A Survey on Framework of location-aware RFID application service system with encryption and decryption techniques

Author1: V.Sree Rekha, Lecturer in Computer Science, Sri Durga Malleswara Siddhartha Mahila Kalasala, Vijayawada.

Author2: Dr.R. Padmavathy, Lecturer in Commerce, Montessori Mahila Kalasala, Vijayawada.

Abstract

Radio Frequency IDentification is one of the famous wireless induction system. It consists of tag, reader and application. Each RFID tag in this system is assumed as a unique ID itself. When an independent tag approaches antenna then the induction takes place between them. Where the antenna reads the information and content is recorded in the tag. The information is then translated into the computational data by the reader. Due to the tag portability and untouched data transmission in wireless applications for tracking based on these systems were proposed. These tags are small transponders that respond for the user queries from a reader by transmitting a serial number or some identifier wirelessly. They are frequently used to track items in production environments as an advanced barcode and to label items in supermarkets. This paper presents a few applications that are possible using RFID technology by tracking lost items, identify moving objects etc. Due to the usage of such technology there is need to provide privacy and propose certain solutions. In recent years, RFID systems are used to trace objects and asset worldwide. In addition, few supply chain management systems can be combined with RFID to form goods tracking systems and help enterprises to manage their raw materials and utilisation of products. More number of applications were introduced by people for their quick processing of objects in a short time efficiently.

Keywords

Induction, RFID, antenna, tag, portability, transponders, queries, identifier, barcode, technology, privacy, solutions.

Introduction

For the purpose that the right of intellectual property and the right of the valid users are further protected and maintained, integration of the software and hardware encryption is needed. Since each RFID tag with a unique ID (UID) which records the on demand information can be used as the individual identification, the small and cheap RFID tag can be considered as the hardware/software encryption/decryption key corresponding to the files or applications. In the next section, we give some descriptions for related RFID application and system. RFID tags are used to identify hardware in any application. They are used in health care where patients must always wear the tag designed for identification. The location and condition of the patient is monitored regularly at all times within the health unit due to the short distance wireless signal. To protect such hardware many software applications are introduced to adopt software encryption as the identification to protect the intellectual property of the applications. By considering the serious situations of pirate, intellectual property protection is important and famous issue. Password protection is the best method to protect any application. Software is designed in such a way that it is assigned a serial number or some calculated function to process it. Through a valid authentication only one can access the software to enable the application.

Password protection is the popular encryption method to protect the applications. Each application or file of software is assigned an on demand given serial numbers or calculation function. People who use this application have to input the correct serial number then enable the application. Considering today's applications, personal multimedia services or software applications are popular. Customers use the personal multimedia devices such as MP3, PDA, iPod, Laptop, etc., to download the multimedia or application files from the server or website via Internet. In other words, many files or data are disseminated and exchanged via Internet. In addition, many hackers can crash the software encryption with fewer costs. It makes that the piratical files are transmitted widely and the protection of intellectual property exists in name only.

RFID encryption and decryption for intellectual property protection

Authentication

The goal of authentication is to make sure that an entity is what it claims to be. In the context of RFID it means that tags can distinguish authorized readers from other readers. This can be done by using encryption with a preshared key. The other way around is much more difficult. Here a reader has to ensure that the tag it is reading is not altered or copied. As it turns out it is a rather hard problem. Encryption is typically used to establish some trust between both participants of a conversation (in addition to privacy). The main problem for this approach is the very limited resources on the tag itself. Most tags have only a few hundred logic gates, but most encryption Scheme. In addition to weaknesses in encryption algorithms themselves, RFID tags provide unwillingly more help to break those algorithms. Many current tags "export" lower layer properties, such as the power and timing of the back scattered signal and the processing delay which differ from input to input. That extra information can be used to break encryption even more easily. Newer tags try to fix that problem by two independent circuits for computation and back scattering.

