Information Security Issues of RFID

Zoltán Nyikes
Óbuda University/Doctoral School on Safety and Security Sciences,
Budapest, Hungary
nyikes.zoltan@mil.hu

***Abstract*— After presenting a brief history of RFID, the author discusses the general and security issues related to RFID and their possible solutions. Information security is examined as an integral part of overall security. Furthermore, various information security solutions and technologies are presented to address specific security issues. From the wide range of application possibilities, the author has selected document protection and administrative security. Paper-based documentation cannot be completely ruled out from everyday life. Although great progress has been made in the field of authentic instruments and banknotes, many security elements have not yet appeared in everyday life. The various application possibilities of "smart" paper and digital watermark can be considered here. When examining the question of future development, the author presents some of the likely alternatives predicted by experts of the industry for the forthcoming years.**

I. General introduction to RFID

RFID (radio frequency identification) is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal or person. RFID is coming into increasing use in industry as an alternative to the bar code. The advantage of RFID is that it does not require direct contact or line-of-sight scanning. An RFID system consists of three components: an antenna and transceiver (often combined into one reader) and a transponder (the tag). The antenna uses radio frequency waves to transmit a signal that activates the transponder. When activated, the tag transmits data back to the antenna. [1]

A. A brief history of RFID

The first radio-frequency identification technology was developed during World War II. Sir Robert Alexander Watson discovered and perfected the radar, which was used only for reconnaissance and detection. It was not yet capable of identification. In 1939 British scientists accidentally discovered that when a pilot was making a swinging movement of the plane, the shape of the reflected radio waves was changing, which allowed to distinguish between friendly and hostile aircraft in the radar screen. This can be regarded as the first passive RFID system, which eventually lead to the development of the first active aircraft detection system, the IFF. The boom of the RFID technology in the 1970s was preceded by its introduction in the 1960s. R. F. Harrington's studies on electromagnetic fields provided bases for the subsequent spread of RFID. Its first commercial applications started in the early 1960s. Sensormatic was a leading company in the development of RFID solutions. The EAS anti-theft system is still a widely used technology today. Major developments took place both in America and in Europe in the 1970s to introduce RFID in the monitoring of animals, vehicles and production processes. It became widely popular among farmers to track their livestock. The Los Alamos Research Institute also developed a system to track nuclear devices during these years. In the 1980s, the research and development phase was followed by the implementation of new solutions and their application in various products. In the United States it was primarily used to keep track of delivery processes, to ensure personal access and to identify animals. In the 1990s the range of RFID applications further expanded: it was introduced in motorway tolling, as well as in immobilizers or (skiing) season tickets. The first microwave Schottky diodes integrated on CMOS circuits allowed the creation of microwave RFID tags with a single IC, which allowed greater read range and faster data transfer rates. The UHF RFID gained momentum in 1999, when the Auto-ID Center was founded. The company developed a low cost RFID tag containing a microchip. The tag is only used to store a serial number, which requires smaller memory, therefore it is cheaper. The serial number is searchable in an Internet-based database to receive further information about the product. Before that the RFID TAG had been a mobile database. Today large multinational trading companies are planning the full implementation of RFID. Besides the US Department of Defense, various pharmaceutical and tyre manufacturing companies are interested in the technology. The really widespread use of RFID can be expected nowadays, after the second generation standards have been approved by EPCglobal. [2]

B. Possible applications of RFID

- Logistics, commercial warehouses;
- Library and archival applications;
- To trace assets, asset inventory;
- Production optimization;
- Supply chain management;
- Retail trade;
- Toll systems;
- Security and access control systems;
- Livestock. [3]

C. RFID tags classified

TABLE I.
RFID TAGS ARE CLASSIFIED AS CLASS 0 THROUGH CLASS 5, DEPENDING ON THEIR FUNCTIONALITY [4]

Class 0	UHF read-only, preprogrammed passive tag
Class 1	UHF or HF; write once, read many

