Privacy and Security Study of RFID

Submitted by

Anagha Gala
anaghagala@yahoo.com
Dilip Kamath
dilip_kamath@yahoo.com
Vijay Arora
Vijay.arora@mail.com

Abstract: The objective of this paper is to analyze the security and privacy aspects of RFID. It presents a perspective about useful RFID applications and potential privacy invasions. The paper outlines the lab experiment conducted by the project team to secure the RFID data using AES encryption. Possible solutions where this approach can be used and its limitations are noted.

Privacy and Security study of RFID technology

Introduction

Radio frequency identification (RFID) technology has been around since the 1940s. It is a technology that pinpoints the physical location of the item/person containing the tags. While this is a convenient way to track items, it is also a convenient way to track people and their activities through their belongings. The military has been using this technology for several years to track its combat supplies. Wal-Mart compliance requirement of 2005 has given RFID technology the world stage for investigation, education, adoption and criticism.

RFID is used for hundreds, if not thousands, of applications such as preventing theft of automobiles, collecting tolls without stopping, gaining entrance to buildings, automating parking, corporate campuses and airports, dispensing goods, tracking library books, buying hamburgers, and the growing opportunity to track a wealth of assets in supply chain management.

Following table gives a brief history of RFID.

Decade	Event
1940 - 1950	During world war II RADAR system used RFID. Major World War II development effort. RFID explored by Harry Stockman in 1948.
1950 - 1960	Early explorations of RFID technology, laboratory experiments.
1960 - 1970	Development of the theory of RFID. Start of applications field trials.
1970 - 1980	Explosion of RFID development. Tests of RFID accelerate. Very early adopter implementations of RFID.
1980 - 1990	Commercial applications of RFID enter mainstream.
1990 - 2000	Emergence of standards. RFID widely deployed. RFID becomes a part of everyday life.

Landscape of RFID systems

RFID enabled systems have a wide spectrum of adopters - from baggage handling systems to Libraries to targeted improvements in logistics to theft reduction schemes in stores. RFID based systems have been deployed for vehicle tracking, EZ-pass toll payment, Employee ID badges and access control. RFID has been used by military to track shipments and vehicles at war sites. Libraries have been using RFID tags to streamline the check-out process. Several organizations have realized the benefits of an RFID tag. It has been touted by proponents of the technology as a missing link between material flow and information flow.

Still in the nascent stage of the "hype-cycle" (term coined by Gartner group) the desire to jump on this "new" technology bandwagon has been interesting. With organizations in the post "dot-com" economy to do more with less, the technology has been seen has a panacea to improve internal processes and make efficiency inroads into product tracking and tracing. The major driving force behind commercial deployment of RFID technology is presently logistics and supply chain applications. RFID promises more accurate product sell forecasts, inventory control, theft control and cost reduction through better production and sales management.

