IGI PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

ITJ4165

This paper appears in the publication, International Journal of Business Data Communications and Networking, Volume 4, Issue 2
edited by Jairo Gutierrez□□□□□□□□ □□□□

RFID:
New Technology on the Horizon for IT Majors

Eric Puffenbarger, James Madison University, USA

Faye P. Teer, James Madison University, USA

S. E. Kruck, James Madison University, USA

ABSTRACT

Educators have an ongoing challenge as they strive to stay up-to-date with new technology. One emerging technology, RFID (radio frequency identification) tags, has the potential to impact information systems in businesses as well as in our lives. Educators responsible for planning curriculum need to consider how to incorporate topics pertaining to RFID technology into a wide variety of technology courses. Therefore, one purpose of this manuscript is to give curriculum planners and teachers a summary of RFID by: presenting an overview of RFID technology; exploring RFID limitations and possible solutions; and examining the future outlook of RFID. An additional purpose further assists educators in considering how to incorporate this new course topic into the curriculum by providing some teaching resources, objectives and suggestions pertaining to RFID.

Keywords: *curriculum development; educational technology; instructional materials; telecommunications*

INTRODUCTION

Today's educators need to have a fundamental knowledge of a wide variety of evolving technology. It has been stated that teachers need to "cross-fertilize ideas across technology and research domains" (Kalles & Papagelis, 2006). To accomplish this, educators need to continually scan the horizon for developing technology.

One such emerging technology is RFID (radio frequency identification) tags. RFID tags are small, wireless devices that help identify objects, animals, and people.

RFID is just one part of the fast evolving telecommunications industry. Some educators have indicated that it is important for information technology students to learn more about the field of telecommunications (Choi, Teer, & Teer, 2005). As new course

material is considered, either for introductory IT (information technology) courses or more specific upper level IT courses, it is important for educators to learn about RFID and determine if some course coverage should be devoted to RFID.

One purpose of this manuscript is to give curriculum planners and teachers a summary of RFID by: presenting an overview of RFID technology; exploring RFID limitations and possible solutions; and examining the future outlook of RFID. An additional purpose is to provide teaching resources, objectives, and suggestions pertaining to RFID. Hopefully, this will further assist educators as they consider how to incorporate this new course topic into the curriculum.

OVERVIEW OF RFID TECHNOLOGY

RFID is a type of automatic identification similar to bar codes. The difference between the two is that in RFID systems, an electronic device uses radio frequencies to communicate, whereas bar codes require line-of-sight scanning. For example, these tags can be used to track objects in supply chains and can even be found in the pockets, belongings, and bodies of consumers.

There are two types of RFID tags currently being used, UHF (ultra high frequency) and HF (high frequency). Tags can further be classified as active, semi-passive, and passive. Active tags are the most expensive and contain an internal power source; passive tags are powered by external radio signals; semi-passive can function either way. RFID tags are given a unique EPC (electronic product code) and are installed with a transponder and digital memory chip. In addition to the EPC, the data contained within each tag may provide identification, location information, or product specifications.

The RFID system includes an electronic reader which enables data transmitted from tags to be read, stored, and eventually processed. The reader communicates with a host computer that runs software called middleware, which connects the data to specific applications. Readers are essentially a type of interrogator that use an antenna packaged with a transceiver and decoder. The reader sends out a signal that activates or "wakes up" a corresponding RFID tag which transmits its unique EPC code. Data can then be read from or written to the tag.

RFID tags are available in a variety of shapes and sizes, most of which are extremely small. RFID has made considerable progress recently with advancements in the technology, lower costs, and smaller tags. RFID systems have emerged as a practical auto-ID platform in industries as varied as automobile manufacturing, microchip fabrication, and even cattle herding (Weis, 2003). In some medical facilities, RFID tags are being used to double and triple check that the patient in the operating room is having the correct operation (Martin, 2005). RFID tags have also been used in disaster victim identification after the tsunami catastrophe in December 2004 (Meyer, Chansue, & Monticelli, 2006). Additional applications include the use of RFID to detect human activity. For example, an iGlove can track the objects grasped by the wearer. The iBracelet also tracks human activity and was found to be more aesthetically and ergonomically preferred to the glove (Smith et al., 2005). Current news articles indicate that RFID is being implemented in the areas of manufacturing and supply chain management (Loebbecke & Palmer, 2006). However, there are still several issues that

are preventing RFID tags from becoming more prominent in today's businesses and eventually replacing bar codes.

RFID: LIMITATIONS & POSSIBLE SOLUTIONS

Present limitations of RFID are primarily issues pertaining to security, privacy, and technology. In this section, these limitations will be explored and some possible solutions will be examined.

Security Issues

Security is one area of concern that is preventing the widespread adoption of RFID tags. Without the proper controls in place, private information could be stolen from products or other items containing RFID tags. Since most tags are passively powered and rely on wireless networks, they are open to attacks, which in some cases could be easier than picking someone's pocket. Security breaches to RFID tags could include physical attacks, counterfeiting, spoofing, eavesdropping, tracking, or denial of service (DoS). Any of these attacks would have a serious negative impact on a company as well as individual customers.

