Journal scientific and applied research, vol. 12, 2017
Association Scientific and Applied Research
International Journal

Original Contribution ISSN 1314-6289

TYPOLOGY OF RISKS IN RFID

Stefan Kazakov, Jordanka Jordanova

KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN, SHUMEN 9712, 115 UNIVERSITETSKA STR.

E-mail: st.kazakov@shu.bg, j.jordanova@shu.bg

ABSTRACT: *Radio Frequency Identification (RFID) is still evolving technology. It is technology with many possible applications. There are also many different possiblefrequencies, different physical forms of RFID tags, different possible use cases for RFID readers. There are also many standards related to RFID. In this paper state of RFID standards is presented. Typology of RFID systems according to six different criteria was proposed. This overview can serve for engineers, managers and decision makers, when doing first insights into technology.*

KEУ WARDS: *Radio Frequency Identification (RFID)*

1. Introduction

Radio frequency identification technology, known as RFID, has been described as “tech’s official Next Big Thing.” RFID is not actually a new technology, but it is being applied in new ways, spurred by technological advances and decreased costs. Once used during World War II to identify friendly aircraft, RFID is now being used in a variety of public and private sector settings, from hospitals to the highway.

In RFID systems, an item is tagged with a tiny silicon chip and an antenna; the chip plus antenna (together called a “tag”) can then be scanned by mobile or stationary readers, using radio waves (the “RF”). The chip can be encoded with a unique identifier, allowing tagged items to be individually identified by a reader (the “ID”). Thus, for example, in a clothing store, each particular suit jacket, including its style, color, and size, can be identified electronically. In a pharmacy, a druggist can fill a prescription from a bottle bearing an RFID- chipped label confirming the authenticity of its contents. On the highway, cars with RFID tags on their windshields can move swiftly through highway tollbooths, saving time and reducing traffic congestion. At home, pets can be implanted with chips so that lost animals can be identified and returned to their owners more readily. In each case, a reader must scan the tag for the data it contains and then send that information to a database, which interprets the data stored on the tag. The tag, reader, and database are the key components of an RFID system.

2. What is RFID?

Understanding what RFID devices are and how they work is critical to an analysis of the policy issues surrounding this technology. Generic references to "RFID technology" may be applied incorrectly to a wide range of devices or capabilities. For example, RFID by itself is not a location-tracking technology. At sites where readers are installed, RFID may be used to track tagged objects, but this static readability differs from technology such as global positioning systems, or GPS, which uses a network of satellites to pinpoint the location of a receiver. And RFID technology itself can be used for a variety of applications, from contactless identification cards that can be scanned no farther than inches away from a reader, to highway systems utilizing "active" RFID tags that can initiate communication with a scanner 30m away.

2.1 Primary Components of RFID Devices

RFID devices have three primary elements: a chip, an antenna, and a reader. A fourth important part of any RFID system is the database where information about tagged objects is stored.

– The chip, usually made of silicon, contains information about the item to which it is attached. Chips used by retailers and manufacturers to identify consumer goods may contain an Electronic Product Code ("EPC").11 The EPC is the RFID equivalent of the familiar universal product code ("UPC"), or bar code, currently imprinted on many products. Bar codes must be optically scanned, and contain only generic product information. By contrast, EPC chips are encrypted with a unique product code that identifies the individual product to which it is attached, and can be read using radio frequency. These codes contain the type of data that product manufacturers and retailers will use to track the authenticity and location of goods throughout the supply chain. An RFID chip may also contain information other than an EPC, such as biometric data (a digitized image of a fingerprint or photograph, for example). In addition, some unauthorized reading of data. “Reading” tags refers to the communication between the tag and reader via radio waves operating at a certain frequency. In contrast to bar codes, one of RFID’s principal distinctions is tags and readers can communicate with each other without being in each other’s line-of-sight. Therefore, a reader can scan a tag without physically “seeing” it. Further, RFID readers can process multiple items at one time, resulting in a much-increased (again as compared to UPC codes) “speed of read.”

– The database, or other back-end logistics system, stores information about RFID- tagged objects. Access to both a reader and its corresponding database are necessary before information stored on an RFID tag can be obtained and understood. In order to interpret such data, RFID readers must be able to communicate with a database or other computer program.