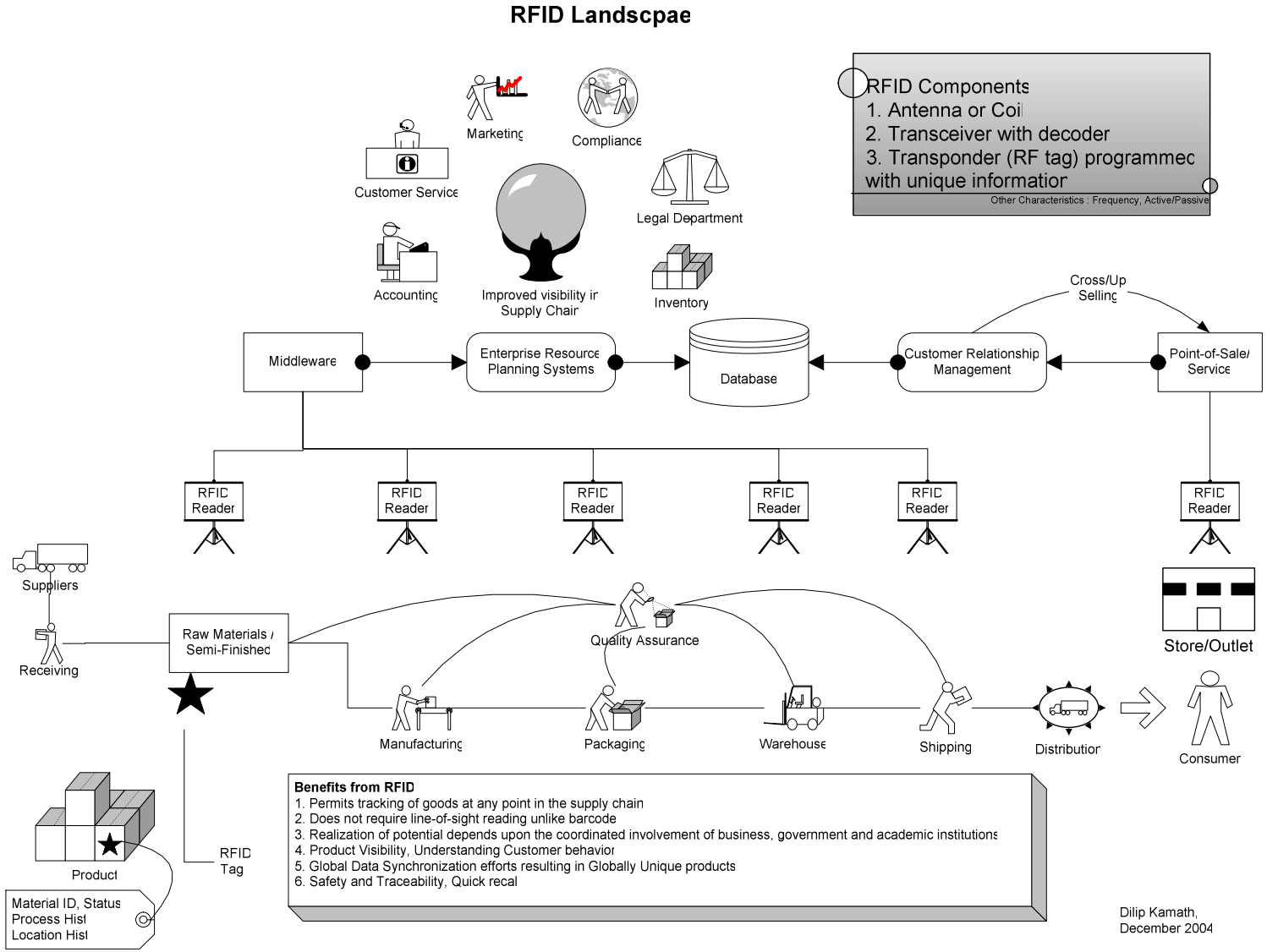
A generic architecture model of RFID implementation can be thought of containing four components:

a. RFID tags and a reader to read the contents of the tag
b. A repository that contains the Item ID that gives the metadata of the tag
c. A manufacturer's repository containing history of events that has occurred on the product carrying the tag
d. A consumer's repository that details the usage/consumption of the tag

Finally, this model will contain a "glue" that is in the form of middleware that will define a temporary or permanent link between two or many components. The nascent nature of the technology and the evolving standards has led to several blueprints of adopted architectures by both consumers and vendors of the technology.

Details of these blueprints are outside the scope of this report, but can be found on several vendor and Auto-Id consortium websites listed in the References section of this report.