Security issues with RFID systems will first be analyzed by examining three main factors: availability, integrity, and confidentiality. These three pillars of security are referred to as the security triad (Glover & Bhatt, 2006).

Availability pertains to the system's uptime at the appropriate performance level or the amount of time that the system is available. Most system administrators would obviously prefer 100 percent availability, but there are various threats that negatively impact uptime. Poorly designed architectures are usually the most common reason for reductions in uptime. However, DoS attacks are another concern. This type of assault could occur when a criminal with the right tools and technology decides to send out a jamming radio signal in an RFID system that renders tags and readers useless.

Integrity addresses the accuracy and authenticity of the data transmitted. Some of the data transmitted via RFID usually includes a company's product and shipping information as well as customer data. Threats to data integrity include both accidental and malicious modification of the data in a system. An example of this type of attack is spoofing, which could occur when someone swaps the tag data for Product A with Product B data to gain some type of advantage.

Confidentiality relates to limiting the access of information to authorized personnel only. Private data about customers or company information involving inventory and supply chains could potentially be read or stolen by intruders. This also relates to the issue of privacy, which will be discussed later. All three of the factors in the security triad can impact each component of an RFID system from the actual tags to the enterprise information system.

RFID tag security is vulnerable because currently the data stored is plain text or unencrypted. Adding encryption requires more space on the tag that results in higher costs, increased processing time, and a larger chip, all of which increase the size of the tag (Glover & Bhatt, 2006). Also, tags can be removed or replaced unless there is some type of physical supervision for RFID tagged items. RFID tags essentially listen and respond to a signal no matter where it comes from or to where it is being sent. To demonstrate the ease of retrieving information from a RFID tag, a Netherlands security firm successfully decrypted a RFID

enabled passport in about two hours (White, 2006). The security firm was able to access a digitized fingerprint, photograph, and all other encrypted and plain text data on the passport by cracking a very predictable algorithm for the tag's password. Authorities in the United States had plans to implement a similar type of RFID tag in all American passports during the fall of 2006, but have now had to rethink the situation.

In a research study involving humans, an RFID tag called VeriChip was placed under the skin of Annalee Newitz. Applied Digital's VeriChip was approved by the FDA (Food and Drug Administration) on October 13, 2004, for medical purposes such as tracking patients and storing medical information (Reynolds, 2004). All of the data on the chip was read and copied in approximately two hours, giving access to all of Newitz's medical records and as well as other private data (Kuchinskas, 2006). This VeriChip would be subject to all the same issues as a product RFID tag and more.

RFID readers are also susceptible to attacks due to the fact that they are normally connected to an internal ethernet using either wireless or wired connections. Again, data that travels from tags to the reader is not encrypted and the tags that are being read are not authenticated by the reader. For these reasons RFID readers are vulnerable to spoofing, DoS, and protocol attacks. Basically, anyone who is connected to the same network, has access to a wireless sniffer device, and possesses a basic knowledge of RFID reader protocols could carry out such an attack. Other problems exist when readers experience a collision. This can happen when the coverage areas of two different readers overlap causing interference with one another (Lahiri, 2005). Similarly, the presence of another wireless network in close proximity can interfere with RFID readers.

Potential solutions to the threats facing RFID readers include: (1) encrypting the data; (2) requiring authentication and authorization before allowing access to a reader's services; (3) establishing a proper authentication process between tags and readers; (4) setting up proper security at wireless access points; (5) strict physical access control to the company's buildings; (6) installing surveillance to monitor merchandise tagged with RFID, (7) using rewritable tags only when appropriate; and (8) installing protection from Internet attacks using firewalls, intrusion detection systems, network sniffers, and better anti-collision protocols. Collisions can also be somewhat solved with TDMA (time division multiple access) algorithms, which instructs each reader to read at different times or intervals (Lahiri, 2005). However, this would also require an intelligent filtering system to prevent tags from being read more than once.

The RFID service bus is another area susceptible to attacks. The service bus contains all middleware components such as the object naming device, EPC event manager, EPCIS server, and the RFID integration server. Middleware essentially allows communication between the data being read and the corporate information system. Threats to this area would most likely be in the form of corporate spies, espionage agents, and intruders. With the right tools, they could gain access to key company information, trade secrets, and other private data that could potentially cause harm. To solve RFID service bus security problems, companies need to seriously consider controlling access to the network using firewalls, intrusion detection systems, and network sniffers. It would also be a

good idea to set up a security infrastructure that will define which network users will be authenticated.

Additional help in providing the needed security infrastructure can be provided in the future by standards organizations. For example, EPCglobal, an international standards organization, maintains an EPC database, which identifies manufacturer, product, version, and serial number. Other functions performed by EPCglobal include providing middleware specifications for data exchange and administering the object name service for matching an EPC to information about the associated item. EPCglobal is currently working on specifications to secure EPCIS communications as well (Claburn & Hulme, 2004).