Due to the demand of existed system integration, some applications related to RFID Encryption and Decryption for Intellectual Property Protection includes: PnP Middleware, RFID Hardware, End User RFID Device and End User RFID Tag, and Encryption/Decryption Procedure. For a normal user, there are two types of RFID devices for the encryption/decryption on RFID system (E/DonRFID system): End User RFID Device for digital content or multimedia information gaining, and End User RFID Tag for in dentifying the legal user. E/DonRFID not only provides the RFID based protection procedure but also includes the Encryption/Decryption method based on RFID character. The encryption and decryption can be implemented by hardware or software solution. The original digital data is encrypted by hardware, software, or combination of hardware and software,

The expected proliferation of RFID tags into the billions has raised many privacy and security concerns. A common concern is the loss of privacy when companies scan tags to acquire information about customers and then using data mining techniques to create individual profiles. This section describes possible scenarios where RFID tags can be exploited. Then it describes what mechanisms exist to defeat those threats or at least make them harder to execute. After that the section concentrates on attacks that are directed against RFID systems.

As RFID technology becomes more sophisticated and item level tagging promises more control and large savings in the supply chain management, companies are tagging items within their production process. To maximize the benefits companies start to require their suppliers to label all items delivered to the company. Anti-RFID activists created a few scenarios to show possible exploits if no precautions are taken. The most common one the unauthorized scanning of tags in order to create user profiles. Other scenarios are scanning the medication a person is carrying to conjecture what illness the person might suffer, or a mugger scanning a crowd of people and singling out a person carrying many valuable items (even money, if tagged as proposed). If tags are replacing credit cards eavesdropping becomes also a problem and must be addressed. The above mentioned issues are privacy concerns, but they are not the only issue. Authentication is also needed. For example, newer tags have rewritable memory available to store extra information during the production process. If stores rely on that information to determine the sales price for example, care must be taken so that customers do not change the type of the item to a cheaper one using portable readers. Also the kill command, a mechanism to permanently disable a tag, must be protected from unauthorized access. Recently a paper raised some concerns in the RFID community that claimed that cell phones can be reprogrammed to disable HF tags. In case that tags carry personal information (such as medical history, credit card numbers) a reader has to be authenticated and authorized before it is allowed access the data. In the previous examples the reader has to authenticate to the tag, there are also scenarios when the tag has to authenticate to the reader, for example to detect forged tags.

Corresponding to the encryption method, suitable RFID tag of user for decrypting is needed. Since three possible ways to protect the digital content are proposed, for the end users, there will be at least three possible states and method of E/DonRFID Encryption/Decryption, to gain the protected digital data, shown as follows:

- Encryption and Decryption by Hardware and Software combination,
- Encryption only by Hardware with Hardware and Software combination Decryption
- Encryption only by Software with Hardware and Software combination Decryption
- Encryption only by Hardware with Hardware Decryption
- Encryption only by Software with Hardware Decryption