An example of such an overall implementation is depicted in the schematic below:


RFID Landscpae
RFID Components
1. Antenna or Coi
2. Transceiver with decoder
3. Transponder (RF tag) programmec with unique informatior
Other Characteristics : Frequency, Active/Passive
Marketing
Compliance
Customer Service
Legal Department
Accounting
Improved visibility ir Supply Chair
Inventory
Cross/Up Selling
Middleware
Enterprise Resource Planning Systems
Database
Customer Relationship Management
Point-of-Sale/ Service
RFID Reader
RFID Reader
RFID Reader
RFID Reader
RFID Reader
RFID Reader
Suppliers
Receiving
Raw Materials / Semi-Finishec
Quality Assurance
Store/Outlet
Manufacturing
Packaging
Warehouse
Shipping
Distributior
Consumer
Product
RFID Tag
Material ID, Status
Process Hist
Location Hist
Benefits from RFID
1. Permits tracking of goods at any point in the supply chain
2. Does not require line-of-sight reading unlike barcode
3. Realization of potential depends upon the coordinated involvement of business, government and academic institutions
4. Product Visibility, Understanding Customer behavior
5. Global Data Synchronization efforts resulting in Globally Unique products
6. Safety and Traceability, Quick recal
Dilip Kamath, December 2004

Security and Privacy Invasion

Hello, I have your privacy tone

Whenever we pick up the phone, we expect to hear the familiar dial tone that tells us that the phone is "on" and you can easily access (call) other person(s). Can you imagine a situation when your phone sends this "familiar" tone to your neighbors along with some personal information about you? RFID tags have this ability to emit a "privacy" tone about its existence and its contents to anyone who is interested in knowing about it. Interestingly the current technology infrastructure makes this information travel on the same frequency as a cordless phone. So the next time you lift your handset to receive a dial tone, you may receive a privacy tone with information about the new cologne your neighbor purchased last week at the Sam's Club.

RFID technology has caused a stir in the private and public domain due to possibility of its potential abuse. RFID technology is a fundamental change in the way information technology captures and handles data. As noted above, a RFID tag can be used at an item level, providing a unique identification number. Due to interoperability between readers, all readers will be able to read the tags and understand the product. This has far reaching privacy implication, since surveillance is possible without a person's knowledge. RFID tags can enable day-to-day movement tracking of people, compromising their anonymity. The tag and the reading process can be silent and invisible, so a person may not really know that his/her privacy is being compromised.

Why the uproar?

For a successful technology, reality must take precedence over public relations, for nature cannot be fooled."

- Richard Feynman

A RFID that is used inside the warehouse and stores has a useful purpose of tracking the items so as to aid inventory management. Similarly RFID deployed for specific usage like criminal identification or pet tracking is definitely useful. The problem in privacy invasion starts when consumers buy products and take them out of the store, with the tags being active. The consumer may or may not know whenever a tag is being read or the information previously collected is being used. The RFID chips of sizes in microns have been developed, making it virtually impossible to find out if an unlabelled product contains RFID.

Usage of RFID in consumer products will enable companies to identify and profile individuals based on the products they purchased or they are carrying. Looking at the advances in the reader technology, it will soon become possible to link related information regarding individual and perform many customized services. The consumer will be targeted more and more specifically and a life-long trail of data can be connected to him/her just like today's credit reports.

Can anyone really track me from my toothpaste?

RFID technology in consumer products and services can create explosion of consumer generated data. This will of course need a network of RFID readers and massive

changes in the data infrastructure of the corporations. Many of the corporations today do not plan to implement item level tagging or track the RFID tag after the sale has been completed. This is partly because of privacy issues and partly because of technical difficulties.
The reading of a tag in a public, uncontrolled environment is subject to many problems like reader range, presence of metals or liquids, presence of obstructions etc. Item-level RFID tagging is often considered to be 5 or more years in the future for retail RFID applications, due to the cost of tags, reader infrastructure and uncertainty about near term applications. Even if highly reliable tags and readers are made available in future, the networks to collect and process this data are a huge cost to companies, providing not so substantial returns. Even though the costs of producing and applying RFID tags reduce to less than 5c, it is not a motivation enough to put them on products below certain price point.
Thus we will see usage of such applications for high-end consumer items. So hopefully you can safely buy toothpaste for next 10 years without worrying!

