EUROSMART
THE VOICE OF THE SMART SECURITY INDUSTRY

RFID technology security concerns: Understanding Secure Contactless device versus RFID tag.

1 Introduction

Contactless products, based on Radio Frequency (RF) technologies, are today deployed all over the world in various applications as goods traceability, transportation ticketing, financial transactions, access control, identity cards, and ePassports.

All these applications use Radio Frequency (RF) as the way to communicate between a card or a tag and a reader but they offer totally different levels of security and privacy to the user.

They are usually designated in the common language under the generic term RFID application creating confusion and legitimate security and privacy concerns among the general public.

There are actually two different types of applications using RF or RFID technology:

1) Radio Frequency Identification (RFID) Tag applications for identifying an object or an animal used typically in supply chain to track objects. This is also used in some cases for people access control.

2) Secure Contactless Device application in an ePassport to get the identity of a traveller or a secure contactless payment card to replace cash payment.

The required levels of security for those two types of applications are totally different. In the first case (RFID Tag) there is little to no protection needed, minimal data storage, low cost and some time long distance reading whereas in the second case there is a maximum of protection needed with amount of confidential protected data stored, encrypted communication and short distance of transaction

To add to the confusion, an additional technology for contactless applications has appeared called NFC: Near Field Communication. Actually NFC is a standard that enables contactless, bi-directional communication between devices which is compatible with existing secure contactless device applications standards.

This paper addresses a technical audience such as decision makers and technical press. The intention is to provide a better understanding of the different RF technologies and standards, their different requirements and corresponding security demands.
This paper specifically addresses secure contactless devices produced under ISO/IEC 14443 versus RFID Tags.

It will also clarify what is NFC (Near Field Communication) technology and its link with secure contactless device and RFID technology.

2 Technical background

Before selecting among available RF based technologies, several aspects are to be considered, such as frequency, baud rate, working distance, desired functionality (Memory size, Microcontroller, Crypto features…). This section provides the technical background as well as an overview of the relevant standards for both RFID Tags and secure contactless devices.

RFID Tags

RFID Tags were the first type of contactless technology product developed (in the mid 1990’s). RFID Tags are mainly used in automation of logistical applications, as enhanced “electronic barcodes”. The main purpose of RFID Tags is to work at a distance of up to a few meters and to be able to communicate with several RFID Tags simultaneously.

Cryptography is not a must in the RFID Tag market segments today. Nevertheless some basic security functions such as passwords and hard-wired crypto features can be integrated into RFID Tags at low cost.

The relevant worldwide ISO standard for RFID technology is ISO 18000 (“RFID for Item Management: Air Interface“). It synthesizes all technical requirements to assure interoperability for each relevant carrier frequency range.

ISO 18000-2 - Parameters for Air Interface <135 kHz
ISO 18000-3 - Parameters for Air Interface at 13.56 MHz
ISO 18000-4 - Parameters for Air Interface at 2.45 GHz
ISO 18000-5 - Parameters for Air Interface at 5.8 GHz
ISO 18000-6 - Parameters for Air Interface at 860-960 MHz
ISO 18000-7 - Parameters for Air Interface at 433 MHz

Several application specific standards also build on ISO 18000.

As an alternative to ISO 18000-6, the American Electronic Product Code (EPC) Global standard is often used for item traceability in UHF.

ISO 15693 (carrier frequency 13.56MHz) is now integrated into ISO 18000-3. This standard is well suited for item traceability applications (working distance up to 70 cm, field density 0.15 to 5 A/m, data baud rate 1.65 to 26 Kbits/s). It is not optimized for applications requiring high security because the field is not sufficient to power microcontrollers and crypto engines and the baud rate allows only small amount of data exchange.

Secure contactless devices

Secure contactless devices (also called proximity cards) were developed ten years ago to address applications for which RFID products (Tags) could not provide the required functionality.

The standards are set by ISO 14443, with the following main characteristics:

- The field frequency: 13.56 MHz
- The field density: 1.5 to 7.5 A/m
- The maximum working distance: around 10 cm
- The communication protocol: reader speaks first
- The data baud rate : 106 to 848 Kbits/s

All these parameters are suitable for applications where security is required because:
- Confidentiality is enforced by proximity working distance and makes data skimming difficult
- A secure contactless device only answers after a proper reader command is received,
- The field density is sufficient to power a microprocessor and a cryptographic engine
- The high baud rate allows an important data volume exchange and allows the implementation of a cryptographic protocol

As the standardization effort started ten years ago, the current standard is the most mature within contactless products. It has been further enhanced by the ISO 10373-6 standard that defines how to check a product is compliant with ISO 14443. This suite of standards allows a complete product specification, ensuring interoperability between chips and readers.

