A Survey of RFID Deployment and Security Issues

Amit Grover* and Hal Berghel*

Abstract—This paper describes different aspects of a typical RFID implementation. Section 1 provides a brief overview of the concept of Automatic Identification and compares the use of different technologies while Section 2 describes the basic components of a typical RFID system. Section 3 and Section 4 deal with the detailed specifications of RFID transponders and RFID interrogators respectively. Section 5 highlights different RFID standards and protocols and Section 6 enumerates the wide variety of applications where RFID systems are known to have made a positive improvement. Section 7 deals with privacy issues concerning the use of RFIDs and Section 8 describes common RFID system vulnerabilities. Section 9 covers a variety of RFID security issues, followed by a detailed listing of countermeasures and precautions in Section 10.

1. INTRODUCTION

A wide range of Automatic Identification (Auto-ID) systems including magnetic stripes, Optical Character Recognition (OCR), barcodes, biometrics, contact memory buttons, and smart cards have been around for many years and have helped in increasing the efficiency as well as efficacy of different business processes. Each of these technologies has their pros and cons and has specific target-applications for which they have their niche markets. Although OCR systems allow simultaneous manual and auto-identification, the prohibitive cost of the readers prevented the widespread use of the technology in applications other than banking and production [1]. While barcodes have proved to be a cost-effective way for managing inventory, they have certain inherent disadvantages such as limited information-storing capacity; a strict line of sight requirement between the scanner and the barcode, which effectively prevents multiple barcodes to be processed simultaneously; limited data redundancy and error correction; and a lack of in-built data-security standards in various symbologies. Biometrics, such as fingerprinting, retina scans, iris scans, and voice recognition are all considered to be strong identification solutions in automatic access control but some people find these technologies obtrusive thereby limiting their exposure. Contact memory buttons are robust Auto-IDs that are capable of withstanding adverse environments that overcome a number of barcode system limitations and support features such as high data storage capacity (up to 8 MB), the ability to write data multiple times, and data security using encryption. However, despite these advantages, the requirement for con-

tact to take place between the reader and the button thus making them suitable for only limited applications; coupled with the fact that these are proprietary systems, has severely restricted their market share [2]. Smart card (and derivatives such as memory card or microprocessor card), solutions use standard credit-card sized plastic cards with an integral data storage system that is designed to make financial transactions secure as well as faster, but they have to deal with the high cost of maintenance of their readers [3].

The globalization of businesses, the rise of e-commerce, and the need for more efficient supply chain management propelled the industry to invent a new generation contactless Auto-ID system called Radio Frequency Identification (RFID), which sought to overcome these limitations and to reduce human intervention in inventory-management and other industrial processes by drastically improving both the speed as well as accuracy of data collection and dissemination. RFID systems rely on Radio Frequency to transmit a tag-specific unique serial number to a reader or interrogator. The earliest predecessor of the RFID concept is believed to be a Soviet spy gadget that retransmitted incident radio waves with audio information. One of the earliest applications of RF transponders was the Friend-or-Foe (IFF: Identification, Friend or Foe) aircraft identification system that was used by the Royal Air Force during World War II to distinguish between enemy and Allied aircraft [4]. In the US, RFIDs have been used since the 1960s to manage nuclear and hazardous material. The modulated backscatter RFID tags, as demonstrated at the Los Alamos National Laboratory in 1973, are widely used today, particularly in the UHF and microwave spectrum. Popular applications of RFID, apart from inventory management throughout the entire supply chain, include patient tracking, toll-gate payment systems, high value asset tracking for defense applications, animal tracking, casino management, automobile security, financial transaction systems, and the tracking of pharmaceuticals etc. Different tag variables, such as the power source, the class, and generation, as well as different system frequencies, standards, and protocols affect various performance parameters such as data transmission range, reading distance, life span, the amount of data, and security issues. These different variables are described in greater detail in the following sections.

2. RFID ENVIRONMENT

Depending on the application that is used, the actual characteristics of the different components will vary greatly. However, the primary components of a typical RFID infrastructure include:

(a) A *transponder* or tag with a unique identifier that facilitates auto-identification of any object to which the tag is attached.
(b) A reader or *interrogator* that manages the radio frequency communication with the tags.
(c) A *middleware* or reader interface layer, which is essentially a type of software that acts as an interface between the basic RFID hardware components, and the software application tasked with data collection related to tag-events.

