WHITE PAPER SERIES / EDITION 1

AUTO–ID LABS

BUSINESS PROCESSES & APPLICATIONS
SOFTWARE & NETWORK
HARDWARE

AUTOIDLABS-WP-SWNET-013

Low-Cost RFID Systems: Confronting Security and Privacy

Damith C. Ranasinghe[1], Daniel W. Engels[2], Peter H. Cole[3]

[1]Auto-ID Labs, School of Electrical & Electronic Engineering, University of Adelaide
Adelaide SA 5005, damith@eleceng.adelaide.edu.au

[2]Auto-ID Labs, Massachusetts Institute of Technology, 77 Massachusetts Avenue, NE-46, Cambridge, MA 02139 USA, dragon@csail.mit.edu

[3]Auto-ID Labs, School of Electrical & Electronic Engineering, University of Adelaide
Adelaide SA 5005, cole@eleceng.adelaide.edu.au

Abstract
In the implementation of Radio Frequency Identification (RFID) systems concerns have been raised regarding information security and violations of end-user privacy. There is a large collection of literature available on efficient and inexpensive cryptographic engines, but they are still extravagant solutions for low cost RFID systems. Security and privacy provided by low cost RFID is both directly and indirectly limited by a number of factors that are unique to low cost RFID. This paper examines security and privacy issues regarding RFID and presents the challenges that arise in view of the unique environment presented by low cost RFID systems.

1. Introduction

A. Brief Overview

This paper focuses on examining and illuminating the problems encountered in providing low cost solutions to ensure security and privacy for low cost RFID systems.

The RFID systems consist of three primary components:

- RFID labels (transponder)
- RFID label readers or interrogators (transceiver)
- Application systems.

Interactions of these components are outlined in Figure 1.

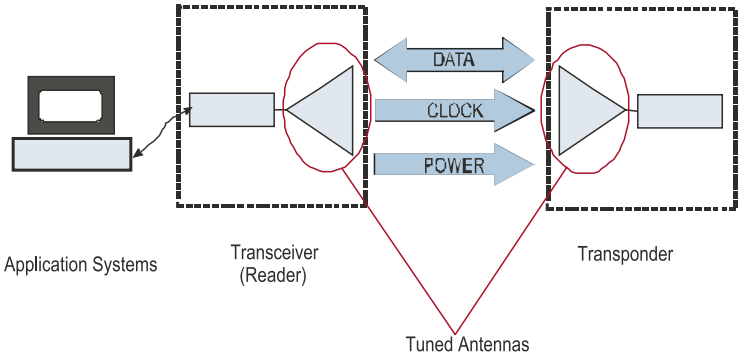

Fig. 1: A high level illustration of RFID component interactions.

Generally, an RFID label consists of a small microchip with some data storage and limited logical functionality, and an antenna. The antenna allows the label to couple to an electromagnetic (EM) field to obtain power or to communicate with the reader or to do both.

RFID labels can be distinguished based on their frequency of operation (HF or UHF), or on powering techniques (active, passive, or semi-passive). Passive labels have no power source of their own and therefore must rely on the EM field created by a reader. Passive labels normally communicate information to a reader by modulating the reader's RF signal (load modulation or backscatter). Hence, these labels fall on to the low cost end of the RFID labels.

The data stored on the label may contain an Electronic Product Code (EPC) [1,2], which is a unique item identification code. An EPC typically contains information that identifies the manufacturer, the type of item and the serial number of the item. This information is also referred to as a label ID. As identified in table 1 below, there are four fields in the Electronic Product Code. They are, in order, a header, defining the variety of EPC among a number of possible structures; a domain manager number (effectively a manufacturer number); an object class (equivalent to a product number); and a serial number.

EPC Type	Header Size	First Bits	Domain Manager	Object Class	Serial Number	Total
256 bit	8					
96 bit	8	00	28	24	36	96
64 bit type I	2	01	21	17	24	64
64 bit type II	2	10	15	13	34	64
64 bit type III	2	11	26	13	23	64

Table 2: Description of ECS types (recreated from [1])

The readers communicate with the labels using a radiofrequency interface. Either a strong energy storage field near the reader antenna, or radiating EM waves, establishes the RF interface. Communication between a reader and a label process may involve interrogating the label to obtain data, writing data to the label or beaming commands to the label so as to affect its behaviour. The readers consist of their own source of power, processing capability and an antenna. The readers are generally connected to a back end database (as outlined in Figure 1).

