RFID Introduction, Present and Future applications and Security Implications

Nandita Srivastava
MSEE Student George Mason University
Advisor:Dr Jens-Peter Kaps

Abstract*—RFID technology has been available for more than fifty years. However It has only been recently that the prices of RFID devices have fallen to the point where these devices can be used as a "throwaway" inventory. This presents numerous opportunities along with innumerable risks. A lot of research is being done to suggest methods which will ensure secure communications in RFID systems. The objective of this paper is to present an introduction to RFID technology, its current and future applications, study various potential threats to security and privacy, and give an introduction to some suggested protocols for efficient security mechanisms.

Index terms---RFID, Security

Manuscript received December 19, 2006. This work was supported in part by the ECE Department of Goerge Mason University.

Nandita Srivastava is with the Electrical Engineering Department, George Mason University, 4400 University Drive, Fairfax, Virginia 22030.

I. INTRODUCTION:

OVERVIEW

THE "Radio Frequency Identification (**RFID**) is an automatic identification system. RFID uses RF to identify "tagged" items .This data is then collected and transmitted to a host system using an RF Reader. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc."

1. Automatic Identification

Object identification is an important part of trade. It's most important use is supply chain management. Due to the volume and variety of traded goods, logistics and inventory costs are extremely high. This problem first exploded in middle of 20th century. Food chains and supermarkets were heavily affected by these costs.
In 1948, Bernard Silver and Norman Joseph Woodland, graduate students at Drexel Institute of Technology in Philadelphia, were the first ones to work on this problem. Their research was initiated by an inquiry of a local food chain store owner about research into a method of automatically reading product information during checkout.

On October 20, 1949, Woodland and Silver filed their patent application for the "Classifying Apparatus and Method", describing their invention as "article classification ... through the medium of identifying patterns".

The Woodland and Silver bar code can be described as a "bull's eye" symbol, made up of a series of concentric circles.

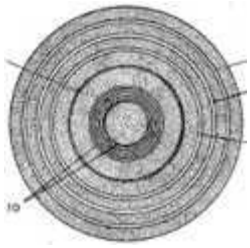

Fig 1.1 The Woodland and Silver bar code [1]

Automatic identification was first used commercially in 1966, but it was soon realized that there would have to be a common standard. By 1970, the Universal Grocery Products Identification Code (UGPIC) was written by a company called Logicon Inc. The standard was further improved and led to the Universal Product Code (UPC) symbol set. To this very day, this standard is used in the United States and Canada. In June of 1974, the first UPC scanner was installed at a Marsh's supermarket in Troy, Ohio, and the first product to have a bar code was Wrigley's Gum.

Fig 1.2 A UPC Bar code

(A) Type of code: (B) Manufacturer: (C) Individual product: (D) Checksum

A bar code works like a light when turned on in a dark room. We can see the walls and furniture in the room by the reflected

light from these items. The scanner device directs a light beam at the bar code. The device contains a small sensory reading element. This sensor detects the light being reflected back from the bar code, and converts light energy into electrical energy. The result is an electrical signal that can be converted into data.

Optical barcodes are ubiquitous and appear almost on every commercial item. There are one dimensional and Two-dimensional barcodes. In two dimensional barcodes more data can be contained in a small surface area. These are used by shipping and transposrt companies, such as UPS, Federal Express and the United States Postal service .

One of the important limitations of barcodes is line of sight requirement with the scanner. The barcode may become dim or indistinct, for example by shrink wrap, decreasing efficiency. Many a times we can see the store clerks struggling to scan the barcodes.

II. RADIO FREQUENCY IDENTIFICATION:

The roots of radio frequency identification technology can be traced back to World War II. The Germans, Japanese, Americans and British were all using radar to warn of approaching planes while they were still miles away. The problem was in differentiating between an enemy plane and a country's own. The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back. This crude method alerted the radar crew on the ground that these were German planes and not Allied aircraft (this was, essentially, the first passive RFID system). Under Watson-Watt, who headed a secret project, the British developed the first active identify friend or foe (IFF) system. They put a transmitter on each British plane. When it received signals from radar stations on the ground, it began broadcasting a signal back that identified the aircraft as friendly. [2].

2.1 RFID System Components

Modern RFID system has three major components.

