FACTA UNIVERSITATIS
Series: **Mechanical Engineering** Vol. 8, N° 1, 2010, pp. 57 - 62

RFID TECHNOLOGY, PRIVACY AND SECURITY

UDC 65.011.56

Stevan Stankovski[1], Gordana Ostojić[1], Milovan Lazarević[1], Božidar Popović[2], Danijel Mijić[2]

[1]University of Novi Sad, Faculty of Technical Sciences, Serbia
E-mail: stevan@uns.ac.rs
[2]University of East Sarajevo, Faculty of Electrical Engineering, Bosnia and Herzegovina

Abstract. *Every day, people interact directly with a Radio Frequency Identification (RFID) device (tag), buying a product or accessing some desired place. The tag can then be interrogated via radio waves by an RFID reader to return a small amount of information, such as an identification code or personal data. Also, the RFID technology is very useful for supplying chain management, item tracking and other areas. At the same time, the RFID technology raises privacy and security issues. For example, applying RFID tags to individual items raises the possibility that the movement of these items can be tracked, or that individuals can be scanned to learn what items they carry. Many other examples can be named to illustrate problems arising from undesired uses of the RFID data. This paper presents some issues that can be very helpful for overcoming the above mentioned problems.*

Key Words: *RFID Technology, RFID Tag, Privacy, Security*

1. INTRODUCTION

Radio Frequency Identification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker or a plastic card, which can be attached to or incorporated into a product. An early, but not the first, work exploring RFID, is the landmark paper by Harry Stockman, "Communication by Means of Reflected Power", *Proceedings of the IRE*, pp. 1196-1204, October 1948 [1].

Advances in radar and RF communications systems continued through the 1950s and 1960s. Scientists and academics did research projects and they presented papers explaining how RF energy could be used for remote objects identification.

Commercial activities were beginning in the 1960s. Sensormatic and Checkpoint were founded in the late 1960s. These companies, with others such as Knogo, developed electronic article surveillance (EAS) equipment to counter theft. These types of systems often use '1-bit' tags which means that only presence or absence of the tag could be detected;

Received March 22, 2010

yet, tags could be produced inexpensively while providing for effective anti-theft measures. These types of systems used either microwave or inductive technology. EAS is arguably the first and most widely spread commercial use of RFID.

In the 1970s developers, inventors, companies, academic institutions, and government laboratories were actively working on RFID, and notable advances were being realized at research laboratories and academic institutions such as Los Alamos Scientific Laboratory, Northwestern University, and the Microwave Institute Foundation in Sweden among others. An early and important development was the Los Alamos work that was presented by Alfred Koelle, Steven Depp and Robert Freyman "Short-range radio-telemetry for electronic identification using modulated backscatter" in 1975.

The 1980s became the decade for full implementation of RFID technology, though interests developed somewhat differently in various parts of the world. The greatest interests in the United States were in transportation, personnel access, and to a lesser extent, animals. In Europe, the greatest interests were in short-range systems for animals, industrial and business applications, although toll roads in Italy, France, Spain, Portugal, and Norway were equipped with RFID.

In the Americas, the Association of American Railroads and the Container Handling Cooperative Program were active with RFID initiatives. Tests of RFID for collecting tolls had been going on for many years, and the first commercial application began in Europe in 1987 in Norway and was followed quickly in the United States by the Dallas North Turnpike in 1989. Also during this time, the Port Authority of New York and New Jersey began commercial operation of RFID for buses going through the Lincoln Tunnel. RFID was finding a home with electronic toll collection, and new players were arriving daily.

Research and development did not slow down in the 1990s since new technological developments would expand the RFID functionality.

IBM engineers developed and patented an ultra-high frequency (UHF) RFID system. UHF offered longer read range (up to 10 m under good conditions) and faster data transfer. UHF RFID got a boost in 1999, when the Uniform Code Council, EAN International, Procter & Gamble and Gillette put up funding to establish the Auto-ID Center at the Massachusetts Institute of Technology. Between 1999 and 2003, the Auto-ID Center gained the support of more than 100 large end-user companies, plus the U.S. Department of Defense and many key RFID vendors. It developed two air interface protocols (Class 1 and Class 0), the Electronic Product Code (EPC) numbering scheme, and a network architecture for looking up data associated on an RFID tag on the Internet. The technology was licensed to the Uniform Code Council in 2003, and the Uniform Code Council created EPCglobal, as a joint venture with EAN International, to commercialize EPC technology. The Auto-ID Center closed its doors in October 2003, and its research responsibilities were passed on to Auto-ID Labs.