The application systems are used to collect data aggregated through readers and the electronic database software uses the data for various purposes. A comprehensive treatment of RFID systems is covered in [1].

B. Low Cost RFID

The current cost of a gate of silicon logic is about one thousandth of a cent [3]. Today, the cheapest RFID labels are passive and cost around 20 US cents [26], in quantities greater than one million. Presently these low cost RFID chips occupy about $0.16(mm)^2$ to $0.25(mm)^2$ [4] of silicon.

Among the hierarchy of RFID labels, the AutoID Centre, now AutoID Labs [5] proposed a Class hierarchy for RFID labels (Figure 2). Class 1 and II represent the low cost end of RFID labels. Class 1 labels have only a read only memory while Class II labels may have some read-write memory. The following sections provide a brief overview of low cost RFID label manufacturing costs, which places a significant constraint on an implementation of a security mechanism.

C. Manufacturing Costs

There are a number of key stages involved in the manufacture of RFID labels after the design of the IC. An outline of the stages is given in Figure 3. Currently the labels falling into the Class I category consist of ICs that costs about 10 US cents [4], the

antenna manufacture to the assembly stage costs around 5 US cents [6], [3] and packaging costs are around 10 US cents [3]. Presently 10 US cents RFID read only chips have design sizes ranging from 0.16(mm)^2 [7] to 0.25(mm)^2 [6]. However these costs will be dramatically reduced by large RFID label orders.

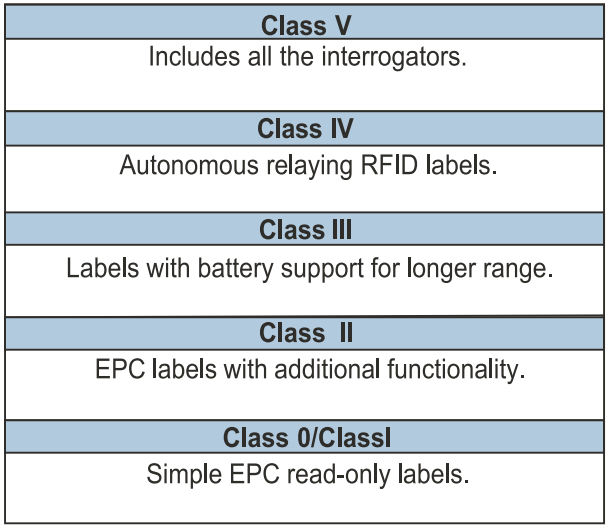

Fig. 2: RFID Class hierarchy

Further improvements to IC manufacturing processes will also bring the cost of the microcircuit even lower. This invariably involves producing more microcircuits per silicon wafer. An instance of such an advancement is a process called wet etching [3]. This process allows the silicon wafer yield to increase by around 10 fold.

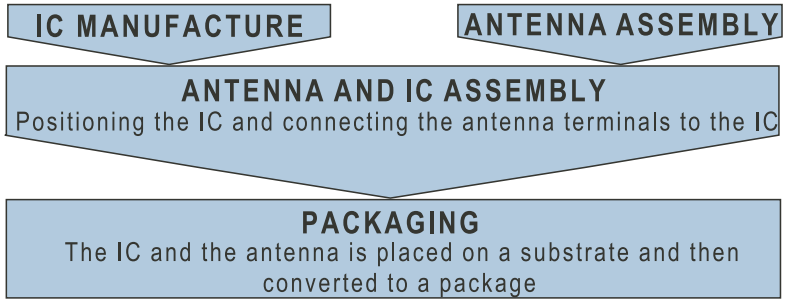

Fig. 3 RFID Label Manufacture

D. IC Components

An RFID microcircuit can be, as discussed below, subdivided into three primary sections: memory, power and label logic circuitry. Current fabrications of Class I labels consist of around 1000 to 4000 logic gates [2] while Class II labels may have several thousand more gates.

Memory: The IC has memory capacity in the order of one or more hundreds of bits. Class 1 labels have read only or write once and read many times memory, while class II labels may have some read-write memory.

Logic: The logic on board the chip will define the label functionality. Primarily, chip logic will execute reader commands and implement an anti-collision scheme that allows the reading of multiple labels by a reader. These logic circuits are highly specialised and optimised for their tasks.