Near Field Communication (NFC)

NFC is a standards based short-range (a few centimetres) wireless connectivity technology that enables, bi-directional communication between devices.
NFC standards are the result of work initiated within Ecma International, a global industry association dedicated to the standardization of technology and consumer electronics, by the creators of the technology, Sony and Philips (now NXP). The standard created by Ecma (ECMA-340) has been adopted by ISO as ISO/IEC 18092 in October 2003.

The Near Field Communication Forum (http://www.nfc-forum.org) was formed to develop the specifications, ensuring the interoperability of the devices and services. NFC forum gathers manufacturers, applications developers and financial services institutions to work together to promote the use of NFC.

NFC splits the components of a communication session into initiators and targets. The initiator is the device that begins and manages the communication and exchange of data. The target responds to requests from the initiator. In traditional RF systems, a device is either an initiator (e.g. the reader) or a target (e.g. the card). The particularity of NFC is that an NFC-enabled device can act as either an initiator or a target.

NFC is closely related and complementary to other contactless technologies. Operating at 13.56 MHz frequency band, at a working distance around 10 cm and with a data baud rate of 424 Kbits/second, NFC is compatible with the ISO 14443 Type A and B standards, NXP's Mifare and Sony's FeliCa technologies.

NFC standard providing identical characteristics to ISO 14443 is a good candidate for applications where security is required and implementation on secure contactless devices.

3 RF technology specific security threats and countermeasures

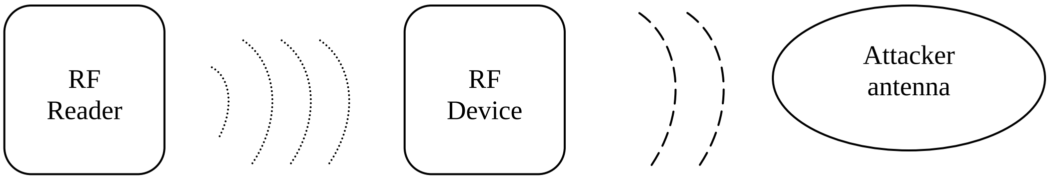
Note that only RF technology specific security threats are considered here, but all the other threats common to smart cards also apply (refer to Application of Attack Potential to smart cards in [6]).

To compare the required security mechanisms, first of all the possible threats need to be defined. In general four main threats can be listed specific to the RF-interface. Some relevant attack paths to illustrate the threats and the possible mechanisms to protect the system are discussed below.

In this section the read/write device of a contactless smartcard or RFID system is called the "Reader", the secure contactless device and RFID Tags are summarized as the "RF device".

Threats (acc. to [1]):

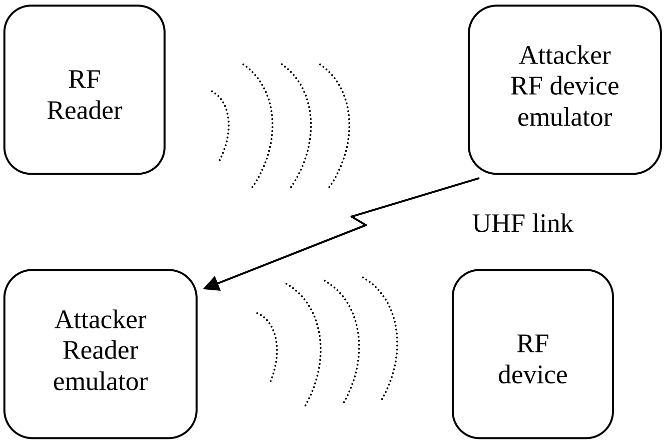
1. **Skimming or Eavesdropping:** An attacker tries to read the data exchange without interfering with the communication. Even though this threat is not limited to contactless communication (but needs to be considered in a contact system too), the use of the radio frequency and its typical behaviour decreases the effort to read the data exchange over a larger distance (compared to a contact interface). Furthermore, it is more likely that the attack would go unnoticed.



Skimming/Eavesdropping

2. **Unwanted activation and use of an RF device:** An attacker tries to activate the RF device without knowledge of the authorized user of the system. This threat is specific to the use of an RF-interface, because basically no direct contact between the attacker's system and the user's' device is required (if no protection is available).