Big brother in small chip

Virginia might put them in drivers' licenses, and Japan is putting them in students' backpacks. – **National Public Radio**

Many of the inhibitions and panic regarding the RFID is generated by perception rather than reality. People are fearful of not knowing who is watching them. They want to know who is interested in the goods they are buying and using. It boils down to who's checking you out when you go past the checkout lane in the market.
Looking at it in a more pragmatic way, today's credit cards, frequent shopper cards, employee cards, e-commerce websites provide a variety of information and people can be profiled for the activities they do. The basic difference is since the data is distributed, there is no centralized way to link all transactions and get a complete picture about an individual. Analysts envision a time when systems will be used to identify and track every item produced on the planet. RFID technology and the proposed Object Naming Service can potentially make it much easier to achieve this. The unification of the technology will result in surveillance to highest degree and privacy may not exist even in people's own home. This is a scary scenario, taking the "Big brother is watching you" phrase to a new meaning.

Myth vs. Reality

"Travel bags enabled with RFID tags offer more than tracking of the baggage. They can be used to link a traveler and their contents of the bag". This is the claim made by several transportation authorities. But in reality, you really do not need RFID at all. No traveler's bags go beyond the check-in gates without the boarding pass. A boarding pass can help trace all checked-in baggage to the owner.
"Once RFID technology is used by stores, all information about a consumer can be tracked." This is misleading. Reality is that stores already have mature systems in place to track a consumer even now. Current traceability mechanisms include credit card transactions, Store Cards/Frequent shopper cards, manufacturer warranty paperwork, maintenance agreements (3-5 year warranty papers for replacement/repair of expensive products) etc.

Euphoria around RFID adoption is caused by several reasons like Wal-Mart compliance and Hype cycles created by vendors and analysts.

Analysts envision a time when the system will be used to identify and track every item produced on the planet
Source: RFID: Tracking everything, everywhere CASPIAN article

Though the above statement brings out the concern about privacy issues, some of the material on CASPIAN website goes to the extreme with panic laden statements. Also, this appears as one of the comments from "hype cycle". Even if this prediction becomes true, the time frame for this could be decades and society, human behavior and the definition of privacy as we see it now would have metamorphosed differently. Alternately, supply chains may find alternate ways to improve efficiencies or cost prohibitive nature of RFID tags would make the adoption and therefore the ubiquitous usage prediction a moot point.

Increasing need of Encryption and standards

RFID readers in public places can read the RFID data and connect to networks providing real time data about the owners and thus infringe on privacy. Encryption of data will help to solve this problem to certain extent. Encryption of the RFID tag contents will ensure that unauthorized readers are not able to access the data or even of they can get the encrypted content, they do not have the access to encryption key.

In the retail supply chain, encryption will be important for retailers from potential surveillance by their rivals. Encryption could also be suitable for high-privacy applications e.g. medical or criminal related applications, where tags are written to just once and then read many times. One example is using tags to identify blood and other medical samples while ensuring that any patient data stored on the tag is kept confidential. There are many encryption algorithms available which can be suitably used to encrypt the data on RFID.

EPCGlobal has recently ratified its Gen2 global standard that uses frequency and power in a way that complies with the major regional regulatory environments. In addition to improvements in security of the data on the tag, the standard includes the ability to lock the identification fields in the tag, so that they can't be spoofed or changed without a password. It also includes a strong kill mechanism, so retailers and others have the option of automatically erasing all data from the tag as it passes through a reader.

However the standard does not allow for encryption, because one of the user requirements for the standard was that the tags be inexpensive. But security issues will continue to be addressed in the hardware and policy working groups.