- Tag –Transponder
- Reader –Transceiver
- Backend Database

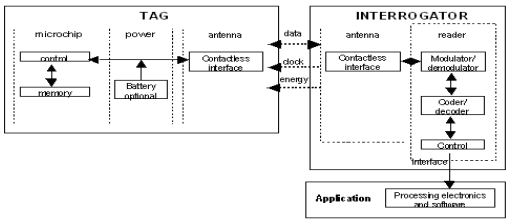

Fig 21. RFID System components

2.1.1 Tags

Tags are typically composed of a microchip for storage and computation, and a coupling element, such as an antenna coil for communication. Tags may also contain a contact pad. Tag memory may be read-only, write-once read-many or fully rewritable.

Broadly the tags have been classified in three categories.

- **Active Tag:** An active RFID tag is equipped with a power source for the tag's circuitry and antenna. The advantages of an active RFID tag includes readability from a distances of one hundred feet or more as well as capability to have other sensors that can use electricity for power. The major disadvantages of an active RFID tag are the limitations on the lifetime of the tag (5 years). They are more expensive and physically larger and they add to the maintenance cost if the batteries are replaced. Battery outages in an active tag can result in expensive misreads.
- **Passive Tag:** Passive RFID tag does not contain a power source; the power is supplied by the reader. The tag draws power from the inductive coupling with reader antenna.The major disadvantages of a passive tag are that the tag can be read only at very short distances, typically a few feet at most. However there are many advantages .The tag functions without a battery which increases the life time to more then 20 years. The tags are less expensive (10¢) and much smaller . These tags have almost unlimited applications in consumer goods and other areas.
- **Semi-Passive Tag:** Like passive tags, semi-passive tags reflect (rather than transmit) RF energy back to the tag reader to send identification information. However, these tags also contain a battery that powers their ICs. This allows for some interesting applications, such as when a sensor is included in the tag so it can transmit real-time attributes, such as temperature, humidity, and timestamp. By using the battery only to power a simple IC and sensor—and not including a transmitter—the semi-passive tags achieves a compromise between cost, size, and range.

	Passive	Semi Passive	Active
Power Source	None	Battery	Battery
Transmitter	Passive	Passive	Active
Max range	10M	100M	1000M

Table 2.1: Active, Semi-Passive and Passive Tags [4]

2.1.2 Readers

An **RFID reader** is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. A number of factors can affect the distance at which a tag can be read (the read range). The frequency used for identification, the antenna gain, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the

object to be identified will all have an impact on the RFID system's read range. The RFID reader provides the connectivity between individual tags and the tracking/management system. Depending on the application and operating conditions, there may be a multiplicity of readers to fully service a specific area.

Overall, the reader provides three main functions

- Bidirectional communication with the tags.
- Initial processing of received information.
- Connection to the server that links the information into the enterprise.

2.1.3 Backend Database

Often, the RFID reader contains a networking element such as wired Ethernet or wireless Ethernet that connects a single RFID-read event to a central server. The central server runs a database application, with functions that include matching, tracking, and storage. In many applications, an "alert" function is also present (for example the re-order trigger, for supply chain and inventory management systems, or an alert to a guard, for security applications).

2.2 Tag Reader Air Interface

Passive tags typically receive power through inductive coupling or through far-field energy harvesting. Several challenging issues arise from both powering and communicating over the same signal. For example any modulation of the signal reduces the power to the tag. The vast difference in power between tags and readers creates a unique problem for RFID systems. In some cases, the return signal to the reader may be overwhelmed by the outgoing signal, rendering tag responses impossible to detect. To prevent this from occurring, the return signal is sometimes modulated onto a different frequency, or sub carrier. For example, in the ISO 15693 standard for 13.56 MHz RFID, a sub-carrier of 13.56 MHz/32 (= 423.75 KHz) is used [4].

2.3 Frequencies Regulations for RFID

Most RFID systems operate in the Industrial-Scientific-Medical (ISM) bands, which are freely available to low-power, short-range systems. These bands are defined by the International Telecommunications Union (ITU). In US these are defined by Federal Communications Commission (FCC)

- Low Frequency (LF) 125-135 KHz
- High Frequency (HF) 13.56 MHz
- Ultra High Frequency (UHF) 868-930 MHz
- Microwave 2.45 GHz
- Microwave 5.8 GHz

Devices operating in each band are subject to different power and bandwidth regulations.
For example, systems operating in the 13.56 MHz band are limited to a bandwidth of 14 kHz in the forward channel. The backward channel may use a greater bandwidth, since it has much lower power. In contrast, the 915 MHz ISM band is less restricted and several options are available for reader-to-tag communications. The option that provides the longest read range requires the reader to "hop" among 50 channels every 0.4 seconds, each with up to 250 kHz of bandwidth. This is a trade-off, since tags cannot be guaranteed continuous communication across a frequency hop. As a result, reader/tag communications must be limited to 0.4 seconds. Transactions must be completed within this period, otherwise they will be interrupted by a frequency hop.
Following table tries to summarize the advantages and disadvantages.