Power: Passive RFID chips consist of a rectifier and a storage capacitor, which is used to store and power the circuit in the

absence of a battery. It is important to note here that the capacitor occupies a relatively large portion of the silicon area, and RFID chips consuming larger amounts of power will need higher capacity capacitors and thus will cost more. When all practical considerations are taken into account, present RFID chips require about 150 microwatts of power to operate. Thus, the power consumption of an encryption engine is an important consideration.

E. Frequencies and Regulations

Regulatory bodies around the world govern the operating frequency, radiated power, and bandwidth used for various purposes in different regions of the world. Most RFID systems operate in the Industrial, Scientific and Medical (ISM) bands designated by the ITU [27]. The most commonly used High Frequency (HF) ISM band in Europe and America is centred at 13.56MHz and the UHF band in the US is 902-928MHz [8,9].

Each frequency band provides its own set of advantages and disadvantages. The 13.56 MHz band has a 14KHz powering bandwidth while signalling occupies a greater bandwidth but is implemented by shallow and infrequent reader modulations, producing low amplitude sidebands. For this band typical reading ranges of RFID labels are around 30cm to 50 cm because they operate in the near field [1].

The 902-928 MHz band, under US regulations, allows multiple reader to label communication choices. The regulations allowing the longest communication range require the reader to change its communication frequency every 400 milliseconds. The reader may hop between a stipulated numbers of channels, however the maximum bandwidth of a channel cannot exceed 500 kHz [9]. The technique is referred to as frequency hopping. Because they operate in the far field, because a radiated power of 4W is allowed and because antenna impedances are suitable for matching to the IC circuits, passive UHF RFID labels have reading distances of around 3m to 5m.

It is important to understand the factors contributing to low RFID costs and the limitations placed on these low cost labels before considering the subject of security and privacy. The following sections will consider security and privacy issues that arise from mass utilization of RFID labels and the challenges that are unique to alleviating those concerns.

2. Security and Privacy Issues

RFID systems, similar to other wireless technology, display a number of security and privacy risks to users; both the consumers and the manufactures. The following sections take a closer look at the security and privacy threats created by the use of RFID systems.

A. Security and privacy risks

It is important to define the term ‘security’ and ‘privacy’ in the context of RFID. In terms of RFID, security refers to one or a combination of the following:

- ‘Confidentiality’ or message content security
- Integrity of message content
- Authentication of the Sender and Recipient
- Non-repudiation by the Sender and Recipient, and
- Availability [10].

It is important to note that privacy is a multi dimensional issue involving many areas such as policies, security and law enforcement agencies. A guide to defining privacy can be found in [11]. A criteria for evaluating a RFID system’s privacy implies providing

- anonymity, and
- and unlinkability.

While RFID technology provides numerous benefits, RFID systems generate new risks. Primarily, the communication between the labels and the readers is exposed to eavesdropping and traffic analysis. Thus, an RFID system is constantly under threat from man in the middle attacks, whereby a third party may monitor a conversation between a label and a reader to obtain sensitive information. Illicitly obtained information in this manner may be used to create fake labels, unauthorised readers, or used to discover secret information stored on labels (such as an authentication code).

There is presently no mechanism for a reader to authenticate itself to a label or a label to authenticate itself to a reader. Thus labels and readers are constantly in an un-trusted environment that lacks confidentiality and the integrity of the messages is doubtful, there are no means for establishing nonrepudiation by the readers or the RFID labels.

In addition, the labels themselves are exposed to physical attacks. An adversary may simply use physical attacks to reverse engineer labels to create fake labels for spoofing (see below) or creating many labels to initiate a DOS (denial of service) attack [12], thus raising concerns regarding availability.

Spoofing (imitating the behaviour of a genuine label) presents a serious threat to an RFID system. Spoofing will add a new dimension to thieving. A thief may replace a valid item with a fake label or replace the label of an expensive item with that of a fake label with data obtained from a cheaper item. Thus the lack of a means for authentication allows an adversary to fool a security system into perceiving that the item is still present or this may fool automated checkout counters into charging for a cheaper item. Fake labels may also be used to create imitation items. Thus it is important to be able to authenticate labels to establish their legitimacy.