Since RF communication requires the transmission and / or reception of data, the reader, as well as the tag, are in essence RF transceivers that are equipped with suitable antennas. The reader acts as a transmitter in the reader-to-tag communication, which is referred to as the *for-*
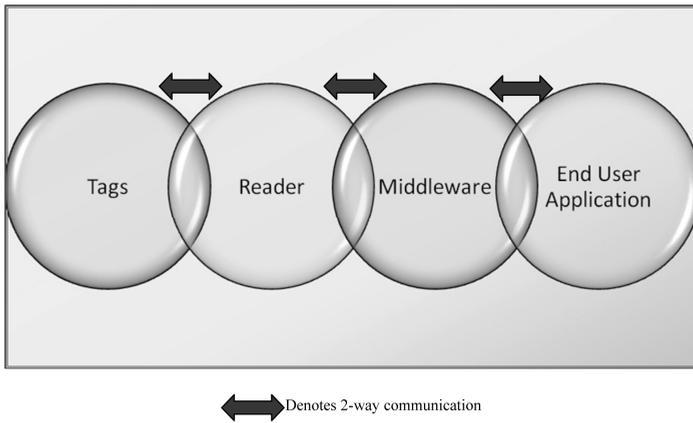
Fig. 1. RFID Infrastructure Components

ward link; and as a receiver in the tag-to-reader communication is referred to as the ***back link***
[5]. The tag communicates by acting in the opposite mode than that of the reader in each of the
link directions. Apart from these fundamental components, certain RFID systems are also
equipped with an optional infrared-capable transmitter known as a ***signpost***, which solves the
problem of ***RF signal bleeding*** and provides more precise location identification [6]. Real world
RFID implementations indicate substantial variations in the type or form of the fundamental
components used, based on application-specific requirements. These variations are described in
the following sections in greater detail.

3. RFID TRANSPONDERS

A typical RFID transponder consists of an integrated circuit and an antenna embedded in a
plastic or Mylar substrate. The IC is responsible for responding to the signals transmitted by the
reader and replying with the tag's unique identifier, and modulating and demodulating the radio-
frequency signal. The actual communication is facilitated by the antenna that absorbs the incom-
ing RF waves and utilizes the absorbed energy to activate the IC. Different applications focus on
different chip characteristics such as the memory capacity, the ability to alter the antenna's im-
pedance, the power conversion efficiency, and the ability to handle data collision. The antennas
reflect the power back by using a process known as ***backscatter***. Unlike ***specular reflection***,
backscattering is a ***diffuse reflection*** (wherein an incident ray is reflected at multiple angles) of
waves, particles, or signals due to scattering (deviation from a straight trajectory by one or more
localized non-uniformities in the transmission medium) back to the direction they came from.
The size and design characteristics of the antenna greatly affect the efficacy of the coupling be-
tween the transponder and the reader's electromagnetic field. The bigger the size of the antenna,
the greater is the range that the tag can support. Coil shaped antennas are best suited for handing
Low Frequency (LF) and High Frequency (HF) radio communication, while traditional radio
antennas are better suited for Ultra High Frequency (UHF) communication [7]. Since radio
waves behave differently at different frequencies, their main characteristics are summarized in
Table 1 [8].

Table 1. RFID Frequency – Antenna relationship

LF	Near	Inductive	Coil
HF	Near	Inductive	Coil
UHF	Far	Radiative	Linear

Near Field communications rely completely on magnetic waves. The range is typically just a few inches and has an inverse sixth power ($1/r^6$) relationship with the range [9].

As per *Gauss's Law or flux theorem*, the electric flux through any closed surface is proportional to the enclosed electric charge.

The integral form of Gauss's law is represented as:

$$\oint_S \mathbf{E} \cdot \mathrm{d}\mathbf{A} = \frac{Q}{\varepsilon_0},$$

Where **E** is the electric field,

dA is a vector representing an infinitesimal element of area, http://en.wikipedia.org/wiki/Gauss%27s_law - cite_note-4

Q is the total charge,

ε₀ is the electric constant,

and **·** represents the dot product.

The surface integral of this dot product denotes the electric flux through the closed surface, **S**.

