in Fig. 6.

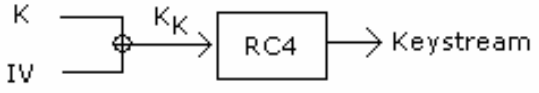

Figure 6. RC4 with dynamic key.

This cipher scheme is the one used in WLANs (*Wireless Local Area Networks*), also known as WEP [8]. This encryption mechanism has a vulnerability, which consists in the transmission of the initialization vector IV in plaintext concatenated with the ciphertext (see Fig. 7). As mentioned previously, many new protocols have been proposed like WPA, WPA2, RSN and 802.11i to solve the vulnerabilities issues of the WEP protocol; however, these standards, and especially 802.11i, need hardware renew and reconsideration of security architecture [8], [9]. As a result, in this paper we propose to modify the existing WEP protocol to make it more secure.

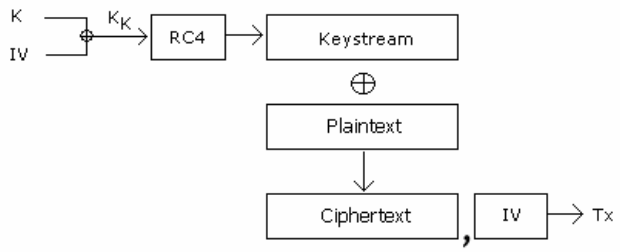

Figure 7. Wired Equivalent Privacy (WEP) protocol.

In order to neutralize the WEP security problem, we consider not transmitting the initialization vector; instead, we generate it in each entity in the communication system (see Fig. 8). That is, the generation of the IV is done by a lineal increment of its value for each data frame transmitted, and accordingly we obtain different values for the dynamic key K_K. Note that a somehow similar approach has also been reported in [9] in which the idea is to update the shared secret key based on factors like network traffic and number of transmitted frames, and the results have shown that the proposed modification to the existing WEP protocol makes it more secure and robust in terms of message privacy [9].

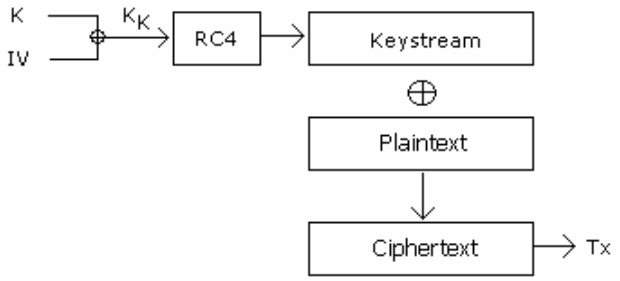

Fig. 8. Modified WEP protocol.

The generation of the IV may be also randomly done, taking part of the keystream generated in the last encryption. However, this approach is not as secure as the aforementioned, because the probability of generating the same dynamic key K_K for two different messages is high, thus the first perfect secrecy condition defined by Shannon would be broken.

5. HARDWARE IMPLEMENTATION

In this section we present the hardware implementation of the proposed security layer for RFID systems. Implementing the security layer with the extensions for encryption and authentication requires some considerations concerning the architecture of an RFID tag. RFID seems to be the future of next generation networks, but this will be only possible if the cost of implementation declines. Hence the architecture of tags must be simple enough to reduce manufacturing costs. In order to see the

robustness and effectiveness of the security layer in a real system, we implemented it using VHDL in FPGAs communicated through RF transceivers.

One of the great advantages that VHDL has is the fact that the design of the systems can be made in a modular way. The modular design consists in dividing the main system in components in order to create subsystems specialized in certain tasks. The block diagram in Fig. 9 shows the main components of the designed system. The control unit is responsible for commanding the operation of the other modules. The communication unit is responsible for carrying out the communication protocol, which involves user authentication and data coding. The cryptographic unit is responsible for executing the ciphering algorithms, providing the communication unit with the messages encrypted. The configuration unit is responsible for configuring the transceivers used to implement the air interface. The port unit is responsible for linking the FPGA with the transceiver.

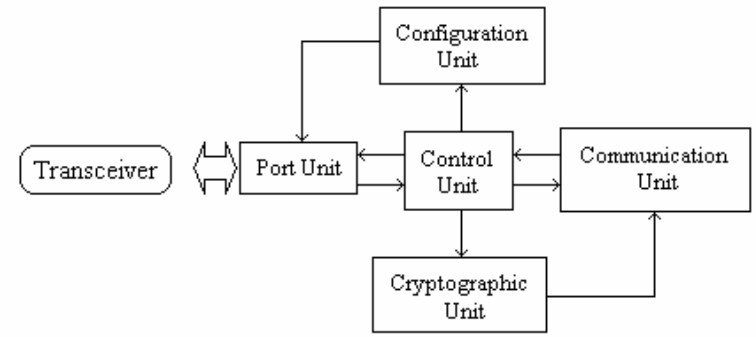

Figure 9. System block diagram.