Although all RFID systems have these essential components, other variables affect the use or set of applications for which a particular tag is appropriate. As discussed further below, key factors include whether the tag used is “active” or “passive”; what radio frequency is used; the size of the antennas attached to the chip and to the reader; what and how much information can be stored on a tag; and whether the tag is “read/write” or “read-only.” These factors affect the read ranges of the systems as well as the kind of object that can usefully be tagged. They also impact the cost, which is an especially important commercial consideration when tagging a large volume of items.

2.2 Passive v. Active Tags

There are three types of RFID tags, differentiated by how they communicate and how that communication is initiated:

– **Passive tags** have no onboard power source – meaning no battery – and do not initiate communication. A reader must first query a passive tag, sending electromagnetic waves that form a magnetic field when they “couple” with the antenna on the RFID tag.” Consistent with any applicable authorization, authentication, and encryption, the tag will then respond to the reader, sending via radio waves the data stored on it. Currently, depending on the size of the antenna and the frequency, passive tags can be read, at least theoretically, from up to 10 meters away. However, real-world environmental factors, such as wind and interference from substances like water or metal, can reduce the actual read range for passive tags to 3 meters or less. Passive tags are already used for a wide array of applications, including building-access cards, mass transit tickets, and, increasingly, tracking consumer products through the supply chain. Depending on the sophistication of the chip, such as how much memory it has or its encryption capability, a passive tag currently costs between 20 cents and several dollars.

– **Semi-passive tags**, like passive tags, do not initiate communication with readers, but they do have batteries. This onboard power is used to operate the circuitry on the chip, storing information such as ambient temperature. Semi-passive tags can be combined, for example, with sensors to create "smart dust" – tiny wireless sensors that can monitor environmental factors. A grocery chain might use smart dust to track energy use, or a vineyard to measure incremental weather changes that could critically affect grapes. Devices using smart dust, also known as "motes," currently cost about $100 each, but, in a few years, reportedly could drop to less than $10 apiece.

– **Active tags** can initiate communication and typically have onboard power. They can communicate the longest distances – 30 or more meters. Currently, active tags typically cost $20 or more. A familiar application of active tags is for automatic toll payment systems, like the Northeast's "E-ZPass," that allow cars bearing active tags to use express lanes that don't require drivers to stop and pay.

2.3 Radio Frequency

Communication between RFID tags and readers is also affected by the radio frequency used, which determines the speed of communications as well as the distance from which tags can be read. Higher frequency typically means longer read range. Low-frequency ("LF") tags, which operate at less than 135 kilohertz (KHz), are thus appropriate for short-range uses, like animal identification and anti-theft systems, such as RFID-embedded automobile keys. Systems that operate at 13.56 megahertz (MHz) are characterized as high frequency ("HF"). Both low-frequency and high-frequency tags can be passive. Scanners can read multiple HF tags at once and at a faster rate than LF tags. A key use of HF tags is in contactless "smart cards," such as mass transit cards or building-access badges.

The third frequency, Ultra-High Frequency ("UHF"), is contemplated for widespread use by some major retailers, who are working with their suppliers to apply UHF tags to cases and pallets of goods. These tags, which operate at around 900 MHz, can be read at longer distances, which outside the laboratory environment range between three and possibly fifteen feet.36 However, UHF tags are more sensitive to environmental factors like water, which absorb the tag's energy and thus block its ability to communicate with a reader.

2.4 Read/Write Capacity

Finally, another important feature of RFID tags is their "read/write" capacity, or "read- only" status. These terms refer to a tag's ability to have data added to it during its lifetime. The information stored on a "read-only" tag cannot be altered, but a writeable tag (with read/write capacity) can receive and store additional information. Read/write applications are most prevalent when tags are re-used. They are usually more sophisticated and costly than read-only applications. In addition, read/write applications have shorter read ranges. Read-only tags are well-suited to applications like item-level tagging of retail goods, since they are less expensive and, as part of a networked system, can provide a great deal of information by directing the reader to the associated database(s) where information about the tagged item is maintained.