   There are various techniques, and one of the most powerful are Relay Attacks (details can be found in [2]): The purpose of this attack is to make use of the services of an owner's RF device which is neither noticed nor is even close to the Reader performing the transaction. The attacker creates a 'bridge' between the target RF device and a Reader which are not in close proximity to each other, using 2 extra devices and an extra communication link like e.g. an UHF link. One of the attacker's devices is an "RF device emulator". This emulator device acts like the real RF device on the real Reader. Using an UHF link, the data is transferred between this RF device emulator and the second extra device, the "reader emulator". This reader emulator device operates the real RF device, using the data from the real Reader. Using such a system, an RF device and Reader may interact even though they are not in proximity to each other.



Relay attack

3. **Denial Of Service:** An attacker tries to interfere the whole system such that the system does not work anymore. Using (illegal) RF transmitters with high output power may easily block the RF-interface.
4. **Man In The Middle Attack:** Using the relay attack principle, the data exchange between a real Reader and a real RF device cannot only be used to misuse someone else's RF device, but it can be used to even change the real data during the data exchange [4].

Possible Protection (details can be found in [2]):

Protection against ***Skimming or Eavesdropping*** can easily be done with encryption. Encrypted data might be read over a long distance, but if the data is encrypted, the data is useless. The standard encryption principles use an authentication procedure, which guarantees even a protection against "replay attack", where the encrypted data is used to repeat a transaction. For this protection cryptographic features need to be implemented in the contactless device.

It is not recommended to rely only on the theoretical distances described in ISO standards as one could imagine building a special antenna to listen to the communication at a longer distance than specified.
For example the eavesdropping distance for the communication according to ISO/IEC 14443 using the higher data rates is designed to be limited to less than several 10 cm (details see [3]) but listening has been demonstrated up to a few meters (see [7])

The ***Unwanted Activation*** and use of a RF device depends basically on the activation distance, if the system does not provide any extra protection. As before, it is not recommended to rely only on the theoretical activation distance of a few 10 cm defined in the standards.
The best protection mechanisms rely on an additional activation channel.
The first security measure is to protect the contactless device by a metal shielding while it is not in use.
Another protection used in many electronic passport schemes is an optical reading of the machine readable zone required to authenticate and open the data files. Without being able to optically scan the Contactless device no data can be read. For this protection cryptographic features need to be implemented in the contactless device.

The ***Denial Of Service*** countermeasures depends on the system, whether such an attack can bring benefit, and how to protect the system. For example, the system ensures that an uncompleted transaction does not cause any damage.

The protection against a ***Man In The Middle*** attack can be the same as for unwanted activation, but in addition to that, the data communication between Reader and RF device can use an authenticity check to counter data manipulation. A signature or a data encryption protects the data against manipulation.

4 Examples of application

The **RFID Tags** market covers a wide range of applications fields where asset identification and tracking is needed. RFID Tags are mostly replacing barcode systems as they allow more flexibility in automation. For example, several RFID Tags can be read simultaneously, at a long distance and in any orientation, whereas barcodes have to be scanned one by one.

Usual RFID Tags application fields are:

- Transportation and logistics: Parcel or luggage tracking,
- Retail: High value goods tracking,
- Manufacturing: inventory control, supply chain control
- Library: Automation of books handling process

RFID Tags are designed to be low cost, using low cost chips. The information they contain can usually be read by any reader operating within the appropriate frequency and protocol. The information stored is usually a short static identification number, allowing fast detection.

Some security can be implemented if Tags are using a chip providing read/write memory to store dynamic data and follow for example EPC specification.
The EPC Gen 2 Class 1 specification includes minimal security features with a 32-bit password allowing disabling of the Tag with a “kill” command and another optional 32-bit password to grant access to some memory locations.

These mechanisms are weak compared to the capabilities offered by secure contactless technology and a strong cryptographic algorithm is not available:

- The “Kill” command and “access authorization” command do not use strong cryptographic mechanisms and can be easily cracked
- The Tag also does not provide strong encryption to protect data transmission confidentiality
- The Tag uses a low cost chip with no hardware security features, and is therefore easy to clone.

These vulnerabilities are not critical for managing goods in supply chain or books in a library. But this is an issue when considering a person’s identity and access to sensitive data or restricted areas.