Frequency	Range	Advantage	Disadvantage
125-135 KHz	<1m	No radiation/reflection problems	Slow data transfer Bulky
13.56 MHz	1m	Tolerant of fluids and metals	
UHF	Upto 30m	High rate data transfer /Smallest cheapest tags	Easily absorbed /Reflected
GHz	Higher range		

Table 2.2

2.4 RFID Standards

There are many organizations contributing to the development of RFID standards.

2.4.1 EPCglobal™

(EPCG) is contributing to the RFID-network standards with its EPC (Electronic Product Code) Network. The not-for-profit EPCG is a joint venture between EAN International and the Uniform Code Council (UCC), the group that oversee the international standards for UPCs (universal product codes), or bar codes.

The EPC system defines several classes of products:

EPC Class	Definition	Programming
Class 0	"Read Only" passive tags	Programmed as part of the semiconductor manufacturing process
Class 1	"Write-Once, Read-Many" passive tags	Programmed once by the customer then locked
Class 2	Rewritable passive tags	Can be reprogrammed many times
Class 3	Semi-passive tags	
Class 4	Active tags	
Class 5	Readers	N/A

Table 2.3 EPCglobal, Classes of Tags

Specifications
Generation 2, sometimes called "Gen 2", is the newest and most advanced of EPCglobal's RFID specifications in the UHF (ultrahigh frequency) band (centered around 900 MHz).

	Generation 1	Generation 2
Frequency	860MHz – 930MHz	860 – 960MHz
Memory capacity	64 or 96 bits	96 to 256 bits
Commercial products available as of 9/1/04[8]	Yes	No
Field-programmable	Yes	Yes
Re-programmable (read/write) *(Per EPCglobal specifications—see text for current Class 0, 1 product configurations)*	Class 0 – Specified as read only Class 1 – Specified as Write once/Read many	Yes
Field-killable	Yes	Yes

Fig 2.2 Gen 1 and Gen2 EPCglobal specifications

The table above describes some differences between Gen1 and Gen2 specifications from EPCglobal.

2.4.2 International Organization for Standardization (ISO)

ISO currently defines various standards for RFID for example The Gen 2 protocol is currently being reviewed at ISO as standard 18000-6C. Some of the other standards are

- ISO TC 23: Animal Identification
- ISO TC 104: Freight Containers
- ISO TC 204: Road Telematics
- ISO TC 122: Packaging
- JTC 1/SC 17: Integrated Circuit Cards (ie: credit cards with embedded tags)
- JTC 1/SC 31: Automatic Identification and Data Collection Techniques ("Where's the lost child at the amusement park?") [6]

3. Security Issues

There are many Security issues related to RFID .They can be broadly divided into following categories.

- Tag Access
- Tag Collision

3.1. Tag Access

An RFID system is susceptible to various kinds of attacks. These attacks can be categorized as follows. [4]

- **Physical Access**
  This is possible when the attacker has physical access to the RFID tags. These attacks may include material removal or water etching, energy attacks, radiation imprinting, circuit disruption or clock glitching.These attacks can not happen at a widespread level.
- **Counterfeiting**
  In this kind of attack an attacker may be able to produce its own tags and can initiate queries to the tags.
- **Eaves dropping**
  In this kind of attack the attacker can not initiate the query but may only be able to **listen** to "logical" messages transmitted in protocols, as opposed to the electromagnetic emissions monitored by physical access.
- **Traffic analysis**
  In this kind of attack attacker can not listen to the logical message but still be able to find the number of queries generated thereby by being able to do traffic analysis.
- **Denial of service attacks**
  This kind of attack is limited to disrupting broadcasts, blocking messages or any other denial of service attacks. As RFID becomes widely used this kind of attack could be very crucial.