Finally, EIS (enterprise information system) security flaws have to be addressed. This system includes corporate assets such as the directory, identity management, access control, messaging systems, and a database that uses RFID data. RFID systems generate large amounts of transaction data. Companies utilizing RFID will be storing large volumes of potentially sensitive information that could overwhelm the existing network. As a result, this leaves the system open to intruders, corporate spies, and pranksters. For example, if business sales and or inventory information was stolen it could result in huge financial losses. Plausible solutions include adequate network access control and physical access control to corporate premises. As RFID technology continues to improve, prices will probably drop allowing security methods to become more affordable.

Privacy Issues

Privacy is the right to be left alone when you want to be (Warren & Brandeis, 1890), to have control over you own personal possessions, and not to be observed without your consent (Haag, Baltsman, & Phillips, 2005). Certain types and uses of RFID tags definitely impact privacy (Peslak, 2005). The Pentagon, for example, plans to use RFID to track physical objects; such use raises relatively modest privacy concerns. The San Francisco Library would like to put RFID chips in its books, raising the specter of third parties being able to track our reading choices. Even more troubling are proposals to put RFID chips into government issued identity documents (RFID Technology, 2004). The main concern is that this new technology will lead to the tracking of consumers and possible exposure of private information. Consumer information could be queried by marketers for the purpose of delivering personalized ads.

Further along the continuum of privacy concerns would be thieves using RFID technology to commit identity theft. Eventually, everyday products could be numbered, identified, cataloged, and tracked wherever readers are present (Flint, 2006). RFID tags could also end up inside many types of personal documents like driver's licenses, passports, diplomas, and similar documents (Granneman, 2003). Currently, there is no law requiring that product labels indicate the presence of an RFID tag. The current privacy gap with RFID tags exists because market penetration is moving faster than policy (Kuchinskas, 2006). Those who purchase RFID tagged merchandise, have RFID implants, or other tagged items could be unknowingly exposed to readers, identified, and singled-out. Table 1 summarizes some RFID privacy concerns.

Many steps are being taken to protect consumer privacy. However, there is a delicate balance between satisfying the privacy-rights advocates and meeting the

Table 1. RFID privacy concerns (Glover & Bhatt, 2006, p 202)

RFID Characteristic	Privacy Concerns
• No line of sight • RFID tag is read just by being in close proximity to reader	• Unauthorized person can read your RFID-tagged items from safe distance • Most consumers will not be aware of the tags or that the items are being tracked
• Item-level tracking • RFID tags have higher information storage capacities than most bar codes • RFID tags may include a serial number • Manufacturers and retailers can track items at an instance level • Provides companies with a valuable tool for tracking and managing inventories, sales data, and other product information	• Can potentially be used to identify unique individuals with the objects purchased • The capability to track goods at item level, associate them with individuals, and then be able to automatically locate them in public places causes the most concern among privacy advocates

needs of the business world trying to fully benefit from RFID technology.

In the United States, government legislation regarding RFID privacy has been introduced in many states, but has failed in the majority of cases. Most of these bills will almost certainly be revised and reintroduced in the near future. Two notable bills were the RFID Right to Know Act of 2004, introduced by Missouri Senator Maida Coleman, and a California bill known as SB1834. The RFID Right to Know Act requires that any items with RFID tags have to be packaged with a clearly visible label notifying customers of the tag. SB1834 restricted the use of RFID tags and readers to relating only to product information; thus, customer identification is not utilized. SB1834 required that RFID be studied more carefully before being used in government issued ID cards (Torrieri, 2006).

The E.U. data protection laws require any data that can be directly identified to an individual be subject to Data Protection Directive (95/46). This directive includes several requirements: collection when only necessary and relevant; retention for only as long as necessary; and informed consent, which means a label must include details of how the information in the RFID tag will be used and instructions to the consumer how to disable or remove the tag. (Archer & Salazar, 2005).

There have also been numerous RFID privacy guidelines released by various organizations. For example EPCglobal has set the following guidelines (Glover & Bhatt, 2006, p 205-206):

- **Consumer notice:** This guideline requires that consumers be given a clear notice of the presence of EPC tags on products or their packaging. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

- **Consumer choice:** This guideline requires that consumers be informed of their choices to discard, remove, or disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags will be part of disposable packaging or will otherwise be discardable.
- **Consumer education:** Consumer education is key to dispelling some of the myths about RFID's benefits, capabilities, and limitations. EPCGlobal, working along with its member companies, will strive to provide consumers with the opportunity to obtain accurate information about RFID and its applications, as well as information about advances in the technology.
- **Record use, retention, and security:** The EPC should not contain, collect, or store any personally identifying information. As with conventional bar code technology, data associated with an EPC will be collected, used, maintained, stored, and protected by the EPCGlobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use, and protection of any personally identifying information associated with their use of EPC.