978-1-4673-8740-8/16/$31.00 ©2016 IEEE

	(WORM)
Class 2	Passive read-write tags that can be written to at any point in the supply chain
Class 3	Read-write with onboard sensors capable of recording parameters like temperature, pressure, and motion; can be semipassive or active
Class 4	Read-write active tags with integrated transmitters; can communicate with other tags and readers
Class 5	Similar to Class 4 tags but with additional functionality; can provide power to other tags and communicate with devices other than readers

D. Questions and concerns on RFID

The use of RFID for personally identifiable information has been the subject of debate for years. It raises concerns mainly about the protection of personal data. People see a threat in the way that RFID tags can be read without having to face the owner, as the unique identifier of the stamps can be connected to the owner's personal data. In addition, RFID tags can be placed on any goods without the knowledge of the customer. Moreover, the tags can be read remotely by any readers that are hidden in the environment, so an individual may not even be aware of being "read". For example, a customer cannot deactivate the detectors in a department store. When payment is settled by bank card, the purchased product can be related to the customer. Consequently, the customer can be identified by name. Therefore, it may be possible to track not only the product, but also the customer from a larger distance. Various deactivator gates have already been in use, but their efficiency is still questionable. Of course, radio signals can also be encrypted by different cryptographic methods, but this may be limited by the memory capacity of passive tags. Besides the protection of privacy, another important issue is whether RFID is detrimental to health or to the environment. The RFID-related electromagnetic fields (EMF) are generally weak, and the population is exposed to radiation at a rate that is lower than the current standard limits. Nevertheless, the number of wireless devices has greatly increased by now. [5]

II. RFID AND SECURITY

More recently, the implementation of RFID systems in high security applications has come into focus. It is enough to consider the increasingly popular PayPass credit card-paying system or patient identification. These solutions require the integration of certain security supplements into the existing systems, which are able to prevent unauthorized access or login. These advanced authentication systems reveal the fact of possessing a secret. The purpose of applying an appropriate algorithm is to prevent the compromise of the private key. Today's high security RFID systems have the capability of preventing the following attacks:

• Unauthorized access to the media with the purpose of duplicating or changing the stored data.

• Placement of media of unknown origin within the zone by circumventing authentication algorithms.

• Interception of radio traffic, or falsely creating the impression of an authentic media playback ("replay and fraud"). [2]

A. Mutual symmetric authentication

Mutual symmetric authentication is based on a three-step procedure between the reader and transponder in accordance with the ISO 9798-2 standard, which checks both parties' knowledge of the secret cryptographic key at the same time. [2]

B. Derived key authentication

Each transponder is equipped with a private key in order to improve safety. To achieve this, first the serial number of the transponder must be extracted. The secret key is created with the help of a master key and a cryptographic algorithm. As a result, each transponder receives its own ID, and a serial number that is linked to the master key on the downlink channel. As the first step of the common authentication, the reader retrieves the ID of the transponder. With the help of the master key, the special encryption module of the reader generates the private key of the reader. [2]

C. Encrypted connection

The solution described in the previous chapters is now completed with a potential attacker. In this case, there are two types of attackers. The first type attempts to stay in the background and retrieve valuable information in a passive way by interception. The second type, however, actively participates in the data exchange, and modifies its content for its own benefit. Cryptographic solutions can be used against both types of attackers. The value of data will be encrypted, and, as a result, the attacker cannot draw any conclusions on its original content. Data link encryption works on the same principle. In case of sequential encoding, each character is encrypted individually, while in block coding encryption is done by character blocks. The biggest difficulty of the RFID systems with encrypted data traffic is the distribution of the symmetric key before its use. [2]

The **stream encoders** are a set of cryptographic algorithms which encrypt the characters of the open text in succession, but by different functions. First, a random key will be generated, which will be the shared key between the parties in the information exchange. The key will then have an XOR connection with the characters of the open text. The random key must have at least the same length as the open text, otherwise statistical attacks of the repeated patterns can be expected. In addition, each key is used only once, which requires a high level of safety in the key distribution. In this form, stream encoding is completely unsuitable for RFID systems. In order to overcome the complications caused by key distribution and generation, true random number generators were replaced by "pseudorandom" generators, along with "pseudorandom" keys. [2]