3.2 Tag Collision

Readers may attempt to read a single tag from among a population of many. When multiple
tags respond simultaneously to a reader query, conflicting communication signals may
cause interference. This interference is called a *collision* and may result in a failed transmission.
Readers and tags must employ a method to avoid collisions, referred to as an anti-collision algorithm. Binary tree walking is one such algorithm

3.2.1 Binary tree-walking scheme

In this scheme, a reader will query all tags in the vicinity for the next bit of their ID. If two different bit values are transmitted from among the population of tags, the reader will be able to detect the collision. The reader will then broadcast a bit indicating whether tags who broadcast a 0 or tags who broadcast a 1 should continue. Essentially, the reader chooses a "branch" from the binary tree of ID values. Tags which do not match the reader's choice will
cease participating in the protocol. As the reader continues to move down the branches of the binary tree, fewer tags will continue operating. If all tags are unique, at the end of the protocol only a single tag will remain in
operation. This process of addressing and isolating a single tag is referred to as ***singulation***.

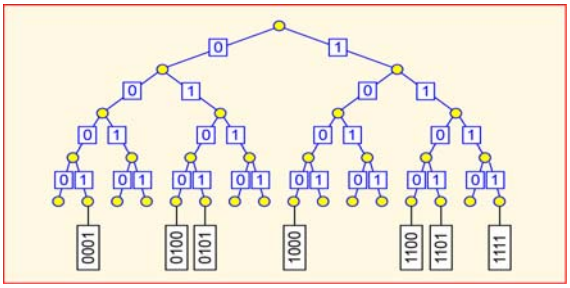

Fig 3.1 Binary Tree Walking

3.3 Limitations of designing secure RFID systems

Securing an RFID system has two major drivers, Active attacks as well as the Eaves dropping attacks.

3.3.1 Tag design

The active attacks can be prevented normally by public key cryptography and symmetrical crypto graphic principles.However this capability is limited due to the following reasons. [4]

- Cost
- No of Bits which can be stored on a Tag (96 bits)
- No of Read operations which can be performed
  The clock cycles available during a tag read operation depend on the operating frequency, tag technology and on various other factors. For example, tags operating at 915 MHz are required to hop frequencies every 400 ms due to RF regulations. The clock on a tag may operate at some multiple or fraction of the communication frequency.
- Power dissipation
  Power dissipation depends on the tag technology, operating frequency, power coupling mechanism and various other factors.
- No of gates which can be put on a tag chip
  Number of gates is limited because of the need for the smaller size of the tags.For example 200-2000 maximum.For cryptographic algorithms like AES or DES ,the number of gates needed is 20,000-30,000. This limitation reduces the capability to have extensive cryptographic capabilities in the tags.

3.3.2 Asymmetrical Channel Strength

In case of passive tags Asymmetry exists between the between the forward (tag-to-reader) and backward (reader-to-tag) channels. Since passive tags receive power via the forward channel, it is much stronger than the backward channel. As a result the forward channel may be monitored from a much greater distance than the backward channel. For example, a 915 MHz passive tag may have a 3-meter operating range, yet its forward channel may be monitored from 100 meters. In ideal conditions, a 915 MHz forward channel could theoretically be monitored from a kilometer. This asymmetry in channel strength could be exploited through eavesdropping. However to monitor the backward channel, an eavesdropper would have to be within the short range of the backward channel (e.g. 3 meters). It is because of this reason the consumer privacy can be compromised.

4. Security Proposals

This section gives a small introduction to various methods which can be used to protect RFID security. Active querying attacks may be addressed by limiting who is permitted to read tag data through access control. Eavesdroppers may be dealt with by ensuring that tag contents are not broadcast in the clear over the forward channel.

Secure Access

4.1 Security for Tags With No Cryptographic Capabilities [7]

- **Tag Killing:** The most straightforward approach for the protection of consumer privacy is to "kill" RFID tags before they are placed in the hands of consumers. A killed tag is truly dead, and can never be re-activated. The standard mode of operation proposed by the AutoID Center is that a tag can be killed by sending it a special "kill" command (including a short 8-bit "password") [12, 13]. For example, a supermarket might use RFID tags to facilitate inventory management and monitoring of shelf stocks. To protect consumer privacy, checkout clerks would "kill" the tags of purchased goods; no purchased goods would contain active RFID tags.
- **Active Jamming:** Active jamming of RF signals is another, related physical means of shielding tags from view. The consumer could carry a device that actively broadcasts radio signals so as to block and/or disrupt the operation of any nearby RFID readers. This approach may be illegal – at least if the broadcast power is too high – and is a crude, sledgehammer approach. It could cause severe disruption of all nearby RFID systems, even those in legitimate applications where privacy is not a concern.
- **Tag Shielding:** An RFID tag may be shielded from scrutiny using Faraday Cage —a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). If high-value currency notes come equipped with active RFID tags, then it is likely that those foil-lined wallets will become big sellers! At least one company already offers a Faraday-cage-based product for privacy purposes [17].