Disabling tags

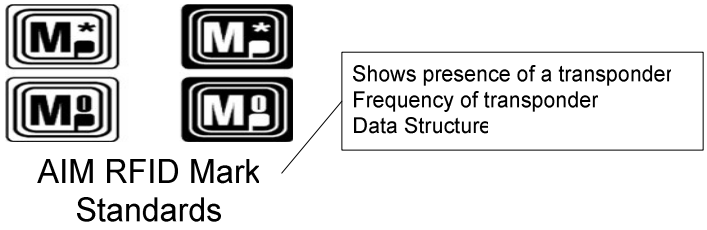
Once merchandise is sold at a retail outlet or an item leaves a final manufacturing work center, the RFID tag may not be used by the owner system. At this stage of its lifecycle, the tag needs to be shut-down so that it becomes unusable. This process is known as "tag killing" and is used by consumers either to disable the tags or to remove it from the

merchandise. Currently there is no standard for tag killing in the industry. This opens up privacy concerns as to what is being tracked and who is tracking them and how the tracked information is going to be used. There are multiple ways of invalidating a tag – physical removal of tag, sending a "kill" command and removing the contents of the tag or to use a blocker tag. As in the case of encryption, there are no standards across the industry on the disabling tags.

Standards

RFID technology is being used globally. Many entities are participating in the standards process. EPCGlobal and ISO are the popular standards on the market. Other initiatives in defining standards in this area include, but are not limited by:

- EPCGlobal's RFID specifications – Generation 1 and Generation 2 standard has been released.
- ISO 18000 – Passive UHF-frequency radio-frequency identification standards
- Project JumpStart – Pharmaceutical industry initiative involving Abbott Laboratories, Johnson & Johnson, Pfizer, Proctor & Gamble, McKesson Corp, CVS and Rite-Aid with involvement from FDA
- AIM North America Standards Action Group (NASG) – AIM RFID Mark standards to separate license tag from a data-rich tag and help improve reading efficiencies



- U.S. Government's Government Smart Card interoperability specification (GSC-IS). Customs-Trade partnership against Terrorism (C-TPAT) etc.

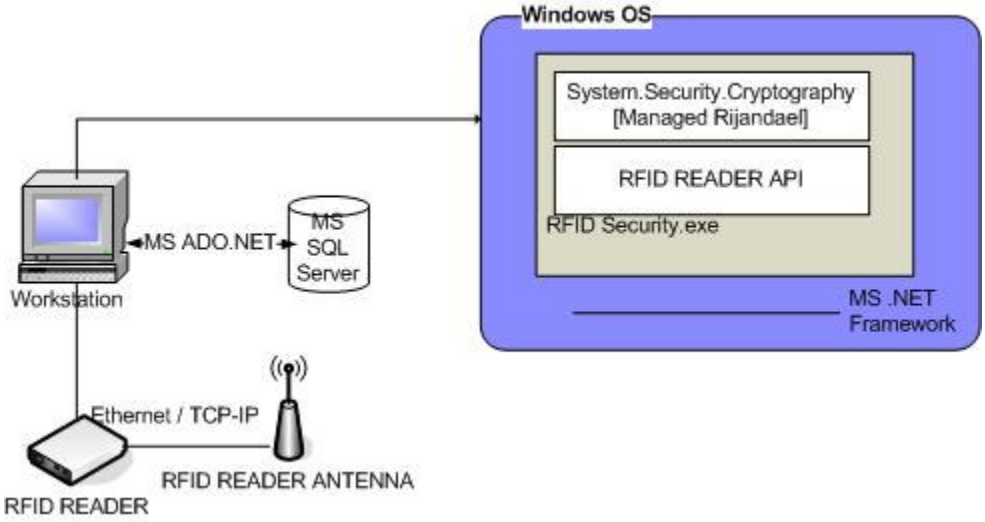
RFID Data Encryption Experiment

To demonstrate securing the information on the RFID tag, we developed a small application using passive RFID tags and AES encryption algorithm. This experiment was conducted as a proof of concept of the encrypted RFID usage.