D. Other security recommendations

In case of **Hash-based** access control, by taking into account the resource management of cheap smart tags, a simple security procedure based on one-way hash functions will be presented in the followings. Typically, the scheme is implemented by using hardware. The tags working in locked or unlocked mode separate a small

section of their memory to store the metaID earmarks. In order to lock a tag, its owner stores the hashed version of a random key as the metaID of the tag in the transponder. This can be done by RF or in a direct physical way. In order to unlock the key, the host retrieves the metaID of the tag, finds the key in the database, and then returns it to the transponder. The tag hashes the key, and compares it with its own metaID. As soon as these two hashes correspond with each other, the key unlocks itself, and provides full functionality for the surrounding readers. In order to prevent any abuse of unlocked tags, tags should be kept unlocked only for the duration of information flow. The method provides great protection against unauthorized access by taking advantage of the difficulty of inverting a one-way hash. However, it does not prevent spoofing attempts, only detect them. Furthermore, the reading device can also check the content of the tags with the help of the back-end. [2]

In the case of **random access control**, the solution uses one-way hash functions, which is efficient for a small number of tags, and prevents unauthorised requests, while the tags remain able to respond to the request of certified readers. In addition to the above-mentioned transponders which are able to calculate one-way hash functions, this solution can also generate random numbers. At the request of the reading device, the transponder first generates a random number, and then it retrieves the concatenate of the ID and the random number from the hash. [2]

In the case of **asymmetric key** negotiation, the readers can gain much information from the asymmetry between the uplink and downlink channels during the transmission of data which are sensitive to interception. [2]

The method of **Chaffing and Winnowing disturbs** the interception equipment by filling the communication with useless messages, or chaffs, which are continuously filtered by the transponders with the help of a simple MAC (winnowing) when useful data is being sent. [2]

Detection units may also be added to the RFID system to detect unauthorized reading.

In the case of screaming tags, the above-mentioned units can also be used successfully against DoS attacks, as they can detect off-mode transponders. [2]

III. Application of RFID with respect to document security

The concepts of security and safety refer to Digital and/or Photocopied/Printed Data Security/Information Security, as well as brand and packaged product security against unauthorized access or modification, partial or complete deletion, damaging or destruction. It also means the full protection of the confidentiality availability and integrity of the data or product.

A. Data security and protection system

Depending on the method and the degree of detectability, security solutions have the following groups:

- Overt Security Solutions
- Covert Security Solutions
- characters and symbols which can be reconstructed by machine tools, characters, line, colour or other code sequences, which can be made visible by using radiation (lasers, ultraviolet, infrared, radio, x-ray and electron beam) or chemical reagents. [6]

B. RFID solutions for document management

Document identification with RFID stickers

• RFID is used on the document in the form of an identification sticker.

• The collision-free technology allows the identification of hundreds of documents per second; therefore it is ideal for archive application

• The management of high safety level documents: the sticker can record who, when and how long had access to the document [7]

E-Inks, such as materials containing liquid-dispersed, positively charged white particles and negatively charged black microcapsules, which become white or black depending on the polarity of the magnetic or electric field, and their planar distribution carries two-dimensional visual information. [6]

Liquid RFID Ink Solutions were developed by Cross ID Communication Materials, and they are able to identify the materials or products to which they are added, by emitting radio signals. By adding this liquid to printer and photocopier ink, a tamper-proof, high security printing product can be produced. [6]

The Smart Paper, the media type of the future, which can be programmed by using the semiconductor polymers, microchips, radio frequency devices, or printed integrated electronic elements placed on the surface of the paper. [6]

The Digital watermark first appeared in the market of printed and photocopied products in 1992. It can consist of, for example, a number and code combination which may be reconstructed by a machine only and a digital signature. The visible or invisible watermark can be placed on the surface of the media, or embedded into the material of the media, depending on the purpose of protection. [6]