The FPGA used for the implementation is the Xilinx xc3s200 model, from the Spartan3 family. The transceiver used for the air interface is the Atmel AT86RF211DB model. The system is implemented using two FPGAs, communicated through RF transceivers, which simulates the behavior of an RFID network composed by a reader and a tag (see Fig. 10).

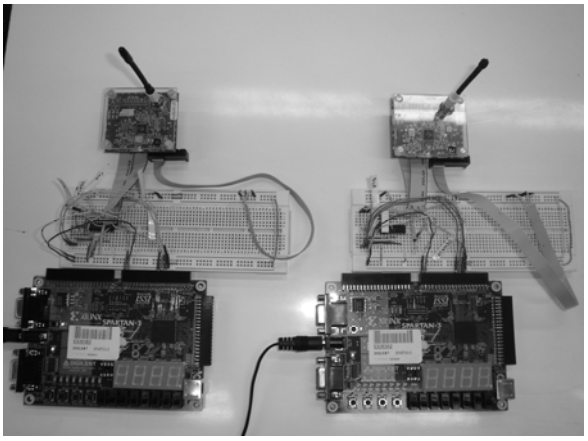

Figure 10. Hardware implementation of the proposed security layer for RFID systems.

The implementation of this modified WEP protocol can be realized very economically on FPGAs using a number of 192 gates like shown in similar approaches [18]-[20]. It is important to note that the low cost demanded for RFID tags causes them to be very resource limited. In general, they can only have between 5000 and 10000 logic gates [6]. Within this gate counting, only between 250 and 3000 gates can be committed to security functions. Note that encryption algorithms like Data Encryption Standard

(DES) or Advanced Encryption Standard (AES) require more than 20000 gates to be implemented [6]. Furthermore, power restrictions should be taken into account, since most RFID tags in use are passive [6], [7].

6. EXPERIMENTAL RESULTS

The experimental results of the proposed security layer for RFID systems are reported in this section. The operation of the system implemented is carried out under the following circumstances:

- Symmetric- key K_B - 0x1736001002FF4AA0
- Session key K_S - 0x2386AB420011FF00
- Reader identifier ID_A - 0x01
- Tag identifier ID_B - 0x03

As described in Section 4, the authentication mechanism is composed by 4 stages. In the first stage, the reader sends a 120 bits frame composed by the session key K_S, the reader identifier ID_A, a random number r_1 and the CRC field. The session key K_S and the reader identifier ID_A are encrypted under the symmetric-key K_B. On the other hand, the random number r_1 and the CRC are encrypted under the session key K_S. The plaintext and the ciphertext of this message are shown in Table 1.

	SOF	K_S	ID_A	r_1	CRC	EOF
Plaintext	D	1736001002FF4AA0	01	01	D845A29B	B
Keystream	-	D8A37B1D58F4619F	FD	40	0A0EF438	-
Ciphertext	D	CF957B0D5A0B2B3F	FC	41	D24B56A3	B

Table 1. Information sent in the first authentication stage

In the second stage, the tag sends a frame composed by the random number r_1 and another random number r_2. This frame is encrypted under the session key K_S (see Table 2).

	SOF	r1	r_2	X	CRC	EOF
Plaintext	D	01	02	0000000000000000	6050E91C	B
Keystream	-	C4	5B	69F17B40010475D6	4EIEE1E1	-
Ciphertext	D	C5	59	69F17B40010475D6	605E08FD	B

Table 2. Information sent in the second authentication stage

In the third stage, the reader sends back the random number r_2, which is encrypted under the session key K_S. The plaintext and the ciphertext of this message are shown in Table 3.

	SOF	r_2	X	CRC	EOF
Plaintext	D	02	000000000000000000	05E05D79	B
Keystream	-	A2	24C612D07F702AB106	E1E16E41	-
Ciphertext	D	A0	24C612D07F702AB106	E4013338	B

Table 3. Information sent in the third authentication stage

In the last stage the tag sends its identification number ID_B, which is encrypted under the session key K_S. The plaintext and the ciphertext of this message are shown in Table 4. If the reader has this identification number in its database, the tag is authenticated and identified as an authorized user. If the perfect secrecy conditions constituted by Shannon are established, there is no way to deduce the encryption key from the ciphertext. The implemented system is a symmetric-key system; therefore, the only way to break the security layer is by obtaining the encryption key in the key distribution process.