However, RFID will be used in a vast range of objects which cannot be placed conveniently in containers, such as clothing [1, 16], wrist-watches. Therefore there is a need for authenticated access to RFID tags. Below are some proposals which facilitate this.

- **Insubvertible Encryption-** This is a cryptographic primitive but does not need the tag to have any cryptographic capabilities. This is suggested to avoid tracing**.** Authorized users can store encryption into a RFID chip that can be randomized by anyone. In this scheme cipher texts which is produced contains implicit proofs of being "safe" to randomize. if the proof is invalid the randomizer has the option to obliterate the contents with "safe" but meaningless ciphertexts, destroying the adversarial hidden channel and preventing tracing. There fore the legitimate issuers can initiate and re-set the contents of RFIDs, enabling them to use it for recognizing the tag later. Illegitimate issuers can also re-set the value of tags—these are passive entities—but any contents they write to them will be destroyed by honest readers that participate in the scheme. [11]

4.2 RFID Tags with Cryptographic Capabilities

- **Hash Lock:** This proposal is based on the public-key cryptographic primitives or symmetric primitives requiring secure key distribution. Each hash-enabled tag in this design has a portion of memory reserved for a temporary *metaID*. The Tag owner "locks" tags by first selecting a key at random, then computing the hash value of the key. The hash output, designated as the *metaID* s stored on the tag and the tag is toggled into a locked state. The key and the metaID are stored in a back-end database. To "unlock" a tag, the owner first queries the metaID from the tag and uses this value to look up the key in a back-end database. The owner transmits this key value to the tag, which hashes the received value and compares it to the stored metaID. If the values match, then the tag unlocks itself and offers its full functionality to any nearby readers. [4]

- **Authentication using AES algorithm** :In this proposal the authors talk about using AES algorithm for authentication in a challange response based protocol.As per the standards for 13.56MHZ frequency, the time for tag to respond is 32 clock cylces at a frequency of 100KHz,which is not enough for AES algorithm for encryption.So a protocol of interleaved challenge and response protocol is This gives the tag enough time (18ms) to encrypt message using AES .In this way in the system proposes that 50 tags could be authenticated in 1 second. The authors proposed AES implementation as a 32 bit architecture which allows to quarter the power consumption as compared to 128 bit.This comes at a cost of increasing the time for encryption which can be derived from using interleaved challenge respond.[19]

- **HB Protocol for RFID:** In this approach presented by S.Weis and A. Jules a particular human-to-computer authentication protocol designed by Hopper and Blum (HB) [18, 19], is shown to be practical for low-cost pervasive devices like RFID Tags. HB protocol is essentially a challenge and response protocol. Suppose Alice and a computing device C share an k-bit secret $\boldsymbol{x}$, and Alice would like to authenticate herself to C. C selects a random challenge $\boldsymbol{a} \in \{0, 1\}^k$ and sends it to Alice. Alice computes the binary inner-product $\boldsymbol{a} \cdot \boldsymbol{x}$, then sends the result back to C. C computes $\boldsymbol{a} \cdot \boldsymbol{x}$, and accepts if it matches its own calculation. In a single round, someone imitating Alice who does not know the secret $\boldsymbol{x}$ will guess the correct value $\boldsymbol{a} \cdot \boldsymbol{x}$ half the time. By repeating this challenge and response for r rounds, Alice can lower the probability of naively guessing the correct parity bits for all r rounds to 2^{-r}. Alice can also inject noise into her response. The noise bit ν can be easily generated. Alice intentionally sends the wrong response with constant probability η. C then authenticates Alice's identity if fewer than ηr of her responses are incorrect.[10]

- **HB+ Protocol for RFID:** A Jules and Stephen Weis presented HB+ protocol for Authentication against active adversaries .They argue that HB protocol will work against passive adversaries whereas HB+ prevents corrupt readers from extracting tag secrets through adaptive (non-random) challenges, and thus prevents counterfeit tags from successfully authenticating themselves. HB+ requires marginally more resources than the "passive" HB protocol. In this case, rather than sharing a single k-bit random secret x, the tag and reader now share an additional k-bit random secret y. Unlike the case in the HB protocol, the tag in the HB+ protocol first generates random k-bit "blinding" vector b and sends it to the reader. As before, the reader challenges the tag with a k-bit random vector a. The tag then computes $z = (a \cdot x) \Theta (b \cdot y) \Theta \nu$, and sends the response z to the reader. The reader accepts the round if $z = (a \cdot x) \Theta (b \cdot y)$. As before, the reader authenticates a tag after r rounds if the tag's response is incorrect in less than ηr rounds.[10]