3. RFID Today and Tomorrow

3.1 Current Uses of RFID

Workshop participants described a number of RFID applications that consumers may already be using. For example, some consumers are familiar with employee identification cards that authenticate the pass-holder before permitting access. A related use of RFID is for event access – to amusement parks, ski areas, and concerts, where tagged bracelets or tickets are used. Panelists also explained how RFID is being used in a variety of transportation- related contexts. Many automobile models already use RFID tags in keys to authenticate the user, adding another layer of security to starting a car. Another example, the "Speedpass," allows drivers to purchase gas and convenience store goods from ExxonMobil stations. RFID is also transforming highway travel, with the advent of E-ZPass in Northeastern and Mid-Atlantic states and similar programs in other regions of the country that allow drivers to pass through tolls without stopping to pay. An active tag on the vehicle's windshield lets a reader installed at the tollbooth know that a tagged vehicle is passing through; information flows from the tag, to the reader, and then to a centralized database, where the prepaid or checking account associated with that vehicle is charged.

3.2 RFID in the Supply Chain

To the extent that the much-touted "RFID revolution" is underway, it is occurring somewhat out of public sight – in warehouses, distribution centers, and other stages of the supply chain. Workshop participants discussed how RFID's impact on the flow of goods through distribution channels has implications not just for manufacturers, suppliers, and retailers, but also for consumers. Many panelists reported that as a result of more efficient distribution practices generated by RFID use, consumers may find what they want on the store shelves, when they want it, and perhaps at lower prices.

Participants discussed how RFID may help prevent these lapses by improving visibility at multiple stages of the supply chain. RFID readers can gather information about the location of tagged goods as they make their way from the manufacturer, to a warehouse or series of distribution centers, and to the final destination, their store. Also, as one workshop participant explained, RFID enhances the accuracy of information currently obtained through bar code scanning, which is more vulnerable to human error. According to this panelist, access to more – and more accurate – information about where products are in the distribution chain enables retailers to keep what they need in stock and what they do not need off the shelf.

Workshop participants also touted the discipline that RFID imposes on the supply chain by, for example, reducing “shrinkage,” or theft. One panelist explained how RFID may lower costs by keeping shipping volumes leaner and more accurate. Other panelists described how RFID tags can be read much faster than bar codes, citing tests indicating that RFID’s scanning capability can result in goods moving through the supply chain ten times faster than they do when bar codes are used. According to another participant, RFID will facilitate quicker, more accurate recalls by enabling the tracking of a product’s origin and its location in the distribution chain. Further, this panelist asserted, RFID will enhance product freshness by monitoring expiration dates of consumer goods, so retailers know when not to offer items for sale.

3.3 RFID Use in the Public Sector

Panelists also discussed how RFID is being used or contemplated for use by government entities to meet objectives similar to those their private-sector counterparts hope to achieve. Workshop participants discussed a variety of ongoing and proposed government RFID applications.

3.4 Emerging RFID Applications

The Workshop also addressed emerging RFID applications and when such uses are expected to be implemented. According to panelists, one sector that is the focus of extensive RFID research is health care, where RFID devices can be used to track equipment and people within a medical facility. Other proposed applications contemplate using RFID in different ways. For example, one

Fig. 3. Basic types of attacks relating to data/tag relationship, tag/tagged item relationship and tag/reader relationship

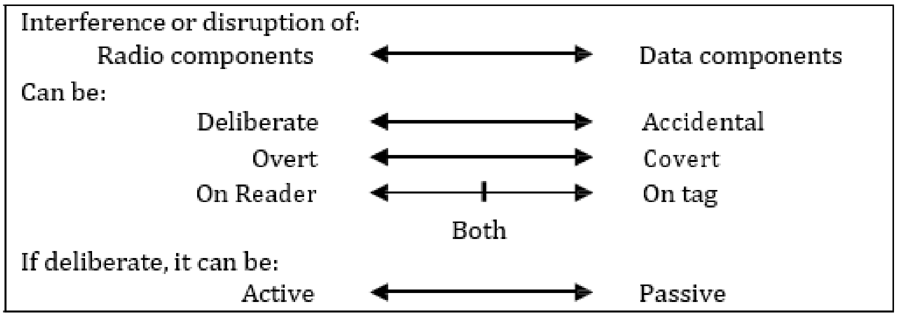
Table 1. Types of attacks according to their purpose: spying, deception, denial of service, protection of privacy