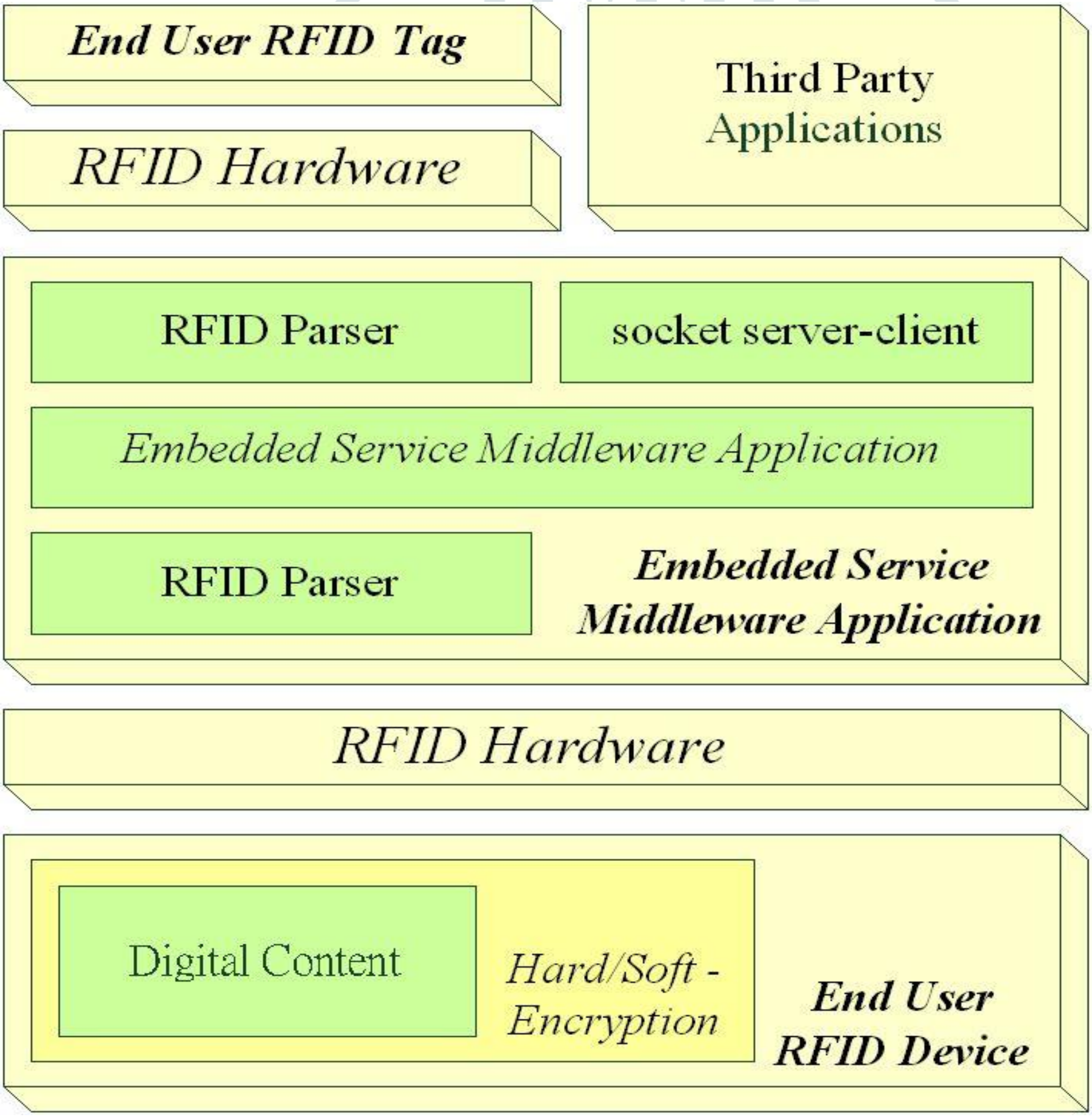

Figure 1

The framework of RFID Encryption and Decryption for Intellectual Property Protection

Process

First, depending on the digital content storage hardware such as CD-ROM disk, the commercial RFID tag can be embedded into the disk when the disk is made. According to the characteristic of RFID tag, each RFID tag can be set with different individualities. The different encryption code, unique ID, information of the digital content, or authentication serial number can be recorded in the RFID tag. In addition, the RFID tag embedded in the disk is not rewritable. Hence, different disks equip the different IDs of RFID tag. When the RFID reader inducts the tag, the information about this storage can be scanned and presented. In other words, only the digital storage with the valid RFID tag is legal and true.

Second, since the content or data are digital, these software, content or data, can be encrypted as the secret codes or cipher. The key for encryption and decryption can be recorded in the RFID tag. Without the specific key, these secret codes or ciphers cannot be recovered as the original data. In other words, the digital content that recorded in the storage device (such as CD-ROM disk) can be secured. The decryption key can be recorded in the RFID tag embedded in the storage or a palm RFID tag (such as a RFID toy).

For the end users, End User RFID Device/Tag is used. The storage, whether hardware (CD-ROM) which includes the encrypted digital content, or software (files or ciphers), is called End User RFID Device. If the End User RFID Device is hardware, the third party RFID Hardware can induct the RFID tag embedded in the hardware. After identifying the End User RFID Device, the application or user can execute and read the digital content if only Hardware - Encryption/Decryption is used.