An adversary may initiate a DOS attack to bypass or avoid security systems. A DOS attack is easily carried out by placing a large number of fake labels for identification by a reader. Persons may also have the ability to disrupt an RFID system implementation by destroying or corrupting a large batch of labels. Labels are also vulnerable to protocol attacks. Hence, labels may be repeatedly asked to perform an operation, thus making them unavailable to an authorised reader. Labels clearly need to be able to defend against such simple brute force attacks as this raises concerns regarding system availability.

Another avenue for attacking an RFID security mechanism might be a physical attack on an RFID label or a reader to discover the label ID. Thus, providing an adversary with adequate information to perhaps, create imitation goods of expensive items in large quantities.

There is also a clear possibility for unauthorised interrogators to read label contents from unprotected RFID labels due the lack of a mechanism for authentication. Unauthorised readers may be used to violate “anonymity” or “location privacy” by accessing labels with no access control [12]. Even if labels are protected, a traffic analysis attack (or using predictable label responses) may be used. Hence an individual with a number of labelled items may be scanned by a third party to either identify the individual or reveal his or her location or provide valuable data to market researchers or thieves in search of wealthy victims. Similarly, competitors of an organization (such as a rival supermarket) may over time scan another organizations inventory labelled with RFID labels over time or eavesdrop on the organization’s own valid operations to obtain valuable information, such as sales data, to ascertain the performance of its competitors [13].

A further privacy concern resulting from RFID labelled items carried by an individual is posed by the possibility of tracking, albeit with technical difficulty, individuals (violation of "unlinkability"). Correlating data from readers obtained from multiple locations can reveal the movement, social interactions or financial transactions of an individual. Even if a security protection is applied to the data on a RFID label, individuals may be tracked through a "constellation" of predictable label responses. Hence, a person's unique taste in items may betray their location, movements, or identity.

Privacy issues generated by RFID are also partially a policy issue as the mechanisms used to ensure security and privacy are most effective when implemented in conjunction with a well-formed policy. However, there are already existing privacy polices that can be applied directly in the context of RFID [21]. They may however need to be clarified, refined or amended to make them more suitable to RFID Systems. An example of such a public policy formulation is the "Bill of Rights" [20]

Major issues that must be dealt with in policy formulation are those generated by

- Unique Identification of all label items
- Collection of information (who collects, how do you use it, ownership of that information)
- Dissemination of that information, and
- Mass utilization of RFID technology.

It is important to note that existing barcode systems have many of the same risks; they can be read by a simple bar code reader, can be destroyed easily, and can be spoofed, however they do not have the potential for these operations to be performed wirelessly and apparently unobtrusively on an immense scale.

B. Challenges to RFID Security and Privacy

There are many challenges to providing security and privacy for low cost RFID systems (Table 2). These difficulties are a result of the nature of electromagnetic waves and the constraints placed upon RFID systems.

Challenge	Description
Cost	Storage limitation. Silicon area
Regulations	Radiated power, frequency of operations, available bandwidth
Power consumption	Power consumption of the label IC circuit, power required to operate E^2PROM.
Performance	Label performance and system performance goals.
Power disruptions	Sudden loss of power

Table 2: An outline of challenges faced by low cost rfid

The primary challenge lies in the scarcity of resources on an RFID IC. Low cost labels are not self-powered and only consist of a fraction of the gates available on smart cards. Cryptographic systems and protocols need to fit into a label footprint without dramatically increasing the cost of a label. The number of gates available for a security mechanism is in the range of 400-4000 gates.

Security mechanisms and communication protocols need to be carefully designed to avoid leaving the label in a vulnerable state during sudden loss of power or interruptions to communications. It is also important for security mechanisms to take into account the more powerful signal strength of the forward channel (reader to label transmissions) which can be detected hundreds of meters away compared to the tag to reader communication channel which can be received from no greater than 20m using highly sensitive receivers.

EM regulations pose restrictions on the isotropic radiated power at stated distances. This implies that there is a maximum limit

on the power available at a given label distance from a transmitter. Thus, passive labels with size limited by a particular label class or an application are receiving power from a stated power flow per unit area. The power available to the label is one factor contributing to the determination of the type of security scheme and the cryptographic hardware used in a label. Cryptographic hardware consuming considerable power (in the range of tens of microwatts) will severely diminish the label reading distances and degrade the performance of the whole RFID system implementation. Furthermore, a security mechanism employing a memory write will have to account for the additional power required to operate a labels E^2PROM.