Consumer acceptance of the RFID technology is a complex issue. In the past, various theories evolved to explain adoption of the RFID technology. One of the most important challenges is to solve the issues of privacy and security of the RFID based applications. In the text below, some issues of concern in the matters of privacy and security are explained.

2. PRIVACY AND THE RFID TECHNOLOGY

Privacy refers to the information privacy needs of consumers. Of primary concern in regard to RFID usage in retail is the collection of personal information that pertains to consumer shopping preferences, actions and behavior [2]. It is the collection, use and disclosure of this information, particularly when it may be incorrect or unverified, to track and monitor individuals without their awareness or approval, that is commonly recognized as one of the most prominent threats. This privacy concern is similar in all the case studies to be explored in this paper, which will again provide for an important platform for assessing the ways in which value and privacy are related. Finally, the dimension of control is another important variable in the consumer acceptance of technologies. It relates to the individual's ability to control the information that is collected and stored by the technology or its ability to record, track or identify that individual's actions. The level of control that is provided either inherently through the technology or by the service provider, whether that be perceived or real, is seen as an important element that, when combined with the value proposition, can affect consumer acceptance. Interestingly, the case studies to be discussed all provide for different means or levels of control in regard to end users and their privacy. It is important to point out that an assessment of barriers and threats especially with regard to Privacy is necessary on a case-by-case basis, as classifications can only provide a general overview over a group of applications with shared characteristics, which are shown in Table 2 [3] while the barriers to the RFID applications deployment are shown in Table 1 [3].

Table 1 Barriers to the deployment of RFID applications [3].

User controlled	Barriers: Privacy/Security: Low Interoperability: Low	Barriers: Privacy/Security: Medium Interoperability: Medium	Barriers: Privacy/Security: Medium Interoperability: High
User accessible	Barriers: Privacy/Security: Medium Interoperability: Low	Barriers: Privacy/Security: Medium Interoperability: Medium	Barriers: Privacy/Security: High Interoperability: High
User informed	Barriers: Privacy/Security: High Interoperability: Low	Barriers: Privacy/Security: High Interoperability: Medium	Barriers: Privacy/Security: High Interoperability: High

The main concern about RFID seems to be that it may enable third parties to track individuals that buy certain goods. While such controls are put in place to protect the privacy of individuals, it is still important to recognize that where the technology provides the capability, it will almost always be exploited in some way by unscrupulous people. It may appear that, regarding wide usage of the cases, privacy has not been a barrier to their adoption and consequent acceptance by the society in large. While the privacy concerns still exist and indeed, many individuals remain concerned about their privacy in relation to such technologies and services, on the whole, it would seem that consumers have accepted each technology because the benefit of the technology is in the first place.

Table 2 Classification of RFID systems by data-protection and user control [3].

	Data-protected	Data-shared	Data-unprotected
User controlled	●information on the tag is stored in a way only interpretable by this specific system ●user controls access to information on the tag ●user controls information related to her/him stored in the system	●information on the tag is stored in a way only interpretable by a defined set of systems ●user controls access to information on the tag ●user controls information related to her/him stored in the system	●information on the tag is stored in a way that does not effectively prevent the interpretation by other systems ●user controls access to information on the tag ●user controls information related to her/him stored in the system
User accessible	●information on the tag is stored in a way only interpretable by this specific system ●user has access to information stored on the tag and in the system	●information on the tag is stored in a way only interpretable by a defined set of systems ●user has access to information stored on the tag and in the system	●information on the tag is stored in a way that does not effectively prevent the interpretation by other systems ●user has access to information stored on the tag and in the system
User informed	●information on the tag is stored in a way only interpretable by this specific system ●user is informed of the data collection and its purposes but has no direct access to the information	●information on the tag is stored in a way only interpretable by a defined set of systems ●user is informed of the data collection and its purposes but has no direct access to the information	●information on the tag is stored in a way that does not effectively prevent the interpretation by other systems ●user is informed of the data collection and its purposes but has no direct access to the information

3. SECURITY AND THE RFID TECHNOLOGY

RFID presents security and privacy risks must be carefully mitigated through management, operational, and technical controls in order to realize the numerous benefits the technology has to offer. When practitioners adhere to sound security engineering principles, the RFID technology can help a wide range of organizations and individuals realize substantial productivity gains and efficiencies. The RFID security is a rapidly

evolving field with a number of promising innovations expected in the oncoming years [4]. Each RFID system has different components and customizations so that it can support a particular business process for an organization; as a result, the security risks for RFID systems and the controls available to address them are highly varied.