4.3 Secure Anti-Collision

The Binary Tree-Walking anti-collision algorithm discussed in the previous section has an inherent security flaw due to the asymmetry between forward and backward channel strengths. Every bit of every "Singulated" tag is broadcast by the reader on the forward channel. At certain operating frequencies, a long-range eavesdropper could monitor these transmissions from a range of up to 100 meters and recover the contents of every tag

Many research papers have been submitted to deal with this. Some of the approaches are discussed below.

- **Blinded Tree-Walking:** This is a variant of binary tree-walking which does not broadcast insecure tag IDs on the forward channel and does not adversely affect performance. Also called "Silent Tree-Walking". Assume a population of tags share some common ID prefix, such as a product code or manufacturer ID. To singulate tags, the reader requests all tags to broadcast their next bit. If there is no collision, then all tags share the same value in that bit. A long-range eavesdropper can only monitor the forward channel and will not hear the tag response. Thus, the reader and the tags effectively share a secret bit value. When a collision does occur, the reader needs to specify which portion of the tag population should proceed. If no collisions occur, the reader may simply ask for the next bit, since all tags share the same value for the previous bit. .[4]
- **Randomized Tree-Walking:** The general idea behind Randomized Tree-Walking, due to Rivest [85], is for each tag to generate a temporary random

pseudo-ID each tree traversal. The reader will perform a normal tree-walking scheme on the pseudo-ID values. Once a tag is singulated, it will send its normal ID over the backward channel.[4]

- **Blocker Tag:** Consumer privacy can also be obtained by a basic blocker tag .This simulates the full set of 2*k* possible RFID-tag serial numbers. We may call such a tag a "full blocker" or a "universal blocker." Now, whenever the reader queries tags in the subtree of a given node *B* for their next bit value, the blocker tag simultaneously broadcasts both a '0' bit and a '1' bit. This forced collision drives the reader to recurse on all nodes, causing the reader to explore the entire tree. If the reader had enough time, memory, and processing power to complete the tree-walking algorithm in these circumstances, it would output the entire set of all 2*k* possible tag serial numbers. This set is very large, at least of the size of 264 in even the most basic system – and the reading process is designed to execute very rapidly. In practice, therefore, the reader may be expected to stall after reaching only a few hundred leaves in the tree. The net effect is that the full blocker tag "blocks" the reading of all tags. There can also be "Selective Blocker Tags".[7]

III. RFID CURRENT APPLICATIONS AND VENDORS

This section presents some existing applications of RFID. An effort has been made to present some vendors involved in the application. There are almost as many RFID applications as there are business types. Broadly they can be divided into following categories.

5.1 Automotive - Auto-makers have added security and convenience into an automobile by using RFID technology for anti-theft immobilizers and passive-entry systems.

Vendor-Texas Instruments: Texas Instruments offers several Passive tags and Readers in different frequency ranges. These include: low frequency (134.2 kHz), high frequency (13.56 MHz), and ultra-high frequency (860 - 960 MHz). Below is the description of one of the company's RFID tag called DST.

Digital Signature Transponder (DST): DST consists of a small microchip and antenna coil encapsulated in a plastic or glass capsule. It is a *passive* device. A DST contains a secret, 40-bit cryptographic key which is field-programmable via RF command. In its interaction with a reader, a DST authenticates itself by engaging in a challenge-response protocol. The reader initiates the protocol by transmitting a 40-bit challenge. The DST encrypts this challenge under its key and returns a 24-bit response. It is thus the secrecy of the key that ultimately protects the DST against cloning and simulation. DSTs are deployed in several applications that are notable for wide-scale deployment and the high costs (financial and otherwise) of a large-scale security breach.

Fig 5.1 At left, an Exxon Mobile Speed Pass both inside and outside its casing. At right, an immobilizer equipped car key. The small chip is embedded into the plastic head of the key.

Deployment of DST

- **Vehicle Immobilizers:** Immobilizers deter vehicle theft by interrogating an RFID transponder embedded in the ignition key as a condition of enabling the fuel-injection system of the vehicle. The devices have been credited with significant reductions in auto theft rates, as much as 90%.