The differential form of Gauss's law is represented as:

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0}$$

Where **∇·E** is the divergence of the electric field, and *ρ* is the charge density.
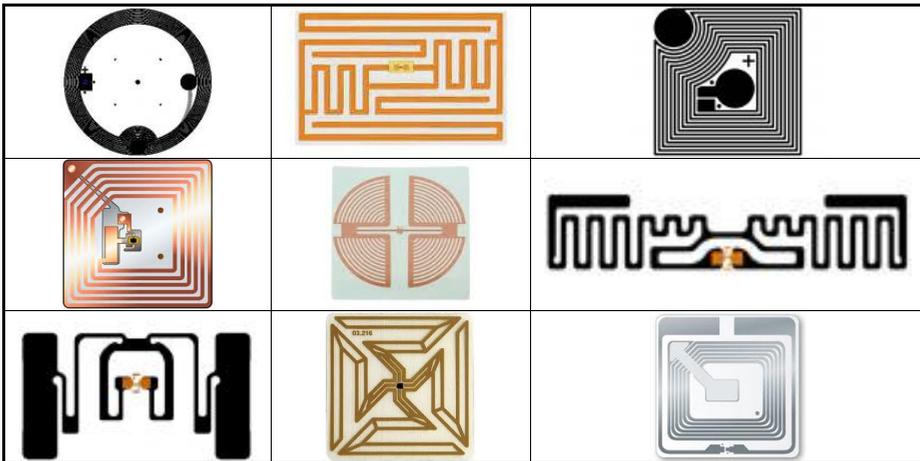

Fig. 2. Different types of RFID Transponder antennas

Application of the Gauss's law in the context of an RFID implementation implies that the amount of power absorbed by the transponder is optimal when the electric field created by the interrogator meets the tags at a perpendicular plane.

Since the strength of the coupling is affected by the antenna's capacitance, inductance and thereby the impedance characteristics, this implies that the design of the antenna plays a critical role in the overall performance of the RFID system. Applications that require RF coupling at different angles are best served by *orientation insensitive* antennas that are characterized by multiple turns and branches, whereas those that require direction-specific coupling on flat surfaces are better served by straight and long tags that provide an enhanced conductive area [10].Passive transponder formats that enjoy industry-wide acceptance include the Alien "12" tag, the Alien "Squiggle" tag, the Avery Dennison Strip tag, and the Rafsec Folded Dipole CCT tag. Based on the application, the antennas come in many different shapes and sizes, some of which are shown in Figure 2 [11].

3.1 RFID Tag Construction Formats

Different applications require transponders with different physical characteristics. Some common tag construction formats include disks or coins, glass or plastic housing, keys and key fobs, smart labels, coil-on-chips, and those that are embedded in smart cards [12]. The various construction formats are summarized in Table 2.

Table 2. RFID Tag Construction Formats

Disks or coins	This is the most common construction format. To withstand higher temperatures, an epoxy resin molding may be used.	
Glass or plastic housing	Animal tracking and identification can be done by injecting these transponders under the animal's skin.	
Keys and key fobs	Immobilizers or door locking applications for high security areas.	
Smart labels	This is a paper thin format where the tag is produced by careen printing or etching.	
Smart cards	Contactless smart cards facilitate transactions without swiping the magnetic stripe.	
Wristband	This facilitates contact-less access control.	

3.2 Tag Classifications

Based on the power source that drives the communication between the tags and the reader, RFID tags can be classified as active, passive, or semi-passive tags. The differences are indicated in Table 3.

The Auto-ID Center further classified different RFID tags on the basis of their functionality into seven different classes. These classes, as recognized by EPCglobal, are summarized in Table 4 [13, 14]:

Table 3. Types of RFID Tags

Active	Has its own battery that is used to broadcast signals over great distances. Usually bigger in size and capable of carrying more information.
Passive	No inbuilt power source. The signal from the RFID reader creates an electromagnetic field that powers the tag. Much cheaper.
Semi-Passive or Battery Assisted Passive (BAP)	Equipped with an onboard battery that drives the chip's circuitry but power for communication of the signal is derived from the reader's electromagnetic field as in the case of passive tags.

Table 4. RFID Tag Classes

1	Class 0	Passive, read-only uses Symbol's proprietary protocol.
2	Class 0+	Passive, write-once using Class 0 protocols.
3	Class I	Passive, read-only backscatter tag with one-time, field-programmable, non-volatile memory.
4	Class II	Passive, write-once, backscatter tag with up to 65 KB of memory and encryption support.
5	Class III	Rewriteable, Semi-passive backscatter tag, with up to 65 KB memory.
6	Class IV	Rewriteable, active tag that uses a built-in battery to power its own communication with the reader.
7	Class V	Similar to Class IV tags, but with enhanced capability to power and read Class I, II, and II tags and to read other Class IV and V tags.