Each type of application uses a different combination of components and has a different set of risks. For example, protecting the information used to conduct financial transactions in an automated payment system requires different security controls than those used for protecting the information needed to track livestock. Factors to consider include:

- The general functional objective of the RFID technology,
- The nature of the information that the RFID system processes or generates,
- The physical and technical environment at the time RFID transactions occur,
- The physical and technical environment before and after RFID transactions take place,
- The economics of the business process and RFID system.

For the RFID implementations to be successful, organizations should effectively manage their risk. Like other technologies, the RFID technology enables organizations to significantly change their business processes to increase efficiency and effectiveness. This technology is complex and combines a number of different computing and communications technologies. Both the changes to business process and the complexity of the technology generate risk. The major risks associated with RFID systems are as follows:

- Business process risk. Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.
- Business intelligence risk. An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.
- Privacy risk. Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. As people possess more tagged items and networked RFID readers become ever more prevalent, organizations may have the ability to combine and correlate data across applications to infer personal identity and location and build personal profiles in ways that increase the privacy risk.
- Externality risk. RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

Organizations need to assess the risks they face and choose an appropriate mix of management, operational, and technical security controls for their environments. These organizational assessments should take into account many factors, such as regulatory requirements, the magnitude of each threat, and cost and performance implications of the technology or operational practice.

When securing an RFID system, organizations should select security controls that are compatible with the RFID technologies they currently deploy or purchase new RFID technologies that support the necessary controls. To be most effective, the RFID security controls should be incorporated throughout the entire life cycle of RFID systems—from policy development and design to operations and retirement. However, many RFID products support only a fraction of the possible protection mechanisms. Tags, in particular, have very limited computing capabilities. Most tags supporting asset management applications do not support authentication, access control, or encryption techniques commonly found in other business IT systems. The RFID standards specify security features including passwords to

protect access to certain tag commands and memory, but the level of security offered differs across these standards. Vendors also offer proprietary security features, including proprietary extensions to standards-based technologies, but they are not always compatible with other components of the system. Careful planning and procurement are necessary to ensure the way in which an organization's RFID system meets its security objectives [4, 5].

4. CONCLUSION

While the privacy and security concerns still exist, consumers seem to have accepted the use of the RFID technologies and services in view of the benefits to be gained from them. The paper presents some facts that are taken into consideration when the RFID technology is to be applied to the matters related to the privacy and security.

REFERENCES

1. Landt, J., *Shrouds of Time The history of RFID*, Aim publication, Aim Inc, Pittsburg, 2001
2. Renegar, BD., Michael, K., Michael, MG., *Privacy, Value and Control Issues in Four Mobile Business Applications*, 7th International Conference on Mobile Business, July 7-8 2008, Barcelona, Spain
3. Krish, A., *RFID Privacy Issues*, Contribution to the RFID Expert Group Meeting on 10 July 2007
4. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., Phillips, T., 2007, *Guidelines for Securing Radio Frequency Identification (RFID) Systems, National Institute of Standards and Technology*, Gaithersburg, MD 20899-8930,
5. Jovanović, V., Filipovic, S., Ostojić, G., Stankovski, S., Lazarević, M.,2009, Analysis *of Possible Use of Identification Technologies in Disassembly*, Facta Univerisitatis: Series Mechanical Engineering, Vol.7, No 1, 2009, pp 81-92.

RFID TEHNOLOGIJA, PRIVATNOST I SIGURNOST

Stevan Stankovski, Gordana Ostojić, Milovan Lazarević, Božidar Popović, Danijel Mijić

Ljudi svakodnevno imaju kontakt sa RFID (Radio Frequency Identification) uredjajima, bilo da kupuju neki proizvod ili pristupaju nekom prostoru. Tada se sa tagova korišćenjem RFID čitača dobijaju podaci koji su ili identifikacioni kodovi ili neki lični podaci. RFID tehnologija se takođe veoma uspešno primenjuje u lancima snabdevanja i ostalim oblastima gde je potrebno praćenje predmeta. Istovremeno problemi sa privatnošći i sigurnošću RFID podataka postaje sve složenije. Postoji veliki broj primera koji islustuju neželjeno korišćenje RFID podataka. U ovom radu su predstavljeni neki od prilaza koji se mogu iskoristiti za prevazilažnje probleme nastalih uled nežljenog korišćenja RFID podataka.

Ključne reči: *RFID tehnologija, RFID tag, privatnost, sigurnost*