Dr. Garfinkel, of MIT, introduced a set of RFID privacy policies in 2002 to protect consumers, which he titled the "RFID Bill of Rights" (Glover & Bhatt, 2006). In the bill, he outlined several guidelines similar to those released by EPCglobal. Well-established organizations, such as CASPIAN (Consumers Against Supermarket Privacy Invasion), the ACLU (American Civil Liberties Union, Privacy International, METI (Ministry of Economy, Trade, and Industry), and EPIC (Electronic Privacy Information Center), among others, have all played a part in attempting to enact legislation regarding RFID technology.

Measures to protect privacy can also be implemented by companies themselves by taking advantage of technological advancements. The simplest and most appealing way is to use kill commands or killer tags introduced by EPCglobal. They allow customers to request that RFID tags on purchased items be disabled or killed by the retailer before leaving the store or business location. Basically, a command is sent to the tag ordering it to render itself useless, thereby protecting consumers from unauthorized identification or tracking. On the other hand, this limits the usefulness of the technology to the point of sale and it could mean longer waiting times if customers decided to have all purchased items disabled. Another method is to use blocker tags developed by RSA Security. A blocker tag is a special type of RFID tag that prevents unwanted scanning of tags (Juels, 2005). Blocker tags work by passively jamming RFID readers, thus preventing other tags from being read. A potential drawback is that blocker tags could cause problems with individuals attempting to commit robberies by hiding products at checkout lines. Screaming tags could also be used by consumers which send out a strong signal burst to prevent other tags from being read.

Technology Issues

Several problems exist with the actual RFID technology. It is still an immature technology that is in the early adopters phase. Rapid upgrades are occurring, but this can also act as an inconvenience to businesses. Tags can be damaged or destroyed under current

handling techniques; defective tag rates can be as high as 20 percent (Lahiri, 2005). RF-opaque and RF-absorbent materials can cause the technology to fail. For instance, if an RF-absorbent substance like water interferes with a tag or if an RF-opaque material, such as metal is tagged, a reader may fail to read the tags. Radio frequencies also cannot pass through another human, which could create problems in high traffic areas. Another limitation for tags is they can easily be affected by environmental factors and surrounding conditions. If RFID tags get wet, they could be disabled or at least have their functionality damaged. UHF tags are currently being used mostly for warehouse supply-chain tracking and HF tags are used for item-level tracking (Schuman, 2006). UHF will start to replace HF tags at item-level, but if they continue to experience error rates a seesaw effect could be created between the usage rates of UHF and HF RFID tags.

RFID readers can be affected by the presence of an additional wireless network or by noise created from nearby electric motors. Incorrect hardware setup such as a wrong antenna placement could cause failure as well (Lahiri, 2005). Only a few tags can be read per second and, as mentioned earlier, readers can experience collisions. Universal RFID technology standards are not in place; therefore, you can have the same type of tags from different vendors perform differently. There does not seem to be a reliable timetable for when the standards issue will be resolved. It is a learning process and there are still not many RFID experts. Business owners should stay patient and when necessary, seek the guidance of consultants that have experience with RFID systems.

Presently, old-fashioned barcodes continue to provide greater stability to businesses. About five billion barcodes are scanned everyday and, with more than 50 existing standards, barcoding is the most widely deployed technology in the world (Lahiri, 2005). Furthermore barcodes cost less, have better accuracy rates, can be placed on almost any material, do not threaten privacy, and are secure. Nevertheless, as RFID technology continues to evolve, business people can research the benefits that an RFID system could provide and determine the technology that works best for a particular application.

Cost is usually the most common reason cited for not using RFID technology. Tags are priced around 20 cents or more depending on the type and features. This price must drop below five cents and in most cases as low as one cent before most businesses will accept it. When comparing the cost of RFID with barcodes, there are many significant differences. Barcode readers generally cost less than $400, while RFID readers can sometimes exceed $800. Installing an RFID system would also involve the time consuming and costly tasks of restructuring the IT infrastructure, training personnel, and educating customers. A survey conducted by AMR Research has shown that RFID in 2005 had an average budget of more than $548K and could increase to $771K by 2007 (Reilly, 2005). Furthermore, RFID systems are very complex to design and implement. As RFID technology improves, prices should continue to drop. Business managers should set a price threshold at which RFID becomes a realistic technological solution; next, they should reevaluate the current situation when this price threshold is reached.

FUTURE OUTLOOK

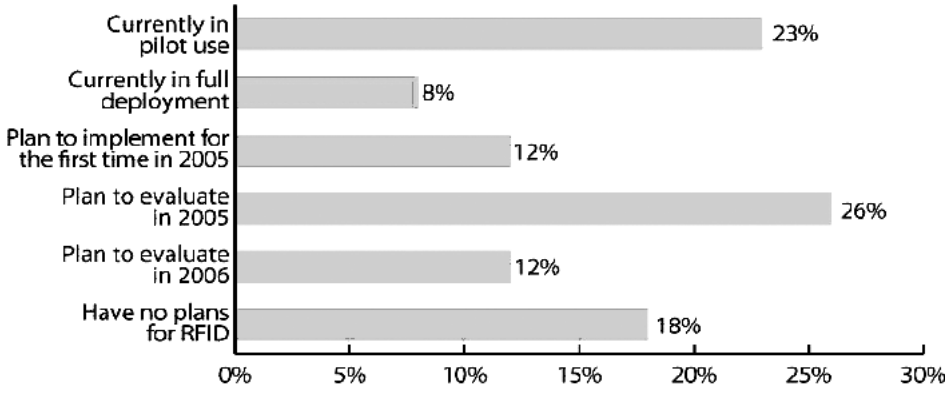
The major push towards adopting RFID technology came when both Wal-Mart and