	SOF	ID_B	X	CRC	EOF
Plaintext	D	03	000000000000000000	8570FD1E	B
Keystream	-	BO	CC29DB8738F0E67970	BEAEC439	-
Ciphertext	D	B3	CC29DB8738F0E67970	3BDE3927	B

Table 4. Information sent in the fourth authentication stage

Even if an intruder has the encryption key, the counterpart will suspend any communication if it is not identified in a proper way. There are two possible attacks in this system: an unauthorized reader or a fake tag. If an unauthorized reader tries to get information from a tag, the latter will not provide any information if the reader does not identifies itself by providing an authorized identification number ID_A. If a fake tag tries to gain access to a private system, it will not succeed if the security system does not find its identification number ID_B in a database. Note that the problem of sharing the keys between readers and tags while avoiding eavesdropping could be solved by using public/private keys. Since active tags provide more processing power, the more complex public key algorithms could be used by this protocol. The overhead of the protocol and therefore the general transmission speed can be adapted by reducing the length of the CRC. The proposed 32 bit–CRC should be regarded as an upper bound and can be changed accordingly to application needs.

7. CONCLUSIONS

Due to the fact that RFID systems are becoming so popular in data networking, it is therefore necessary to consider the security issues that come out from its implementation or design of new applications and systems. These problems are related to data privacy, integrity and secrecy. The security layer reported in this paper is designed with user authentication and encryption algorithms. The chosen authentication scheme is the mutual authentication protocol. By this way, the first attack in RFID systems, unauthorized reading of the information stored in tags, can be neutralized. The algorithm for encryption is RC4 implemented in a modified WEP protocol and the implementation results of this algorithm are comparable with the ones reported in [18]-[20]. In this new approach, the initialization vector is not transmitted; therefore, it is generated in each entity. That is, the generation of the IV is done by a lineal increment of its value for each data frame transmitted, and accordingly we obtain different values for the dynamic key K_K. By this way, the second attack in RFID systems, eavesdropping transmissions, can be neutralized. Note that the low cost demanded for RFID tags causes them to be very resource limited and

therefore encryption algorithms like DES or AES that require more than 20000 gates are not practical. Furthermore, power restrictions should be taken into account since most RFID tags in use are passive [6], [7]. Finally, an extension of the work presented in this paper could be the implementation of an RFID network considering anti-collision protocols.

8. REFERENCES

[1] Weis, A. S., Security and Privacy in Radio-Frequency Identification Devices, Master Thesis. MIT, 2003.

[2] Garfinkel, S., A. Juels and R. Pappu., RFID Privacy: An Overview of Problems and Proposed Solutions, IEEE Security & Privacy. May/June 2005, pp. 34-43

[3] Landt, J., The History of RFID, IEEE Potentials, October/November, 2005, pp. 8-11

[4] Feldhofer, M., A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags, Institute for Applied Information Processing and Communications - Graz University of Technology, Austria. February 2004.

[5] Juels, A, RFID Security and Privacy: A Research Survey, IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, , February 2006, pp. 381-394

[6] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda, A., RFID Systems: A Survey on Security Threats and Proposed Solutions, in 11th IFIP International Conference on Personal Wireless Communications – PWC06, LNCS 4217, Springer, 2006, pp. 159-170

[7] Rotter, P., A Framework for Assessing RFID System Security and Privacy Risks, IEEE Pervasive Computing, Vol. 7, No. 2, April-June 2008, pp. 70-77

[8] Hassan, H. R., and Challal, Y., Enhanced WEP: An Efficient Solution to WEP Threats, IEEE 2nd IFIP International Conference on Wireless and Optical Communications Networks, WOCN 2005, March 2005, pp. 594-599

[9] Purandare, D. S., Enhancing Message Privacy in WEP, Master Thesis, Department of Computer Science, University of Central Florida, USA, 2005.

[10] Finkenzeller, K., RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd. ed. Trad. Rachel Waddington. West Sussex: John Wiley & Sons Ltd., 2003.

[11] Oppliger, R., Authentication Systems for Secure Networks. Massachusetts: Artech House, 1996.

[12] Muftic, S., Security Mechanisms for Computer Networks. West Sussex: Ellis Horwood Limited, 1989.

[13] Purser, M., Secure Data Networking. Massachusetts: Artech House, 1996.

[14] Fúster, A., Técnicas Criptográficas de Protección de Datos, 2nd. ed. Mexico: Alfaomega, 2001.

[15] Stinson, D., Cryptography - Theory and Practice, Chapman & HALL/CRC, 2002.