According to three possible states, the end user must have the decryption key for executing the digital content. In this paper, the hardware (RFID tag) or software for the decryption key is called End User RFID Tag. After identifying the End User RFID Device, the end user has to provide the End User RFID Tag for the Embedded Service Middleware Application. Only the information or password of End User RFID Tag is correct and can be used to gain the secured decryption key which recorded in the End User RFID Device, the digital content recorded in the End User RFID Device can be presented.

Considering that the three possible states are based on the RFID induction, the RFID Hardware is divided into two types of equipments: for End User RFID Device and for End User RFID Tag.

According to the three possible ways to protect the digital content, when the protection is based on the combination of Hard/Soft- Encryption/Decryption and Only Hardware-Encryption with Hard/Soft –Decryption, the RFID Hardware for End User RFID Device is needed. Due to that the digital content is protected by the RFID tag embedded in the hardware, the information recorded in the tag has to be inducted before using. For example, if a tag is embedded in the CD-ROM disk, the user should have a CD-ROM driver with the RFID Hardware when reading the disk. In other words, if the protection is based on the hardware belongs to End User RFID Device, the corresponding reader with RFID Hardware is necessary. The RFID Hardware can be embedded in the CD-ROM driver, reader, or other multimedia devices.

In opposition to End User RFID Device, when the decryption is based on the End User RFID Tag key, end user has to own the valid RFID tag for decrypting the digital content. For example, the decryption code is recorded in the RFID tag of End User RFID Device. However, the decryption code is secured by the password which locks the data slot of RFID tag. Without the correct password, end user cannot gain the decryption code that secured in the RFID tag of End User RFID Device. To provide the password, the end users should have the RFID Hardware such as the USB-RFID reader, etc.

To manage the RFID information, Embedded Service Middleware Application is proposed to parse the information from the RFID Hardware. Due to that there are different RFID product, an RFID parser is needed for analyzing and parsing the information from RFID Hardware. After gaining the requirements or response, the Embedded Service Middleware Application searches the corresponding applications and passes the information. Possible ways to retrieve the protected digital data

The whole framework of location-aware RFID application service system

In the location-aware RFID application service system, the RFID antennas and reader are deployed 1) at the specific area or location such as the entrance of the rapid transit system or the information service machine, or 2) within the handheld devices such as PDA or mobile phone. When a user is given a readable RFID tag, the related information or the user's on demand service conditions about the user is given by himself and on demand recorded in the database. When the user requires the local area public or personal services, the user should be at the tiny induction area such as a local area information center or a service station. Then, the RFID system placed in the specific area inducts the RFID tag and gain the information such as UID from the RFID tag. The reader of RFID system then sends the information to the local area server via Internet.

After receiving the information and parsing the message from RFID system, the content of RFID tag can be identified. If end user RFID tag is used, the embedded server service middleware can search and present the local information such as local area shopping information, traffic information, or the customization information, recorded in local database that match the on demand conditions of the RFID tag user. In other words, the RFID user can be directly served with sufficient local area related information. If other further information needed, the embedded server service middleware can send the user's request to the remote main server to obtain the requested service or to the other business applications via Internet for extra service obtaining. At last, the user can gain the location-aware information or services via user interface. In opposition to end user RFID tag, when a user of end user device with RFID System actively scans the RFID tag of the commercial advertisement, the handheld device can send the scanned RFID tag information via wireless network or cellular mobile system to the local area server with embedded server service middleware embedded. Then, as the procedure of end user RFID tag, the embedded server service middleware searches for the requested services and transmits these services to the user's handheld device by wireless network or cellular mobile system.

In addition, the users can use handheld device middleware application to select the tag content recorded in handheld device database if needed. Then, the RFID API controls the RFID system embedded in the handheld device to re-write the content (such as UID) of the tag of the handheld device. At last, the RFID content requirement from other business applications or systems can be provided through the RFID tag of the handheld device.

In addition, the database can record the history of the user's requirements. The statistic user requirements can be used to classify that what kind of the service the user requests most. Next time the system can provide the personal services according to the classified results. In other words, the users can be served with the services they most pay attention to.

Current RFID Technology

This section describes out of which parts RFID tags consist of, how they work in principle, and what types of tags do exist. It focuses on how tags are powered and what frequency ranges are used. The section concludes by covering a few important standards.