	Spying	Deception	Denial of Service	Protection of privacy
Falsifying content		+		
Falsifying tag identity		+		
Deactivating		+	+	+
Detaching		+		+
Eavesdropping	+			
Blocking		+	+	+
Jamming		+	+	+
Falsifying reader	+			

Security challenges raised by RFID can also be structured according to the traditional dimensions of information security: loss of availability, integrity and confidentiality.

3.5.2 Risks related to tags and readers

Many events can disrupt a RFID system. They can be categorized as interference or disruption of either the hardware, or the radio, or the data components of the system. Interference or disruption to the physical components of readers and tags can be deliberate or accidental, overt or covert. Accidental or deliberate disruption of the radio components can be of the reader or tag or both. Deliberate attacks can be active or passive. Interference or disruption on the data components can be of the tag or reader data or both.



RFID systems, as any information system, include software and hardware components. However, their main specificity lies in the hardware components, namely the tags and readers as well as the methods of energy exchange they use to communicate.

Availability is the assurance of timely and reliable access to data services for authorized users. It ensures that information or resources are available when required. For instance, Denial of Service (DoS) attacks target the availability of a system. Consequences of disruption of availability of typical RFID systems could be, for example, delays in processing identity documents (*e.g.* disabled RFID passports) thus possibly disturbing airport border control processes, preventing individuals to access public transportation systems (*e.g.* subway access card) or work premises (*e.g.* access control cards), preventing an owner to access his/her vehicle (*e.g.* RFID car keys), preventing automatic processing of medicine information in a health context leading to dangerous errors for patients (*e.g.* medicine tagging).

Threats to the availability of the physical components of a RFID system can be overt or covert. Overt attacks on tags include cutting the electrical circuit on the tag, detaching the tag from the tagged item, discharging the battery of an active tag, or masking the antenna (shielding) with a conductive material or paint. Such strategies could be pursued to evade anti-theft RFID systems in stores. They could also be used for privacy protection purposes: companies have developed RFID blocking wallets (for RFID credit cards) and passport cases that are presented as privacy protective apparel.

Covert attacks can be conducted by overloading receiving components to stop them from functioning or to destroy them, for example by subjecting a passive tag to a high energy field in close proximity. Hackers have demonstrated that a strong energy field generated by an inexpensive, modified, single-use camera flash light can produce this result.

Integrity is the underlying assurance that data has not been altered during a transmission from the point of origin to the point of reception. Consequences of loss of integrity in common RFID systems could include, for example, delays and misdirection in the supply chain or confusion in retail operations due to corrupt or erroneous information. In some cases, loss of integrity generates loss of availability. For example, corrupt access cards would not enable individuals to access the transportation system. If car ignition key information is altered, then it is likely that access to the car will be impossible.

A man-made unwanted signal can also be used to inject a false signal, compromising the system's integrity. Reader identity could be falsified to access, modify or kill a tag. For example, a "kill" command could be sent before the tag is read by the legitimate reader and lead to fraud in a retail context, or disrupt supply chain information. Tag cloning and emulation could be used to falsify the identity of goods, and, for example, replace them with cheaper item identifiers. Automobile thieves could clone car keys. Cloned credentials could enable individuals' identity to be stolen to enable access to restricted areas in the work environment. Cloning could lead to identity theft if the cloned credential can be used as a proof of identity.

Confidentiality is the assurance that information is accessible only to those who are authorized to have access. When the data relates to an individual, loss of confidentiality results in data protection violations. Consequences of loss of confidentiality in typical RFID systems could include, for example, stealing competitor information in the supply chain or in the retail environment, stealing a vehicle by gaining access to electronic key information and cloning the chip. According to a Japanese newspaper, data about passengers' latest entry and exit stations stored in a Japanese public transport access card (Suica card) can be read by basic RFID readers, such as the one embedded in Sony Clié PDA. A journalist claimed that the possibility to read such information at a distance could potentially facilitate stalking. The vulnerability of passport information (including biometric data) has been pointed out as a possible source of fraud or crimes involving identity theft (see Annex III). Unauthorized remote access to data is sometimes also called "skimming".