the Department of Defense issued mandates requiring that their top 100 suppliers begin using RFID tags in shipments (Brewin, 2003). Wal-Mart underestimated many of the problems with RFID, such as the cost, and as a result deadlines were not met (Feder, 2004). Wal-Mart and other corporations continue to test various RFID tracking systems. Examples of these trials include Benetton tracking apparel, Gillette tracking consumer packaged goods, Michelin tracking tires, the European Central Bank tracking paper currency, hospitals tracking patients and personnel, and payment systems like Exxon Mobil's SpeedPass™ (Electronic Privacy Information Center, 2006). Ford Motor Company's use of RFID in their Dearborn plant was very successful. Ford is currently planning to implement RFID technology in four additional plants (Hamblen, 2006).

Eventually RFID tags will be placed in objects not just to store and track information, but to make those objects smart, more useful, easier to maintain, and easier to recycle (Roberti, 2006b). Thus, as new applications for RFID are created, new business opportunities will flourish. These types of applications could be smart shelves that know all of their contents courtesy of internal RFID readers or smart refrigerators that work in a similar fashion.

Over the next year or two we can probably expect to see key advancements being made in RFID technology, falling prices, and agreeable standards and protocols being passed. As that happens, RFID's place in our society will start to take shape. Research has indicated that some companies are re-examining the use of barcodes and may implement RFID tags where they are cost-effective and make the most sense (Eschinger, 2005; Reilly, 2005; Roberti, 2006a). AMR Research surveyed 500 companies in order to assess the RFID market from 2005 through 2007 (Reilly, 2005). At the time of the AMR Research survey, 31 percent of the respondents were in full deployment or in pilot use of RFID. Twelve percent responded that their

Figure 1. RFID deployment survey (Reilly, 2005)



company planned to implement RFID in 2005; 26 percent said their company would evaluate RFID in 2005; and 12 percent said their company would evaluate RFID in 2006. The results of the AMR Research survey are presented in Figure 1. A Gartner research reports states that in 2007 there will be a 50 percent annual growth in RFID sales (Eschinger, 2005). This is illustrated in Figure 2.

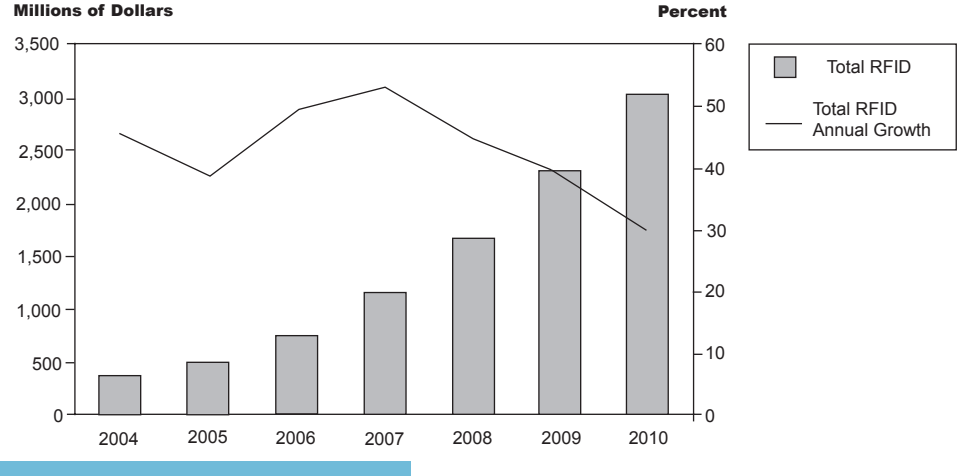
IMPLICATIONS FOR EDUCATORS

Because of the high cost of deployment and the impact on existing IT infrastructures, it seems that in the past users have been reluctant to adopt RFID (Webster, 2006). Even though RFID still has many limitations to be addressed, some have predicted that 2007 will be the year that RFID technology takes off (Eschinger, 2005b; Roberti, 2006).

Recently Comp TIA (Computer Technology Industry Association) announced a RFID certification in an effort to develop the workforce and provide the industry with a standard for measuring employee competency in RFID technology (Certification Magazine, 2006). IT certifications, such as RFID certification, typically developed and administered by a manufacturer or a professional organization can have numerous benefits. Some of advantages include: acquiring knowledge and skills that allow individuals to move into a new area; gaining exposure to the latest software or technology; increasing an individuals level of expertise; and gaining the ability to contact and network with world-wide top-performing professionals in the field (Al-Rawi, Lansari, & Bouslama, 2005).