[16] Myers, J., RFC 2222: Simple Authentication and Security Layer (SASL), October 1997. Status: Proposed Standard. Updated by RFC2444.

[17] L. R. Knudsen, W. Meier., B. Preneel., V. Rijmen and S. Verdoolaege, Analysis Methods for (Alleged) RC4, LNCS 1514, Springer-Verlag, Berlin, Germany, ASIACRYPT 1998, pp. 327-341.

[18] Kitsos, P., Kostopoulos, G., Sklavos, N., Koufopavlou, O. Hardware Implementation of the RC4 Stream Cipher, in Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems, MWSCAS 03, Vol. 3, December, 2003, pp. 1363-1366.

[19] Hämäläinen, P., Hännikäinen, M., Hämäläinen, T., Saarinen, J., Hardware Implementation of the Improved WEP and RC4 Encryption Algorithm for Wireless Terminals, the European Signal Processing Conference (EUSIPCO 2000), 2000.

[20] Galanis, M., Kitsos, P., Kostopoulos, G., Sklavos, N., Goutis, C., Comparison of the Hardware Implementation of Stream Ciphers, The International Arab Journal of Information Technology, Vol. 2, No. 4, October 2005, pp. 267-274.

Authors Biography

Vicente Alarcon Aquino

Received the B.Sc. degree from the Instituto Tecnológico de Veracruz in 1991, the M.Sc. degree from the Instituto Nacional de Astrofísica Optica y Electrónica in 1993, and the Ph.D. and D.I.C. degrees from Imperial College London, London UK in 2003, all in Electrical Engineering. From 1993 to 1998, he was an Assistant Professor in the Department of Electrical & Electronic Engineering at the Universidad de las Américas, Puebla, Mexico. From 1998 to 2000, he was a Laboratory Demonstrator in the Communications and Signal Processing Laboratory at Imperial College London, UK. Currently, he is Titular Professor and Coordinator of Postgraduate Studies in the Department of Computing, Electronics and Mechatronics at the Universidad de las Américas Puebla, Mexico. His research interests include wavelet theory applied to communication networks, network security, intrusion detection and monitoring, and path restoration in MPLS networks. He has authored several technical publications published in conference proceedings and journals and has been an invited speaker at many national conferences. Dr. Alarcon-Aquino has served as member of technical program committees and as technical reviewer for several journals and national and international conferences. He is a member of the IEEE and author of the book "Introducción a Redes MPLS" (in Spanish) Editorial: El Cid Editor 2007.

Miguel Dominguez Jimenez

Works as an Operation Supervisor at TELMEX Mexico *Teléfonos de México* and is responsible for the coordination and supervision aspects of installation and maintenance of telephone lines, including voice and data services. He received his B.E. summa cum laude in Electronics and Communications from the Universidad de las Américas-Puebla, Mexico in 2006. He received the “Best average grade among Bachelors of Engineering in Electronics and Communications” and the “Best student of the Science and Engineering School” awards in 2007 from his alma mater as well as the “Best Bachelor of Engineering of 2007” award from ANFEI *Asociación Nacional de Facultades y Escuelas de Ingeniería* in 2008. After receiving the B.S., he joined Nortel Networks as a project engineer in wireless and wireline engineering and was involved in network core design in carrier voice over IP solutions. He then received an invitation to join a school of management course of Tenaris University in the Universidad Austral in Buenos Aires, Argentina. In September 2007, he accepted a project engineer position in TELMEX Mexico, where he worked in the implementation of a CDMA Network for rural telephony. His areas of interest are networking, wireless communication systems, communication systems security and project management. He has the CCNA certification from Cisco Systems and the CWNA certification from Planet3 Wireless.

Christian Ohms

Is a recent graduate from the University of Applied Sciences in the city of Kiel, Germany, with a diploma degree in Electrical Engineering. His fields of study were communication technology in general, telecommunication protocols like ISDN, GSM, UMTS, WLAN and WiMax, digital signal processing, microprocessors as well as programmable logic and digital circuits. During his scholastic career, he additionally worked part time as a technical consultant in the customer care department of a major German Internet provider. Within the scope of a student exchange, he stayed for one year and a half in Mexico at the Universidad de las Américas (UDLA) in the city of Puebla. There, he worked as a research assistant being involved in the fields of security algorithms applied to RFID devices under the guidance of Prof. Dr. Vicente Alarcon-Aquino. In continuation of his work at the UDLA, he discussed the development of a VHDL version of the "Tiger" hash algorithm and its implementation on an FPGA device in his thesis, presenting this work in July 2008. After having finished his studies in Germany, Christian Ohms is now focusing on his professional career as an Electrical Engineer.