RFID transponders (tags) consist in general of:

Micro chip

Antenna

Case

Battery (for active tags only)

The size of the chip depends mostly on the Antenna. Its size and form is dependent on the frequency the tag is using. The size of a tag also depends on its area of use. It can range from less than a millimeter for implants to the size of a book in container logistic. In addition to the micro chip, some tags also have rewritable memory attached where the tag can store updates between reading cycles or new data like serial numbers.

A RFID tag is shown in figure 1. The antenna is clearly visible. As said before the antenna has the largest impact of the size of the tag. The microchip is visible in the center of the tag, and since this is a passive tag it does not have an internal power source.

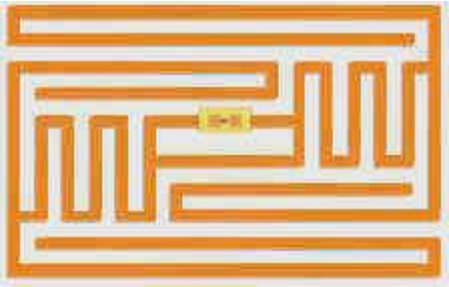

Figure 3: A passive RFID tag

In principle an RFID tag works as follows: the reading unit generates an electro-magnetic field which induces a current into the tag's antenna. The current is used to power the chip. In passive tags the current also charges a condenser which assures uninterrupted power for the chip. In active tags a battery replaces the condenser. The difference between active and passive tags is explained shortly. Once activated the tag receives commands from the reading unit and replies by sending its serial number or the requested information. In general the tag does not have enough energy to create its own electro-magnetic field, instead it uses back scattering to modulate (reflect/absorb) the field sent by the reading unit. Because most fluids absorb electro-magnetic fields and most metal reflect those fields the reading of tags in presence of those materials is complicated.

During a reading cycle, the reader has to continuously power the tag. The created field is called continuous wave, and because the strength of the field decreases with the square of the distance the readers have to use a rather large power. That field overpowers any response a tag could give, so therefore tags reply on side-channels which are located directly below and above the frequency of the continuous wave.

RFID Systems

A RFID reader and a few tags are in general of little use. The retrieval of a serial number does not provide much information to the user nor does it help to keep track of items in a production chain. The real power of RFID comes in combination with a backend that stores additional information such as descriptions for products and where and when a certain tag was scanned. In general a RFID system has a structure as depicted in figure 2. RFID readers scan tags, and then forward the information to the backend. The backend in general consists of a database and a well defined application interface. When the backend receives new information, it adds it to the database and if needed performs some computation on related fields. The application retrieves data from the backend. In many cases, the application is collocated with the reader itself. An example is the checkout point in a supermarket (Note that the given example uses barcodes instead of RFID tags since they are more common; however, the system would behave in exactly the same way if tags were used). When the reader scans the barcode, the application uses the derived identifier to lookup the current price. In addition, the backend also provides discount information for qualifying products. The backend also decreases the number of available products of that kind and notifies the manager if the amount falls below a certain threshold.