One of the hardest things for IT educators to do is to it stay current with evolving technology. As we examine and develop our curriculum and course content, we may find that it is time to integrate topics pertaining to RFID technology within the various technology courses we teach. Some universities have incorporated RFID into their curriculum with support from business while others will need to do this on their own (SAP Gift to IU Kelley School of Business enables hands-on experiences, 2004). Some universities may want to develop a stand alone RFID course. Such courses could be

Figure 2. RFID, worldwide size and growth (Eschinger, 2005)



centered on concepts such as RFID's use in the supply chain or RFID's application in manufacturing systems. If the curriculum does not have room for a stand alone course in RFID, these topics can be incorporated into such courses as the introductory or an intermediate computer information systems course or a telecom course.

Teaching Resources

Educators need to learn more about this technology and develop teaching materials. Currently most of the available teaching reference material for RFID is in the form of (1) professional organizations, (2) books, (3) journals, and (4) Internet resources.

- **Professional organizations:** The Wireless Communications Alliance has a special interest group for those interested in RFID and is located at http://www.wca.org/RFID_info.htm. The Colorado RFID Alliance is a non-profit organization dedicated to bringing together the RFID community in the eastern part of Colorado and is located at http://corfida.org/.
- **Books:** Numerous books were found on the topic of RFID. Information on these books is given in Table 2.
- **Journals:** There is only one refereed journal, The International Journal of Radio Frequency Identification Technology and Applications, which began in 2007 according to Ulrich's Periodical Directory.
- **Internet resources:** While one has to be cautious about the credibility of the Internet resources, there are some excellent Internet sources on RFID. They are primarily targeted to business and industry professionals. Some of the more noteworthy are:
  1. RFID Journal—http://www.rfid-journal.com/. Highlights of this online journal are useful in preparing to teach topics related to RFID. Those most notable for educators include: glossary of terms, global news articles, case studies, white papers, and Webinars. Numerous parts of the journal are open to non-subscribers; there are some items that are available only to fee paying subscribers.
  2. RFID product news—http://www.rfidproductnews.com/. Includes feature articles, information on new products, whitepapers, infor-

Table 2. Books relevant to RFID

Authors	Title	Year	Publisher
Bhuptani, Manish & Moradpour, Shahram	RFID Field Guide: Deploying Radio Frequency Identification Systems	2005	Prentice Hall
Glover, Bill & Bhatt, Himanshu	RFID Essentials (Theory in Practice)	2006	O'Reilly
Graafstra, Amal	RFID Toys: 11 Cool Projects for Home, Office and Entertainment	2006	ExtremeTech
Garfinkel, Simson & Rosenberg, Beth	RFID: Applications, Security, and Privacy	2005	Addison-Wesley Professional
Sweeney, Patrick J.	RFID for Dummies	2005	Wiley

mation on current events, and case studies.

3. RFID directory, UK—http://www.rfid.uk.com/. Contains directories of RFID companies, manufacturers and suppliers.
4. RFID 101.com—Info guide to radio frequency identification (RFID) technology—http://www.rfid-101.com/. An online guide to selecting and purchasing RFID technology products.

Teaching Objectives and Suggestions

Lectures utilizing material obtained through professional organizations, books, journals, and the Internet can be utilized to assist in building a framework of understanding that will enhance the students' understanding of assigned readings and projects. The course syllabus should include the objectives and detailed assignment guidelines for course projects; a description of the course deliverables; and the course evaluation criteria. Some suggested course objectives include:

- Types of RFID technology
- How RFID is being utilized today
- Security and privacy issues with RFID
- Future of RFID technology

In addition to lectures, three specific course activities can be considered: (1) an individual research project; (2) a group research project; and (3) a hands-on project.

It is recommended that the performance of research projects be monitored by requiring the students to turn in two or three interim deliverables at predefined points in the research project. The deliverables from the research projects should be evaluated on content, format, style, and other predefined criteria.

- **Individual research project:** The instructor should provide the students with a list of possible research topics from which each student selects a topic of interest. These topics should coincide with current issues pertaining to RFID. To aid the undergraduate students in the literature search necessary for their research, it is suggested that a professional librarian from the university library be invited to class to provide a tutorial on utilizing research databases.
- **Group research project:** Group research projects can be assigned to groups of three or four students. The group research project will be useful in stimulating the students' learning of new and interdisciplinary concepts in the more flexible and comfortable learning environment of the peer education process. This will also provide students with experience in working in teams, a skill that they need to further develop and practice before entering the workplace.

It is recommended that the group research topic be based on a real world business utilizing RFID. Using real world cases in the group research projects will afford students the opportunity to experience first hand things such as realistic content, real world business objectives, organizational impacts, social values, and ethical issues (Gendron & Jarmoszko, 2003; Hackney, McMaster, & Harris, 2003). The professor will need to guide the students in the selection of a real world case. The students can

be asked to complete their group research project as follows:

1. Describe in detail a specific real world company's application of RFID.
2. Survey the existing literature regarding the specific company's application of RFID and summarize the literature related to that application.
3. If possible, describe the company's future plans regarding RFID.