IV. RFID Forecasts, Players and Opportunities 2016-2026

IDTechEx find that in 2015, the total RFID market is worth $10.1 billion, up from $9.5 billion in 2014 and $8.8 billion in 2013. This includes tags, readers and software/services for RFID cards, labels, fobs and all other form factors, for both passive and active RFID. IDTechEx forecast that to rise to $13.2 billion in 2020. [8]

Using new, unique information researched globally by IDTechEx technical experts, we analyze the RFID market in many different ways. Full analysis by each market is given in great detail including in-depth historic data by application type from 2005 year by year to 2021 and with a 2026 outlook. For passive RFID, forecasts are provided separately for the following application areas. For each we provide the number of tags, average sales price and total value of tags. [8]

In addition, ten year forecasts are provided for battery assisted passive and active RFID and RTLS in the following applications:

- Pharma/Healthcare
- Cold retail supply chain
- Consumer goods
- Postal
- Manufacturing parts, tools
- Archiving (samples)

- Military
- Retail CPG Pallet/case
- Shelf edge labels
- Conveyances/Rollcages/ULD/Totes
- Vehicles People (excluding other sectors)
- Car clickers other tag applications [8]

Additionally, the report provides units, asp and total value for RFID readers as follows:

- UHF Fixed portal
- UHF Embedded and handheld
- HF and LF Hand held, fixed, embedded
- LF Vehicle
- NFC Cellphone [8]

TABLE II.
PASSIVE UHF MARKET DATA SEGMENTS - 10 YEAR FORECAST [8]

Passive UHF market data segments - 10 year forecast	Passive HF RFID market data segments - 10 year forecast	Passive LF market data segments - 10 year forecast
Retail apparel and footwear	Contactless cards/fobs	Livestock and
Retail-other	Smart tickets	Access control
Logistics, conveyances, roll cages	Books	Vehicle immobilizers
Asset management/inventory	Medical	Medical
Medical/health care	Assets/tools	People
Air baggage and cargo	Passports	Other
Access control/ticketing	People	
Embedded	NFC applications	
People	Other	
Other		

ACKNOWLEDGMENT

The current analysis of the topic covered can contribute to the development of the present and future radio frequency identification and registration systems. Quality assurance and cost reduction in information technology are not only supported by the Government, but also gaining a growing role both in the private and corporate spheres, as well as in the public sector. As a consequence, radio frequency identification and the related information security considerations will be increasingly at the forefront of development in the coming years. The aim is to develop such identification procedures which protect the interest of users, and comply with the laws and agreements on the protection of personal data. As the above example of document security has shown, these solutions offer a wide range of applicability, and they could fulfil today's security requirements with minimal innovative effort. High-frequency radio communication chips, which can be stuck or printed on anything or planted anywhere, have already been introduced into various fields including logistics, trade, health, border security, education or law enforcement, and they will be used even more extensively in the future producing vast amount of processed data.

REFERENCES

[1] Margaret Rouse - RFID (radio frequency identification) definition, http://searchmanufacturingerp.techtarget.com/definition/RFID, 20 Sept 2015

[2] Studies on RFID systems in view of application and technology – Inter-University Centre of Telecommunications and Informatics (ETIK), Budapest, September 2006

[3] IT café – European agreement on the ethical use of RFID tags http://itcafe.hu/hir/eu_eb_rfid_intelligens_cimke_kroes.html, 20 Sept 2015

[4] EPC-RFID INFO – RFID Tags, http://www.epc-rfid.info/rfid_tags, 5 October 2015

[5] Éva Juhász – RFID – A Current Issue (20 July 2011) http://krono.inaplo.hu/index.php/inter/8-networkstudies/916-rfid-egy-aktualis-kerdes, download: 10 October 2013

[6] Emil Eiler – Security printing for the protection of digital data, brands and documents, packaged products and consumers, MAGYAR GRAFIKA 2007/7.

[7] László Rácz – RFID-Radio Frequency Identification-[Online] http://www.allaminyomda.hu/file/1000185, download: 10 October 2013

[8] Raghu Das, Dr. Peter Harrop – RFID Forecasts, Players and Opportunities 2016-2026, (October 2015) http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2016-2026-000451.asp, download: 5 October 2015