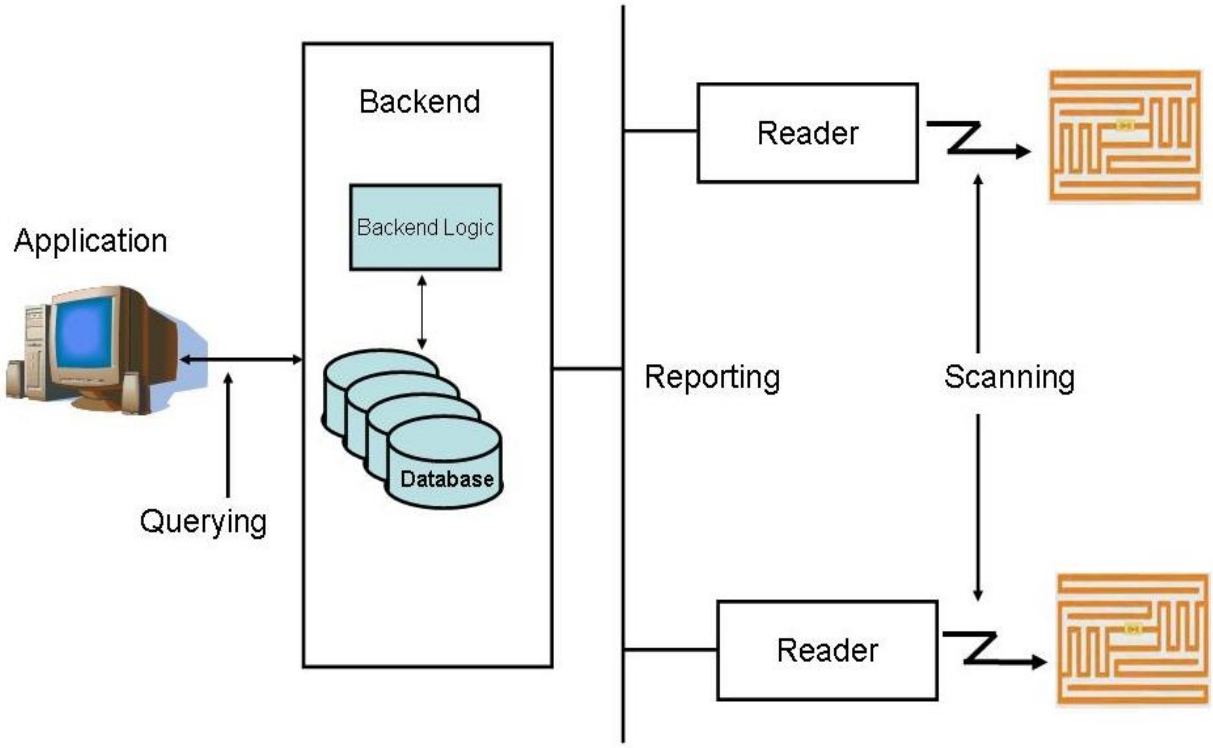

Figure 4: A simplified RFID system

This section describes how RFID tags work in general, what types of tags exist and how they differ. The three frequency ranges that RFID tags typically use are LF, HF, and UHF. Also the difference between passive, semi-passive, and active tags was explained and their advantages and disadvantages were compared.

Conclusion

In this chapter, we show applications and systems based on RFID technology which integrated into the existed service systems. The RFID technology can enhance the automatic management procedure. Identification and tiny information exchanging can be achieved. Individual or personal services can be provided to different consumers. However, to establish the RFID embedded systems and applications, the cost, convenience, feasibility should be considered. To adopt RFID system, some extra costs such as RFID tag and hardware should be overcome by the enhanced performance of management. In other words, to implement the RFID systems for the consumers, to enhance the convenience for consumers will be an important issue than the cost.

References

URLs:

[Baja Beach Club] Uses implanted RFID tags to identify and charge VIP members: http://www.bajabeach.es/
[VeriChip] Company that produces human-implantable RFID chips: http://www.verichipcorp.com
[EZ-Pass] Electronic toll collection for toll roads and bridges: http://www.e-zpassiag.com
[Speed Pass] Paying at Exxon and Mobile gas stations with RFID tags: https://www.speedpass.com/forms/frmHowItWorks.aspx?pPg=howTech.htm&pgHeader=how
[Wiki-RFID] Wikipedia-RFID: http://en.wikipedia.org/wiki/Rfid
[Wizard Wars] The invention of IFF in WWII: http://www.vectorsite.net/ttwiz1.html
[US. Patent 3,713,148] The probably first RFID patent: http://patft.uspto.gov/netacgi/nph-Parser?patentnumber=3,713,148
[US Patent Office] http://www.uspto.gov/
[ICAO] International Civil Aviation Organization: Guidelines for RFID enabled passports: http://www.icao.int
[ColoradoLaw] Colorado State Legislature: Colorado state legislature makes aluminum underwear a misdemeanor, http://www.state.co.us/gov_dir/leg_dir/olls/sl2001/sl.162.htm