The schematic below describes our lab setup. The setup consists of following –

- RFID reader
- RFID tags
- Workstation controlling the reader

RFID Reader is connected to the computer via a serial port connection. It can also be connected using a TCPIP connection. Most readers allow assigning them a static IP address, which enables communication to it using TCP/IP. Most RFID readers comply with standards from either ISO or EPC. The reader manufacturers provide with APIs which are called to communicate with the readers.



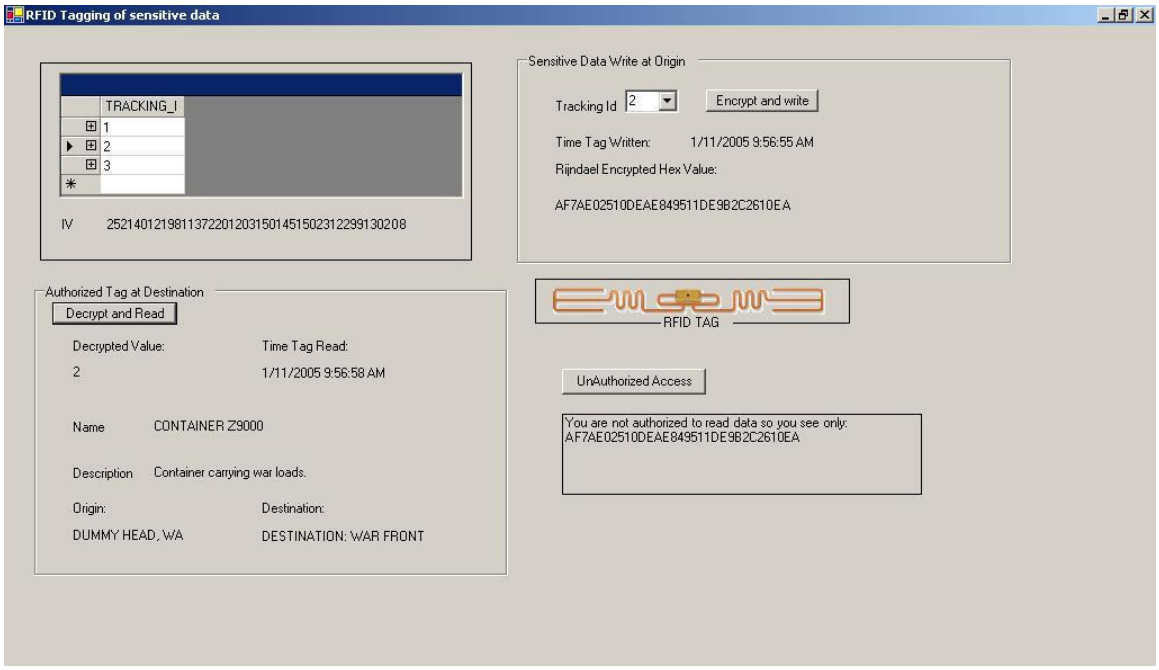
We used ALR9780 RFID reader manufactured by Alien Technologies. This reader can connect up to four antennae. The reader has following specifications –
Model: ALR-9780
Frequency: 902-928 MHz ISM band
Specification: EPC Class 1
Antennas: 4-ports, 50 Ohm, reverse TNC connector
We used passive RFID tags that were printed using RFID printer.

How did we secure the tag?

The above proposed architecture secures the data on the RFID tag after encrypting with Rijndael Encryption. The user logged in at the workstation encrypts the data using a user interface designed for the specific purpose. There are 2 elements in the encryption – the actual number and an IV number which is a “secret” identifier. The data is transmitted to the tag using the RFID reader, which can also function as a writer for tags.

At the time of reading, the user has to specify the IV number to authenticate the reader to the tag. The content read from the tag is decrypted using the IV and the Rijndael algorithm. The 128 bit number produced by encryption is written to the tag. The person not in possession of IV number can see only the encrypted data and hence can not decrypt the data from tag.
The tag reader is connected to computer that displays the correct product information once the tag is successfully decrypted and read.