UHF regulations for frequency hopping specify a maximum time limit on the use of a frequency channel. This regulation places a severe limitation on a label's transaction time as a label cannot be assumed to be in continuous communications across a frequency hop. This results in a limitation on the time allowed for a transaction between a label and a reader to 400 milliseconds in the US. This is a requirement that must be adhered to in the design of security and privacy mechanisms. Furthermore, user performance requirements establish a time limitation on a label operation since at least 100-300 labels must be read per second.

3. Cryptography

Security and privacy issues concerning RFID are solvable using a set of security mechanisms. A security mechanism is a collective term used to refer to a combination of cryptographic primitives and protocols used to provide security. Hence, it is appropriate to consider the subject of cryptography to examine the range of cryptographic tools available for RFID applications.

A. Cryptographic primitives

Cryptography is an ancient art that has been used throughout the human evolution to provide security and to protect the privacy of individuals or organisations. Providing security and privacy for RFID systems will inevitably involve using some cryptographic primitives already in existence or newly defined along with suitable protocols that take into account the unique nature of RFID systems.

There are numerous cryptographic systems. All of these systems (with the exception of few, such as one-time pads) are based on some mathematically hard problem and the level of security provided by the system will depend on the difficulty of the mathematical problem.

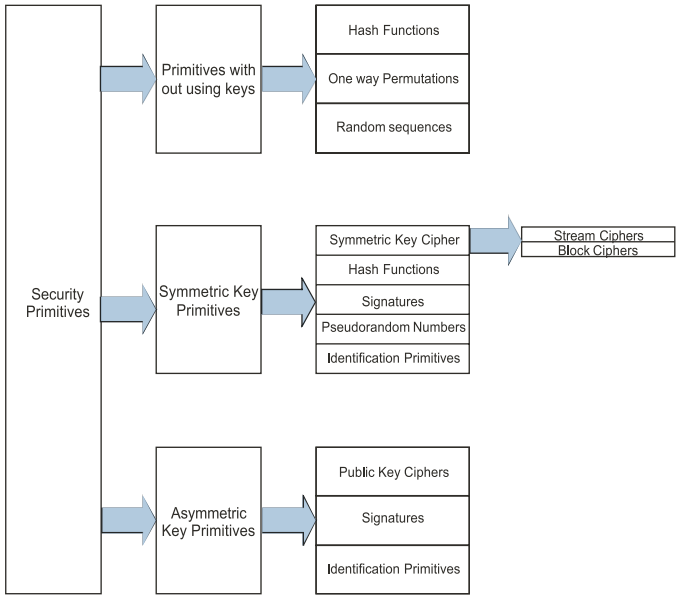

Fig. 4: Classification of cryptographic tools (diagram recreated from [17])

It is important to define the difficulty of a problem before the level of security provided by a cryptographic system can be discussed. A mathematical problem is said to be difficult if the time it takes to solve the problem is immense compared to the size of the inputs to the problem. Modern cryptographic systems are based on mathematical problems where the fastest known algorithm takes exponential time to find a solution. This implies that the time taken to solve the problem increases exponentially as the size of the inputs to the problem increases linearly. Thus the level of security provided by a cryptosystem is often expressed in the number of operation required to break the cryptosystem and the level of security provided by a cipher should compliment the commercial value of the information protected by the cryptographic system. Figure 4 gives a classification of a broad range of cryptographic primitives. A more complete description of these primitives can be found in [28].

B. Level of Security

Many cryptographic systems have been broken because of increased computational resources, development of faster and better algorithms or problems being proved to be easier than when they were first conceived. This is the reality of any cryptographic system. However, the concerning issue is not that the system will eventually be broken, but the range of possible attacks on a security mechanism to breach security.

Most attacks on wireless security schemes range from session hijacking, replay attacks, fault inductions and man in the middle attacks. Other forms of attacks on possible RFID security systems can be gleaned by considering smart card operations. An analysis of smart card operation in hostile environments is presented in [14].

As has been mentioned in Section 2 physical attacks are still possible with protected labels, however, the ability to gain useful information from a protected label is a much more difficult problem. A physical attack on an RFID label or a reader may yield an adversary secret information providing security to an RFID system. A complete overview of possible physical attacks and countermeasures are outlined in [16] while specific lower cost physical attacks are presented in [15].