- **Electronic Payment:** Used in Exxon Mobil Speed Pass system, with more than seven million cryptographically-enabled keychain tags accepted at 10,000 locations worldwide.

5.2 Animal Tracking - Ranchers and livestock producers are using RFID technology to meet export regulations and optimize livestock value. Wild animals are tracked in ecological studies, and many pets that are tagged are returned to their owners.

Vendor-Advanced ID Corporation: Provides Low frequency (LF) and UHF RFID chips and readers

- **Pet Identification:** Since 1994,they have marketed low frequency (LF) chips and readers to **A**merican Veterinary Identification Devices ("AVID") for the purpose of permanent identification in the pet industry
- **Livestock Tracking:** Their ultra high frequency (UHF) chips are used in visual ear tags.Each UHF tag or LF microchip is uniquely numbered, providing positive global identification of an individual animal.

5.3 Asset Tracking - Hospitals and pharmacies meet tough product accountability legislation with RFID; libraries limit theft and keep books in circulation more efficiently

Vendor-AXCESS Inc. Manufacture various kinds of Active Tags for supply chains. Some of them are

- Asset Tag
- Vehicle Tag
- Credential Tag
- Personnel Tag
- Patient Tag

Fig 5.2 A typical Asset Tag

5.4 Supply Chain - WalMart, Target, BestBuy, and other retailers have discovered that RFID technology can keep inventories at the optimal level, reduce out-of-stock losses, limit shoplifting, and speed customers through check-out lines. WalMart is using the technology to reduce 'out-of-stocks' and control excess inventory .

Vendors - Alien Technologies: Alien Technologies recently sold 500 million RFID tags to Gillette at a cost of about ten cents per tag. Alien Technology offers a range of EPC compliant UHF solutions for pallet, case and item level tagging. Alien manufactures electronic product code (EPC) Class 1 ,Gen 2 tags.

ALL-9338-02 "Squiggle™"
- EPC Class 1, Gen 2
- General purpose for use on corrugate, plastic and paper.

Fig 5.3 A Gen- Tag by Alien Technologies

ALR-9800
Alien's new-generation, multi-protocol reader, designed for EPC Class 1 Gen 2 compliance.

Fig 5.3 A Gen-2 Reader by Alien Technologies

Other Vendors: There are many more vendor of RFID Tags and Reader and Integrated systems.some of them are Impinj,Symbol,Xterprise[18]

6. Emerging applications of RFID

- **Tracking apparel:** Marks & Spencer, one of the largest retailers in the UK, is tagging apparel items with ultra high frequency (UHF) tags beginning in Fall, 2003.

- **Tracking consumer packaged goods (CPGs):** In 2003 UK Super market chain Tesco ran a three-month test of " Smart Shelve " .The test was performed on DVDs stocked in Tesco's flagship Sandhurst store, near London, DVDs were tagged and programmed. Shelving units were equipped with 13.56 MHz readers from Philip semiconductors. The system put a time stamp next to each movement of a product. So if a dozen DVDs left the backroom at 4:47 PM and never got to the shelf, the retailer could check who had access to the backroom at that time and focus the investigation on those employees that had access. This test was however capped at WalMart and Gillette.

- **Tracking tires:** RFID Technology could be used in tire recalls." Instead of having to recall tires nationally or 'from the East Coast,' tire companies will be able to recall a bad lot from the twelve stores they were distributed to. We can only imagine how much money could be saved in such an example. Some analysts' projections anticipate auto-related RFID investments approaching as much as $2 billion by 2011. Michelin has developed a patent-pending RFID tire transponder, pictured below, which consists of a UHF RFID integrated circuit and two spring-wire antennas. Not only does the tag identify the tire, it actually monitors the tire temperature and pressure, using the kinetic energy from the tire to power itself as it rotates.

- **Tracking currency:** The European Central Bank was moving forward with plans to embed RFID tags as thin as a human hair into the fibers of Euro bank notes by 2005, in spite of consumer protests. The tags could allow currency to record information about each transaction in which it is passed. Governments and law enforcement agencies hail the technology as a means of preventing money-laundering, black-market transactions, and even bribery demands for unmarked bills. However, It has yet to be implemented.