Secure Contactless devices address mainly applications where information has to be protected from disclosure, and securely transferred between the device (the card) and the reader. The advantage of contactless is the easy and fast transmission of data.
Main applications of contactless smart cards are:

- Fast Payment cards as MasterCard® Paypass™, Expresspay™ from American Express® and Visa® contactless payment programs.
- Personal Identification as the Personal Identity Verification card for US government (DOD)
- Electronic passport that have already been issued in the tens of thousands for different countries as Denmark, France, German, Italy, Norway, Portugal, Russia, Singapore, Slovenia, Sweden, The Netherlands, UK, USA and other Visa Waiver Program Participating Countries.

NFC is a new standard for the RF transport layer. Its characteristics compatible with ISO 14443 makes it usable for Secure Contactless devices.

NFC-enabled devices are mostly used for purchases, access facilities or transportation with applications running on smart cards and more and more on mobile-phones. A lot of trials are deployed all over the world especially in Mobile-payment application.

For these types of contactless or NFC-enabled applications, security features are needed to ensure confidentiality and/or integrity of the processed data.

Secure contactless device technology provides the level of protection required as it allows the usage of:

- Reliable hardware chips with security features protecting against physical attacks and cloning
- Powerful cryptographic engines for strong encryption to keep confidentiality and integrity of data stored or transferred
- Mutual authentication mechanisms to allow authentication of the reader by the device and vice versa
- Dedicated access control through unique authentication mechanisms

The use of Secure Contactless technology allows the design and implementation of an appropriate level of security, according to the type of application. This security and flexibility cannot be provided by RFID Tags.

5 Conclusion

RF technologies are used for different categories of products.

The RFID technology used in Tags provides low cost products for mass production applications such as supply chain or traceability of goods. For this type of application no sensitive information is transmitted, therefore the need for secure transmission is not considered a ‘must’.

Secure contactless technology must be used when sensitive information is transmitted or transaction integrity is required.

- The identity of a person should not be faked, modified, or monitored without permission
- Financial transactions should not be modified or denied

When security of payment, security of personal information, or security of a state are involved, a high security level is required to preserve confidentiality and integrity of the data transmission. This requires powerful products based on secure contactless technology with a demonstrated security level.

Secure Contactless smart card technology provides the same level of security as secure contact smart cards. They use smart card secure microcontrollers with physical security features to protect from tampering and cloning. They use powerful microprocessors that allow strong cryptographic protocols. The use of smart card contactless technology allows secure management of stored and transmitted data using strong encryption, random challenge, access control through authentication and therefore provides countermeasures to defend against the attacks described in section 3.

About EUROSMART
Eurosmart is an international association located in Brussels representing the Voice of the Smart Card Industry for multi-sector applications. The Association is a non-profit organization committed to expanding the world's smart card market, developing smart card standards and continuously improving quality and security applications.
The Eurosmart Security Working Group represents a competent body of experts combining knowledge of the major players of the Smart card industry in the complete range from the semiconductor, the software development up to the final production and the personalization.
The Eurosmart Security Working Group main mission is to Optimize security efficiency in term of assurance, methodology & cost., in different sectors of the industry Banking, Government, Telecom and actively participate in various expert groups at EU Level (for SEPA implementation), Fraud Prevention Expert Group (security standard)

Additional information on Eurosmart can be found at http://www.eurosmart.com

6 References

List of references:

[1] Rikcha Study:Security Aspects and Prospective Applications of RF ; Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, D-53175 Bonn; ISBN 3-922746-56-x

[2] Klaus Finkenzeller: RFID-Handbook, 2nd edition; Fundamentals and Applications in Contactless Smart Cards and Identification; Wiley & Sons LTD; April 2003; ISBN: 0-470-84402-7

[3] Wolfgang Tobergte (NXP), Renke Bienert (NXP): NXP White paper, Eavesdropping and activation distance for ISO/IEC 14443 devices, 2007

[4] Ziv Kfir, Avishai Wool: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems

[5] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960MHz Version 1.0.9 –January 2005

(http://www.epcglobalinc.org)

[6] Application of Attack Potential to Smartcards -April 2006 Version 2.1 Revision 1

[7] Ilan Kirschenbaum; Avishai Wooly: How to Build a Low-Cost, Extended-Range RFID Skimmer; February 2, 2006 , School of Electrical Engineering Systems, Tel Aviv University,

[8] Gerhard Hancke : A Practical Relay Attack on ISO 14443 Proximity Cards -University of Cambridge, UK

[9] Ernst Haselsteiner and Klemens Breitfuß: Security in Near Field Communication (NFC) Strengths and Weaknesses- Philips Semiconductors Mikronweg 1, 8101 Gratkorn, Austria

[10] Ari Juels : RFID Security and Privacy:A Research Survey- RSA Laboratories 28 September 2005