In addition to the possible attacks mentioned above, there will be specific attacks on the cryptosystem employed by the security mechanism. These attacks are a result of certain weaknesses in the cryptographic scheme or due to certain flaws that may have entered into the protocol employed in the security mechanism.

4. Low Cost RFID and Cryptography

Security and privacy issues concerning RFID are solvable using a set of security mechanisms. However, most of the plethora of available security primitives are too costly to be implemented on an RFID chip with around 4000 gates. For instance, private key cryptosystems such as AES are not suitable, since a commercial implementation of AES typically requires 20,00-30,000 gates [17, 28]. This is far more than the number of gates on an entire low cost label. However the SHA-1 specified by the US Department of Commerce is a possible candidate for an encryption rule but hardware implementations of SHA-1 are also currently too costly to meet the cost budget of low cost RFID labels [12]. Nevertheless, it may be possible to create new hash functions by using existing or new private key cryptosystems.

There have been a number of security schemes outlined in [12 and 18]. A proposed scheme for controlling access to a label uses the difficulty of inverting a one-way hash function [12]. This mechanism can prevent unauthorised readers from reading labels [4].

The primary flaw in this approach lies in the fact that a successful discovery of a MetaID and a label ID pair will allow an adversary to engage in spoofing. The hash locking method requires the implementation of a suitable hash function and the appropriate logic to implement the details of a communication protocol. The greatest challenge lies in the successful implementation of a hardware efficient hash algorithm on the label IC. Since any reader can obtain the MetaIDs from labels, this scheme does not solve the problem of location privacy violations. The scheme is also susceptible to man in the middle attacks since an adversary can query a label, obtain its MetaID, retransmit the value to a reader, and later unlock the label with the reader response.

Randomised access control is another variation of the above scheme described in [4] but with similar flaws and difficulties. It is also not known whether keyed pseudorandom number functions required to implement the scheme are a more efficient hardware implementation than a symmetric key encryption such as a hash function. The hardware complexity of keyed pseudorandom number functions is still an active area of research [16].

The theory of Cellular Automata (CA) [18] developed by Wolfram has been used do develop a number of different cryptographic systems. Cellular Hash (CH) [19] is one such outcome and there is a rich variety of inexpensive encryption mechanism developed based on the chaotic nature of CA system [22,24,26]. CA may be built out of a feedback shift register and a single pair of gates. Thus they provide a compact solution for low cost RFID. In addition, CA based hashes scale well as the size of the hash digest increases but CA hashes require many parallel calculations and thus they may impose considerable demands on a tag's available power. However it is possible to perform CA operation in series but that will be at the expense of RFID system performance.

The CA cryptosystem encountered in CAC by Subhayan Sen [22] presents a rather involved cryptosystem. However the estimated size of the un-optimized pre-layout area is about 4.25mm^2, which is far bigger than a typical RFID silicon design, which is about 0.25mm^2. Even if optimisation halves the design, it is still too extravagant for a low cost RFID chip. However, improvements and a scaling down of the design may be possible since the analysed design was for a 128 bit key. Nevertheless most CA based cryptosystems have been shown to be vulnerable to differential cryptanalysis or have been shown to form an affine group [23].

Use of non linear feed back shift (NLFSR) registers to design a hash by using a complicated feed back function is a possibility since a shift register implementation does not require complex hardware. However an important consideration should be whether the additional cost of a NLFSR provides an adequate security [28].

An important consideration that is often overlooked is the ability for a cryptographic system to use a piece of hardware repeatedly to result in a more secure encryption engine. Most modern UHF RFID chips use on board oscillators with frequencies over 1 MHz. Thus within the operation trimming constraints imposed as a result of US regulations, will allow a tag to expend around 400,000 clock cycles during a 400 millisecond period. Thus, it may be possible to redesign hardware for existing cryptographic primitives to exploit this unique scenario. However, this will be at the compromise of tag reading speeds.

Despite the resource limitations of an RFID label, it will be able to become a party to computationally intensive security system provided that the designer is able to transfer the demanding bulk of the computations to a backend system, such as the reader itself,

or a backend network of computers which may act as a proxy to the security mechanism. In essence it is a transfer of complexity out of the chip onto a shared resource with greater capability to execute the task.