- **E Passports**: In order to increase the security of United States travel documents, the Government has developed a new 'electronic passport' system. This will contain RFID tags: chips that will wirelessly send passport and biometric information to an inquiring RFID reader. This new passport system has already been deployed in October 2006. Except for Andorra, Brunei and Liechtenstein, all of the 27 countries whose citizens can travel to the

U.S. without a visa are now issuing "e-Passports," Reading a passport's RFID chip requires a password generated by scanning the machine readable data on the inside front cover. Additionally, a small shield in the front cover is supposed to only allow wireless passport reading when the booklet is open. However A German computer security consultant has already shown in Aug 2006 that he can clone the electronic passports that the United States and other countries are beginning to distribute this year.

- **Elderly Health Care**: By tagging key objects in a senior's home – such as prescription drug bottles, food items, and appliances – and embedding small RFID readers in gloves that can be worn by that individual, that person's daily habits can be monitored remotely by a caregiver. This system would develop more accurate record-keeping for medical treatment purposes and could facilitate independent living for senior citizens.**VeriChip** is one such chip. It is a human-implantable RFID (radio frequency identification) device from VeriChip Corporation, a wholly owned subsidiary of Applied Digital Solutions of Delray Beach, Florida. On February 10th, 2006, a surveillance company in Cincinnati became the first American business to use the VeriChip for access to its datacenter.

- **Immigration Tracking:** Scott Silverman, Chairman of the Board of VeriChip Corporation, proposed **VeriChip** as a way to identify immigrants and guest workers. This however has attacked by privacy experts who warn that once people are numbered with a remotely readable RFID tag like the VeriChip, they can be tracked. Once they can be tracked, they can be monitored and controlled.[19]

7. Future RFID Applications

- **"Smart" products**
  Clothing, appliances, CDs, etc. tagged for store returns
- **"Smart" appliances**
  - Refrigerators that automatically create shopping lists
  - Closets that tell you what clothes you have available, and search the Web for advice on current styles, etc.
  - One such application is **VistaCrafts RFIQin**, available in Japan, which comes with 24 recipe cards. The pan reads the card you show and "tells" the cook top what to do to perfectly monitor each cooking step and perfectly reproduce the most difficult recipes. Each pan handle is embedded with an RFID chip that uses a proprietary signal to communicate with coordinated chips in the cook top and special recipe cards that monitor each cooking step for a particular dish.

Fig 7.0 VistaCrafts RFIQin

Fig 7.1 **RFID recipe cards**

- **RFID-enabled mobile phones (e.g., Nokia):**
  Scan movie poster to learn show times
  Scan consumer product to get price quotes
- **Recycling** Plastics that sort themselves

III. Bibliograpphy

[1] About Inventors web site
http://inventors.about.com/library/inventors/blbar_code.htm
[2] Royal Air Force. History: 1940.
http://www.raf.mod.uk/history/line1940.html.
[3] Electronic privacy information center.
http://www.epic.org/privacy/rfid/
[4] Security and Privacy in Radio-Frequency Identification Devices by Stephen August Weis Massachusetts Institute Of Technology May 2003
[5] Wikepedia Electronic encyclopedia
http://en.wikipedia.org/wiki
[6] International Organization for standardization.
http://www.iso.org/
[7] The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. A. Juels, R. L. Rivest, and M. Szydlo. ACM CCS '03.
[8] Texas Instruments. http://www.ti.com/rfid/
[9] RFID Journal. www.rfidjournal.com

[10] "Authenticating Pervasive Devices with Human Protocols" Ari Juels and Stephen A. Weis Advances in Cryptology -- CRYPTO 2005, Presentation Slides LNCS, volume 3621, pages 293-308, 2005
[11] Untraceable RFID Tags via Insubvertible Encryption (Giuseppe Ateniese, J. Camenisch and B. de Medeiros), in 12th ACM Conference on Computer and Communications Security (CCS), 2005.
[12] EPCglobal http://www.epcglobalinc.org/
[13] Tom Ahlkvist Scharfeld. An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Indentification System Design. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, August 2001.
[14] http://www.axcessinc.com/
[15] Alien Technologies. http://www.alientechnology.com/
[16] ActiveWave Inc. http://www.activewaveinc.com
[17] Mobile Clock mCloak: Personal / corporate management of wireless devices and technology, 2003. www.mobilecloak.com.

[18] RFID Exchange
http://www.rfidexchange.com/applications.aspx
[19] Strong authentication of RFID systems using AES algorithm Martin Feldhofer, Sandra dominikus, Johannes Wlkerstofer