At the completion of the projects, each group can present the results of their final group research project to the entire class. In addition to a class presentation utilizing presentation software such as Microsoft PowerPoint ™, the students can provide the professor with a presentation file, a written project report, and a few test questions the group feels the class could answer after listening to the formal presentation. The questions collected from all the groups may be used on an exam to test the level of understanding of all students on all research project presentations. Such a procedure can be very useful in garnering student attentiveness during all group presentations. The instructor and all class members may evaluate each of the group research presentations based on pre-arranged guidelines.

- **Hands-on practice using RFID:** To enhance the students understanding of technology and its application in the real world, it is important to give students hands-on experience with technology in a lab environment (Greca, Cook, & Harris, 2004). Robert Yoder (2006) utilizes an inexpensive RFID reader and tags in a university lab setting to teach a variety of basic principles. Hands-on practice opportunities, in which the students actually work with RFID components, will be beneficial in enhancing the students' understanding of the course's technical components. Depending upon the learning environment desired by the professor, the hands-on practice opportunities can be offered as lab sessions or as individual take-home assignments.

SUMMARY

Since RFID has the potential to have an impact on information systems in businesses as well as in our lives, it is important that we incorporate topics pertaining to RFID into existing courses and, where applicable, develop in-depth, stand-alone courses on RFID.

The overview of RFID and implications for teaching should be of interest to several groups of readers. Researchers in academic communities should be aware of the important role of RFID in industry and the resulting implications for needed IT research. Second, IT curriculum planners will find this information helpful as they strive to keep the curriculum in tune with the needs of business and industry. Third, IT professors need to be aware of the importance of RFID. Hopefully, IT professors can benefit from the teaching resources and teaching suggestions presented.

REFERENCES

Al-Rawi, A., Lansari, A., & Bouslama, F. (2005). A holistic approach to develop IS curricula: Focusing on accreditation and IT certification. *Journal of Information Technology Education*, *4*, 307-327.

Archer, Q., & Salzar, G. (2005). RFID: a threat to privacy? *Computer Weekly*, *April 5*, 18.

Brewin, B. (2003). Military orders suppliers to use RFID technology. *Computerworld,*

Certification Magazine. (2006). Program updates. *Certification Magazine*, 8.

Choi, Y.B., Teer, F.P., & Teer, H.B. (2005). Management of telecommunications services: A vital new content area and a course model for the college of business. *International Journal of Information Communication Technology Education*, *1*(3), 60-73.

Claburn, T., & Hulme, G. (2004). RFID's security challenge. *Information Week*. Retrieved February 10, 2006, from http://www.informationweek.com/story/showArticle.jhtml?articleID=52601030&tid=13690

Electronic Privacy Information Center (2006). *Radio frequency identification (RFID) systems*. Retrieved February 10, 2006, from http://www.epic.org/privacy/rfid/

Eschinger, C. (2005, November 2). Market share and forecast: Radio frequency identification, worldwide. *Gartner Research*, 2004-2010.

Feder, B. (2004). Wal-mart hits snags in push to use radio tags to track goods. *New York Times*, *Section C, Page 14, Column 5*.

Flint, D. (2006). RFID tags, security and the individual. *Computer Law & Security Report*, *22*, 165-168.

Gendron, M., & Jarmoszko, A.T. (2003). The integration of technology theory and business analysis: A pedagogical framework for the undergraduate MIS course in data communications and networking. *Journal of Information Systems Education*, *14*(4), 361-371.

Glover, B., & Bhatt, H. (2006). *RFID essentials*. Sebastopol, CA: O'Reilly Media.

Granneman, S. (2003). RFID chips are here. *Security Focus*. Retrieved February 9, 2006, from http://www.securityfocus.com/columnists/169

Greca, A.N., Cook, R.P. & Harris, J.K. (2004). Enhancing learning in a data communication and networking course with laboratory experiments. *The Journal of Computing in Small Colleges, 19*(3), 79-88.

Haag, S., Baltzman, P., & Phillips, A. (2005). *Business driven technology*. New York: McGraw Hill.

Hackney, R., McMaster, T., & Harris, A.J. (2003). Using cases as a teaching tool in IS education. *Journal of Information Systems Education*, *14*(3), 229-234.

Hamblen, M. (2006). RFID Successes highlighted at mobile & wireless world. *ComputerWorld*. Retrieved May 26, 2006, from http://cwflyris.computerworld.com/t/553965/225881/20662/0/

Juels, A. (2005). *RFID security and privacy: A research survey*. RSA Laboratories. Retrieved February 11, 2006 from, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

Kalles, D., & Papagelis, A. (2006). Managing the decision tree life-cycle with components. *International Journal of Information Communication Technology Education*, *2*(3), 1-13.

Kuchinskas, S. (2006). The new chip-erati. *Internetnews.com*. Retrieved February 9, 2006, from http://www.internetnews.com/security/article.php/3582971

Lahiri, S. (2005). *RFID sourcebook*. Westford, MA: IBM Press.