5. Expectations from Class I and Class II Labels

The RFID community, in its efforts towards standardization, has produced a list of end user requirements outlined in the following sections for Class I and II labels. One aim of that list has been to address the privacy and security risks posed by Class I EPC labels. The security requirements are an appropriate guideline for considering the level of security and privacy that can be expected and required from a Class I RFID label.

A. Security requirements for a Class I label

Class I labels should provide a "Kill" capability, so that consumers have the choice of completely disabling an RFID label at the time an RFID labelled item is purchased. This process will eliminate privacy concerns of "anonymity" and "unlinkability". It is being suggested that a password be used to restrict access to the kill command by unauthorised readers.

Class I labels should also have the ability to lock EPC data so as to provide one-time, permanent lock of EPC data on the label, so that EPC data cannot be changed by an unauthorised interrogator once it has been written. Interrogators are also prevented from transmitting complete EPC data except when data needs to be written to an RFID label so that the EPC information may not be eavesdropped upon from a distance without being discovered.

B. Additional security requirements for Class II labels

Other requirements were identified as necessary for higher class labels since these labels will have greater functionality and thus more hardware. These requirements are aimed at providing a secure forward link for communication with an RFID label. These labels should also have the ability to mask label reads while an RFID labelled product is in transit (transport between two locations). The ability to read, write or kill would not be enabled on a masked label unless a predetermined password or another method is used to confirm to the label that an authorised reader is performing the unmasking.

6. Conclusion

Perfect Secrecy is only a mathematical concept; in reality, there will always be a human element that is difficult to quantify into any mathematical formulation. Thus, it is practically impossible to have a perfectly secure system. Once this is understood then it is possible to move onto addressing security and privacy issues shadowing RFID. The paper has identified a lot of security and privacy risks to RFID systems and has discussed many of the methods used for security and privacy in non-RFID contexts. Most of these however, are too area or power hungry to fit well within the limitations of RFID systems and many of the encryption hardware available is for smart card technology. Even though the solutions can be applied directly to RFID, the main obstacle is that smart card processors are much more powerful than a typical RFID label consisting of only 200-4000 gates [4]. Thus, the solutions are not portable to an RFID platform if we expect the cost of the secure labels to remain below the 50 cents mark.

It is evident that RFID privacy and secrity are challenging areas of research. There are a number of specific areas of research which will greatly benefit RFID security and privacy and the outcome of this research will be the wide spread adoption of this technology.

- Cost effective and efficient hardware implementations of symmetric or asymmetric cryptosystems. This may involve finding ways to optimise and improve on the existing cryptographic systems for cost effective and efficient hardware implementation, taking into consideration the specialised nature of low cost RFID-labels.

- Development of new hardware efficient cryptosystems suitable for low cost RFID systems. This may involve the development of hardware efficient hash functions, symmetric and asymmetric encryption, MACs and random and pseudorandom number generators.

- The need to develop protocols with the flexibility to incorporate different cryptographic primitives, security measures and safeguards to prevent rendering labels vulnerable during sudden communication interruptions.

- Improve and optimise coupling between readers and labels. This may involve developing new concepts for formulating coupling between antennas, new antenna design, and analysis so that the available source power to the IC is maximised.

It is important to recognize that the resource limitation of low cost labels suggests that simplicity of small one time pads, which involve one or more small shared secrets between a label and an interrogator, and relatively simple chip implementations should also be considered and must not be discounted. Some of the concerns arising from privacy and security may also be removed by shielded electromagnetic communications between the label and the reader system.

It is important to note that the level of security and privacy will depend on the application. It is evident that there is no universal solution but a collection of solutions suited to different applications. This is addressed within the class hierarchy. There are unique opportunities within the Auto-ID Centre class hierarchy to develop various schemes for meeting the security and privacy levels expected by labels belonging to their respective classes. This opens the gate to a vast number of research avenues that could be pursued in regards to providing both security and privacy to low cost RFID systems.

It must be realised that security will come in many flavours and strength, but low cost will imply that we find mechanisms that are ‘good enough’ and are deterrents than mechanism that are hard to crack. Proposals for implementations of these concepts are outlined in a separate paper.

Most issues concerning privacy are public policy issues however; those that arise from “unlinkablity” and “anonymity” are solvable using a combination of security mechanism and public policy.