The following snapshot is of a demo user interface, which has the reading and writing application combined in one screen.



Advantages:

- The concept of the application allows a simple and usable interface.
- It is possible to use multiple IVs to encrypt the data, creating an additional layer of security.
- The IV data can be transmitted using a secure media to the authorized person.

Disadvantages:

- Reading time of the RFID increases due to decryption of data. Though it is negligible in case of lab environment, under heavy volumes, this may become an limitation.
- Physical security of the tag and the IV data needs to be maintained.

Applicability:
This type of applications will find consumers in various industry sectors where sensitive data is being stored on RFID tags and where there is a strong need for only authorized personnel/consumers to read the data from the tags. This concept is being used for military purposes where the IV data is transferred using the smart card technology. One more possibility is to use the public key of the person or company who is supposed to

use the data, so that they can decrypt the data. Various options can be available for the IV data to be used depending on the implementation, e.g. it can be md5 hash number of a particular name, a public key or a simple credit card number.
The encryption application is more suitable for small / medium volume and high confidentially application areas. It will not be suitable for a large scale deployment.
The reading rate of the tags

Observation and Suggestions

We are seeing transformation in the ways companies track inventories, art works and even financial instruments using RFID. RFID is increasingly becoming ubiquitous in commercial as well as non-commercial applications. Some fear this tracking may trigger "Orwellian" pursuits.

It is possible to strike a technical and social balance between privacy and convenience. The information practices of the RFID will ensure that the consumers are educated enough about RFID and their implications. Proper implementation of RFID systems will ensure that the privacy of customers is not compromised.

Widespread adoption of these devices will be only after an acceptable level of security is achieved.

Source: Gartner Group

Some of the suggestions, we think can alleviate concerns and possibly promote the adoption of RFID technology is:

- Creation of a Universal Reader – Easy to use, competitively priced equipment that not only informs you of a live tag but also disables it at the press of a button. It can be offered free at locations for check. It will be available in common electronic shops like RadioShack.
- Option at the checkout lane to "Yes" or "No" to share personal information and print it out on the receipt. – Though data re-identification strategies currently employed by department stores could challenge this
- Reverse revelation
  - If you illegally scan and find about Mr.Smith, the technology within the reader emails the person whom you tracked with your information (Name, Phone, Address and organization worked for and objective of the scan and whom you sold the information to) – The hunter now feels like the hunted and possibly understands the privacy measure
- Consumer groups pressure against RFID systems that track people. Toll-free number can be provided for class action lawsuit against a merchant whose RFID tags were used to track people. This would put the merchants and companies under pressure to not collect identifiable data and value privacy.
- Security concerns are two fold, one legitimate and the other illegitimate. Allay common consumers fear through education particularly to address involuntary sharing of information and unknowingly sharing of information

Challenges

Challenges to adopting RFID and its usage include integration into existing system and business processes, storage requirements resulting in widespread use of the technology and the data payload that will travel along with each work center and most importantly making a business case to win executive support.

Katherine Albrecht, director of Caspian and a doctoral researcher at Harvard University, has fiercely rebutted the suggestion that her group don't represent widely-held views. She points out that research has found that around 70 per cent of the public are concerned about the implications of RFID.

Wal-Mart, on its website, states clearly its RFID tags will not contain nor collect any consumer information. However, the choice of keeping the tag or throwing it away is left to the consumer. Wal-Mart mentions that it uses only passive tags in retail. Wal-Mart and other retail organizations suggest that once the merchandise is sold and leaves its premises, there will be no tracking as the Customer has the choice to throw the tag away.

EPIC has published a set of guidelines for the usage of RFID tags

- Clear labeling should be provided so that consumers are aware that they are buying RFID enabled product
- The RFID tag should be removable so that the consumer has the option to take it out.