[InformationWeek] Article on RFID enhanced golf balls: http://www.informationweek.com/story/showArticle.jhtml?articleID=57703713
[RadarGolf.com] A company producing a "Ball Positioning System": http://www.radargolf.com
[Oren06] Yossi Oren, Adi Shamir, "Power Analysis of RFID Tags", Power analysis reveals kill passwords on RFID tags
[EPC Global Inc.] <="" a="">http://www.epcglobalinc.org/
[Auto ID Center] http://www.autoidcenter.org/

http://www.spychips.com/

http://www.difrwear.com/

http://www.nocards.org/AutoID/overview.shtml

http://www.rfidupdate.com/

http://www.rfidweblog.com/50226711/rfid_guardian_the_antirfid_device_unveiled.php

Books:

[Westhues05] J. Westhues, "Hacking the prox card," in RFID: Applications, Security, and Privacy, S. Garfinkel and B. Rosenberg, Eds. Reading, MA: Addison-Wesley, 2005, pp. 291-300.

Papers:

[Landt01] Jerry Landt, "Shrouds of Time": outlines history and present of RFID: http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf
[Baude03] P. F. Baude, D. A. Ender, T. W. Kelley, M. A. Haase, D. V. Muyres, and S. D. Theiss, "Organic Semiconductor RFID Transponders", Electron Devices Meeting, 2003.
[Inoue03] S. Inoue and H. Yasuura, "RFID privacy using user-controllable uniqueness", in Proc. RFID Privacy Workshop, Nov. 2003. http://www.rfidprivacy.us/2003/papers/sozo_inoue.pdf
[Feldhofer04] M. Feldhofer, S. Dominikus, and J. Wolkerstofer, "Strong Authentication for RFID Using the AES Algorithm", Cryptographic Hardware and Embedded Systems 2004. http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3156&spage=357
[Fishkin04] K. P. Fishkin, S. Roy, and B. Jiang, "Some methods for privacy in RFID communication", in Proc. 1st Eur. Workshop on Security in Ad-Hoc and Sensor Networks, 2004, http://www.intel-research.net/Publications/Seattle/062420041517_243.pdf
[Haehnel04] D. Haehnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, "Mapping and Localization with WID Technology", International Conference on Robotics & Automation, 2004.
[Juels04] A. Juels, "Minimalistic Cryptography for Low-Cost RFID Tags", Security in Communication Networks 2004
[Krumm04] J. Krumm, E. Eckert, W. H. Glauert, A. Ullmann, W. Fix, and W. Clemens, "A Polymer Transistor Circuit Using PDHTT", Electron Device Letters, 2004.
[Bono05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device", in Proc. 14th USENIX Security Symp., 2005, http://rfidanalysis.org/DSTbreak.pdf
[Micheal05] K. Michael, L. McCathie, "The pros and cons of RFID in supply chain management", International Conference on Mobile Business, 2005.
[Philips05] T. Phillips, T. Karygiannis, R. Kuhn, "Security Standards for the RFID Market".
[Rieback05] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian, A battery-powered mobile device for RFID privacy management", in Proc. Australasian Conf. Inf. Security and Privacy, 2005, http://www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf
[Subramanian05] V. Subramanian, P. C. Chang, D. Huang, J. B. Lee, S. E. Molesa, D. R. Redinger, and S. K. Volkman, "Printed organic transistors for ultra-low-cost RFID applications", IEEE Transactions On Components And Packaging Technologies, 2005.
[Jiang06] B. Jiang, K. P. Fishkin, S. Roy, and Matthai Philipose, "Unobtrusive Long-Range Detection of Passive RFID Tag Motion", IEEE Transactions On Instrumentation And Measurement,

2006.
[Juels06] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal On Selected Areas In Communications.
[Rieback06a] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "The Evolution of RFID Security"; Pervasive Computing, IEEE Volume 5, Issue 1, Jan.- Mar. 2006.
[Rieback06b] Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?", http://www.rfidvirus.org/papers/percom.06.pdf
[Subramanian06] V. Subramanian, P. C. Chang, D. Huang, J. B. Lee, S. E. Molesa, D. R. Redinger, and S. K. Volkman, "All-printed RFID Tags: Materials, Devices, and Circuit Implications", VLSI Design, 2006.