Any system based on radio technology is susceptible to eavesdropping of the radio signal between transmitter and receiver, thus raising confidentiality challenges (as well as integrity challenges if the data can be reinjected). RFID systems based on magnetic induction also generate radio waves that an attacker equipped with the appropriate radio equipment could, in theory, intercept. However, although theoretically possible, it is practically improbable because the energy levels would be relatively low and would be covered by noise, forcing the attacker to operate at short distance of the tags and reader (likely, in an overt manner).

RFID eavesdropping can be both passive and active. The attacker (or "interceptor") may actively send a signal to the tag to get a response, or simply passively listen to the response prompted by a reader activating the tag. Some tags can only reply with data (*e.g.* an identification number). More “intelligent” tags can send back a processed response akin to being actively interrogated with the objective of exploiting a vulnerability.

3.5.3 Risks related to other components

Other components of RFID systems present security risks too. In particular, database security has been identified as a serious and sometimes underestimated concern, since databases containing information associated to tags are likely to be accessed by different enterprises and, sometimes, will be maintained by third parties.

Academic research has also demonstrated that classic Structured Query Language(SQL) and script injection attacks are capable of significantly damaging an RFID system through the use of just one infected RFID tag. RFID tags’ data could include unexpected code or instructions designed, for example, to damage the back- end database of an RFID system, compromise the whole system and/or self-replicate inside the system. In such scenarios, the exploits are not inherently linked to the RFID technology but rather to the quality of the design and coding of the middleware software components, which interact with the RFID devices. Researchers highlighted that RFID applications are potential candidates for exploitation by malware: they involve complex applications with a large amount of source code, rely on generic protocols and facilities as well as back-end databases, they process and store high-value data and, since nobody expects RFID malware yet, they convey a false sense of security.

4. Conclusion

RFID technologies are often presented by their advocates as the “next big IT revolution” and are subject to a considerable amount of communication and publicity, sometimes drifting to technology and marketing “hype” or sensationalism. This phenomenon may increase the visibility of a technology with significant potential benefits to business and individuals. But it may also be counterproductive. The complexity of RFID technologies, their technical variety, and the very large range of possible applications they enable make them prone to being misunderstood. Like any information technology, if RFID were implemented without appropriate consideration of how to address privacy and security risks, it might damage the organization that has deployed it, and cause harm to the individuals involved. Should significant risks be detected in existing or planned sensitive (*e.g.* passports, credit cards), large-scale (*e.g.* transportation systems) or striking (*e.g.* RFID implants) RFID systems, there would be a risk that RFID “hype” becomes RFID fear, damaging the perception of the technology by the general public and handicap its promising future.

Conclusion

RFID is still evolving, but nowadays many standards already exist. There are many possible use cases, applications etc. There are also many variants of technology. It is always a question about environment, when deciding on RFID application. There are many possible criteria to classify RFID systems. For example different frequencies may be used depending on needs and situation of particular organization. RFID is enabling technology,that enables creation of solutions delivering new values and enables error-prone,automatically collected data in real time.

References:

[1]. A. Bogdanov, Pl. Dqnkov, Analysis of used bar codes in logistics, Scientific forum NBU 2014

[2]. Radio Frequency IDentification: Applications and Implications for Consumers, 2005

[3]. RFID Journal. Online publication. Referenced 2005 at http://www.rfidjournal.com.

[4]. http://www.software.net.mx/en/prosoftp4p.htm.

[5]. http://www.bridge-project.eu/.

[6]. http://www.smart-rfid.eu/page.php?3.

[7]. http://www.stop-project.eu/PROJECT/tabid/57/Default.aspx.

[8]. http://www.rfid-in-action.eu/public/.

The present study is conducted with the financial help of Project № РД-08-90/03.02.2017, fund “Scientific studies” of Konstantin Preslavski University of Shumen.