AUTO-ID LABS

References

[1] Cole, P. H., "Fundamentals in Radiofrequency Identification", unpublished, 2003, http://www.eleceng.adelaide.edu.au/Personal/peter/peter

[2] Cole, P. H., and Engels, D. W., "Auto-ID 21st century supply chain technology", Proceedings of AEEMA Cleaner Greener Smarter conference, October 2002.

[3] Sarma, S., "Towards the 5c tag", Technical Report MIT-AUTOID-WH-006, 2001. http://www.autoidlabs.org/researcharchive.

[4] Hall, D., Senior Design Engineer, TagSys, Australia. Personal Conversation, July 2004.

[5] AutoID Labs homepage, http://www.autoidlabs.org

[6] RFID Journal news article, "EM micro readies new RFID chip", March 2003, http://www.rfidjournal.com/article/articleview/350/1/1.

[7] Takaragi, T., Usami, M., Imura, R., Itsuki, R., and Satoh, T., "An ultra small individual recognition security chip", IEEE Micro, November-December 2001.

[8] Cole, P. H., Level 4 Electromagnetic Compatibility lecture notes, 2003, http://www.eleceng.adelaide.edu.au/Personal/peter/peter

[9] FCC Regulations Part 15, 2003. http://www.fcc.gov.

[10] Stajano, F., and Anderson, R., "The resurrecting duckling: security issues for ad-hoc wireless networks", International Workshop on Security Protocols, LNCS, vol. 1796, pp 172-194, 1999.

[11] ISO/IEC 15408, Information Technology- Evaluation Criteria for IT Security, International Organisation for Standardisation (ISO), Geneva, 1999.

[12] Weis, S. A., Sarma, E. S., Rivest, R. L., and Engels, D. W., "Security and privacy aspects of low-cost radio frequency identification systems", Security in Pervasive Computing, 2003.

[13] Sarma, S., and Engels, D. W., RFID Systems, "Security & Privacy Implications", Auto-ID center white paper, Feb 2003. . http://www.autoidlabs.org/researcharchive.

[14] Gobioff, H., Smith, S., Tygar, J. D., and Yee, B., "Smart cards in hostile environments", 2nd USENIX Workshop on Electronic Commerce, 1996.

[15] Andreson, R, and Kuhn, M., "Low cost attacks on tamper resistant devices", International Workshop on Security Protocols, LNCS, 1997.

[16] Weigart, S.H., "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defences. In Workshop on Cryptographic Hardware and Embedded Systems", Lecture Notes in Computer Science, vol. 1965, pages 302-317.

[17] Juels, A., and Pappu, R., "Squealing Euros: Privacy Protection in RFID Enabled Banknotes", Financial Cryptography, 2002.

[18] Wolfram, S., A New Kind of Science, 2nd edition, Wolfram Media, 2002.

[19] Daemen, J., Govaerts, R., and Vandewalle, J., "Hash functions based on block ciphers: a synthetic approach", Advances in Cryptology, LNCS. Springer-Verlag, 1991.

[20] Simson L. Garfinkel. "Adopting Fair Information Practices in Low-Cost RFID Systems", Ubiquitous Computing, September 2002.

[21] Electronic Privacy Information Center. EPIC Website http://www.epic.org.

[22] Sen, S., Shaw, C., Chowdhuri, D. R., Ganguly. N., and Chaudhuri, P. P., "Cellular automata based cryptosystem (CAC)", Lecture Notes in Computer Science, vol 2513, pp 303-314, 2002.

[23] Blackburn, S. R., Murphy, S., and Paterson, K. G., "Comments on "Theory and applications of cellular Automata in Cryptography"", IEEE Transactions on Computers, vol. 46, no. 5, pp 637-638, May 1997.

[24] Wolfram, S., "Cryptography with cellular automata", Advances in Cryptology: Crypto ,85 Proceedings, LNCS, vol. 218, pp 429-432, 1986.

[25] Nadi, S., Kar, B. K., and Chaudhuri, P. Pal., "Theory and application of cellular automata in cryptography", IEEE Transactions on Computers, vol 43, no 12, December 1994.

[26] Alien press release, http://www.alientechnology.com/, 30 March 2004.

[27] International Telecommunication Union (ITU) http://www.itu.int/ITU-R/terrestrial/.

[28] Menezes, A., Van Oorchot, P. and Vanstone, S., Handbook of Applied Cryptography, CRC Press, 1996.