Loebbecke, C., & Palmer, J. (2006). RFID in the fashion industry. *Management Information Systems Quarterly Executive*, *5*(2), 15-25.

Martin, Z. (2005). RFID tags help identify patients before surgery. *Health Data Management*, *13*(7), 14-22.

Meyer, H. J., Chansue, N., & Monticelli, F. (2006). Implantation of radio frequency identification device (RFID) microchip in disaster victim identification (DVI). *Forensic Sciences International*, *157*, 168-171.

Peslak, A. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, *59*, 327-345.

Reilly, K. (2005). AMR research survey finds 69 percent of respondents plan to evaluate, pilot, or implement RFID in 2005. *AMR Research*, July. Retrieved May 17, 2006, from http://www.amrresearch.com/Content/View.asp?pmillid=18470

Reynolds, M. (2004). RFID implants need better privacy protection. *Gartner Web*. Retrieved February 10, 2006, from the Gartner Web database.

RFID Technology: What the Future Holds For Commerce, Security, and the Consumer: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, United States House of Representatives, 108th Cong., 2nd sess. 1 (2004). Retrieved from the Computer & Information Systems Abstracts database.

Roberti, M. (2006a). The bar code is back! *RFID Journal*. Retrieved February 10, 2006m from http://www.rfidjournal.com/article/articleview/2123/1/128/

Roberti, M. (2006b). Forecasts for RFID in 2006. *RFID Journal*. Retrieved February 10, 2006m from http://www.rfidjournal.com/article/articleview/2066/1/2/

SAP gift to IU Kelley School of Business enables hands-on experiences. (2004). Retrieved September 13, 2006m from http://newsinfo.iu.edu/news/page/normal/1761.html

Schuman, E. (2006). Finding ways around RFID's errors. *Extreme Nano*. Retrieved February 11, 2006m from http://www.extremenano.com/article/Finding+Ways+Around+RFIDs+Errors/169743_2.aspx

Smith, J. R., Fishkin, K. P., Jiang, B., Mamishev, A., Philipose, M., Rea, A. D., et al. (2005). RFID-based techniques for human-activity detection. *Communications of the ACM*, *48* (9), 39-44.

Torrieri, M. (2006). California RFID bill holds as senator considers industry concerns. *RFID News*. Retrieved February 10, 2006, from http://www.rfidnews.org/library/2006/02/01/california-rfid-bill-holds-as-senator-considers-industry-concerns/

Warren, S., & Brandeis L. (1890). The right to privacy. Originally published in *Harvard Law Review* 4 (5). Retrieved from http://www.lawrence.edu/fast/BOARDMAW/Privacy_brand_warr2.html

Webster, J. (2006). Forecast 2006: RFID cost and complexity continue to block enterprise use. *Computer World*. Retrieved February 11, 2006 from http://www.computerworld.com/managementtopics/management/story/0,10801,107308,00.html?source=x2305

Weis, S. (2003). Security and privacy in radio-frequency identification devices. *Massachusetts Institute of Technology*. Retrieved February 9, 2006, from http://theory.lcs.mit.edu/~cis/theses/weismasters.pdf#search='stephen%20august%20weis

White, D. (2006). Global RFID passport encryption standard cracked in 2 hours. *MobileMag*. Retrieved February 10, 2006, from http://www.mobilemag.com/content/100/102/C6340/

Yoder, R. C. (2006). Using RFID in the classroom to teach information systems principles. *Journal of Computing Sciences in Colleges*, *21*(6), 123-129.

Eric Puffenbarger is a Web designer at Musictoday, LLC in Crozet, Virginia. He graduated from James Madison University in 2006. He was an active member of the Association for Information Technology Professionals (AITP) at JMU. A manuscript written by Puffenbarger won honorable mention at the AITP national competition in Dallas in 2006.

Faye Teer is professor of information systems in the Computer Information Systems and Management Science Department at James Madison University. Dr. Teer received the Doctor of Business Administration degree from Louisiana Tech University in 1985. She has taught statistics and computer information systems courses at James Madison University since 1986. Her research, primarily in the area of curriculum development, has resulted in publications in a variety of journals.

S. E. Kruck is an associate professor in the College of Business at James Madison University and teaches in the Computer Information Systems and Management Science Department. Dr. Kruck earned a PhD from the Department of Accounting and Information Systems at Virginia Polytechnic and State University and has published articles in Journal of Computer Information System; Journal of End User Computing; Journal of Information Systems Education; Information Management and Computer Security; Journal of International Information Management; Journal of Accounting Education*; and many others. Dr. Kruck on the editorial board of* Journal of Computer Information System and Information Management and Computer Security *is also a CPA in the state of Virginia and has over twelve years of corporate accounting experience.*

This work was previously published in the Int'l J. of Information and Communication Technology Education, Volume 3, Issue 4, edited by L. Tomei, pp. 50-63, copyright 2007 by IGI Publishing, formerly known as Idea Group Publishing (an imprint of IGI Global).