Legislation efforts underway

The current state of RFID application is unregulated and although the technology is very old, successfully implemented public domain applications are few. Example: *EzPass*. This creates a urgent call to apply the basic information privacy principles to the use of personal information collected through RFID technology. There is currently no federal law applicable to the collection and further processing of personally identifiable data gathered through RFID technology. European countries have an existing framework for handling privacy related issues and the RFID systems fall under their purview. Other countries have or have begun to create regulations or guidelines that can help protect consumers against major privacy risks raised by RFID technology.

RFID technology and its implementation must be guided by strong principles of fair information practices (FIPs). The eight-part Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD) provides a useful model (www.oecd.org). We agree that the following minimum guidelines, based in part on these principles, must be adhered to while the larger assessment of RFID's societal implications takes place.

Fair Information Practices provide an excellent model for approaching RFID regulation. In USA, it is being used as the basis for legislations. RFID bill of rights is based on these principles.

We propose an "RFID Bill of Rights" which brings Fair Information Practices to deployment of RFID systems. The Bill of Rights consists of five guiding principles for the creation and deployment of RFID systems:

Users of RFID systems and purchasers of products containing RFID tags have:

1. The right to know if a product contains an RFID tag.

2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.

3. The right to first class RFID alternatives: consumes should not lose other rights (e.g. The right to return a product or to travel on a particular road) if they decide to opt-out of RIFD or exercise an RFID tag's "kill" feature.

4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.

5. The right to know when, where and why an RFID tag is being read.

Source : Simson Garfinkel RFID Bill of Rights

EPIC – Electronic Privacy Information Center is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has been advocating for the Right to Know Act to protect consumer privacy from RFID application. There is currently no federal law applicable to the collection and further processing of personally identifiable data gathered through RFID technology. Legislative developments in various States indicate that state legislatures are aware of their constituents' concerns for the privacy risks that RFID technology raises. The Federal legislation underway is Right to know act being put by CASPIAN - www.spychips.com

At the state level, California, Massachusetts, Utah states have been trying to put legislations for preventing possible privacy invasions. They are mainly around the thinking that customers should know that a RFID tag is present in the product.
California legislation has been defeated. The others are still in process. As consumer awareness is increasing, the pressure for legislation will get more momentum.

Conclusion

RFID technology is here to stay and grow in many areas affecting our lives. The potential benefits that can be gained from this technology are numerous like better tracking and control, reduced costs, easier technical solutions and miniature equipments capable of providing co-ordination in geographically vast areas. The privacy implications of RFID are based on the possible scenarios which can come up in future. In today's scenario, it is still early to call the technology a devil in itself. Comprehensive laws, Education of consumers and privacy oriented system design can outweigh privacy concerns. Encryption is one such design consideration which we explored as part of this paper. Encryption will be a relevant technology in case of small or medium volume and high confidentiality applications.

References

1. EPIC comments to FTC on workshop: "RFID applications and implications for consumers" - July, 2004.
2. Auto-ID Center white paper on Active and Passive RFID tags (2002)
3. http://www.epcglobalinc.org/consumer
4. http://www.rfidjournal.com
5. CASPIAN – Consumers Against Supermarket Privacy Invasion and Numbering
6. http://www.oecd.org - Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD)
7. Wikipedia – Definition of RFID
8. Stop RFID – http://www.spychips.com
9. http://www.epcglobalinc.com
10. Association for Automatic Identification and Data Capture Technologies – http://www.aimglobal.org/technologies/rfid/
11. Additional data on the reader used in the experiment can be found at http://www.alientechnology.com/products/rfid-readers/alr9780.php
12. Association of Automatic identification and mobility – http://www.aimglobal.org
13. Garfinkel, S. "Adopting Fair Information Practices to Low Cost RFID Systems", paper presented at Privacy in Ubicomp'2002 workshop,