4. RFID INTERROGATORS

RFID readers interrogate the tags as they move into the range of the electromagnetic field that has been generated by the radio frequency and supply the tag's unique identification data to the middleware for the specific application. These EPC class 5 devices are responsible for managing the communication between the different components of a typical RFID infrastructure and include components such as an antenna that transmits the RF wave, a **Digital Signal Processor (DSP)** chip that controls data transmitted using frequency or amplitude modulation, and a reader Application Programming Interface (API) that facilitates the end-user application to correctly record and interpret tag read events. The DSP chip is also responsible for the real-time data communication between the transponders and the interrogators. Characteristics such as directivity, signal gain, polarization, radiation efficiency, form factor, and tag density play a crucial role in selecting readers for different applications. Signal directivity is an important issue when *'phantom-reads'* introduce errors because RF signals are also read from adjoining interrogation zones. An antenna's gain combines its directivity and electrical efficiency and describes how well the antenna transforms input power into radio waves.

$$G = E_{antenna} \cdot D$$

Where **G** = gain
E$_{antenna}$ =Antenna efficiency, and
D = directivity
The power gain for a particular direction given by an elevation θ and azimuth φ,is represented as:

$$G(\theta, \phi) = E_{antenna} \cdot D(\theta, \phi)_,$$

Where **D(θ,Φ)** = directive *gain*.
Antenna efficiency is either expressed as the ratio between its radiation resistance and its total resistance or as the ratio between its input power and its radiated power:

$$E_{radiation} = \frac{R_{radiation}}{R_{total}} = \frac{P_{radiated}}{P_{input}}$$

Where **R$_{total}$ = $R_{radiation}$ + R_{coil} + R_{ground} + R_{other}** , (i.e., the sum of coil losses [Rc], ground losses [Rg], and other losses [Ro] including ohmic and capacitive losses.)

Polarization refers to the orientation of the antenna with respect to the electromagnetic field and can be linear or circular. Radiation efficiency depends on the antenna design and reflects the strength of the transmitted signal. The form factor classification for mobile interrogators indicates either a dedicated reader or an add-on interface to conventional computers using technologies such as PCMCIA (Personal Computer Memory Card International Association), SDIO (Secure Digital Input Output), or Compact Flash cards [15]. Tag density refers to the maximum number of transponders that a reader can register per second.

The ***maximum transmission range,*** r$_{max,}$ for RFID tags is given by the Friis free space formula: [16]

$$r_{max} = \frac{\lambda}{4\pi} \sqrt{\frac{P_t G_t G_r \tau}{P_{th}}}$$

λ = wavelength
P_t = transmitted power from the reader
G_t = gain of transmitter antenna
G_r = gain of receiver tag
τ = power transmission coefficient
P_{th} = minimum threshold power of the reader

4.1 FFCA, AEN, and PLCM: RFID ImplementationConsiderations

An RFID implementation requires proper planning to ensure that the new deployment does not interfere with any existing equipment that uses electromagnetic radiation and also to ensure that appropriate RFID components are chosen to deliver optimum performance, given the envi-

ronmental constraints. This is achieved by using a technique known as the ***Full Faraday Cycle Analysis (FFCA).*** The FFCA has two primary components: AEN and PLCM. AEN is the ***Ambient Electromagnetic Noise*** in the environment that is created by other gadgets that can interfere with the radio frequency communication of an RFID implementation. A detailed AEN analysis includes identifying all the spots that are susceptible to AEN along with their measurements. Based on the cause of the AEN, steps can be taken to either eliminate the AEN or to find a way to accommodate it by selecting the appropriate technologies / components for the RFID solution. The next stage is the process of mapping out the RF path in the different interrogation zones based on the AEN measurements. This process is known as RF ***Path Loss Contour Mapping (PLCM***) [17].

5. RFID STANDARDS AND PROTOCOLS

5.1 Electronic Product Code

The ***Universal Product Code (UPC)*** is a barcode symbology used for tracking retail inventory in stores. UPC is based on GS1's GTIN-12 and consists of twelve numeric characters that uniquely identify a company's individual product. The structural detail of a UPC symbol is shown in Figure 3.

The limited amount of data that a UPC barcode can accommodate implies that one of its limitations is that it gives information only about the manufacturer and product code, but not about each individual piece of item.

Typical Universal Product Code Symbol

Out of the total 12 digits encoded, the company prefix can be 6 to 10 digits long

Fig. 3. UPC Symbol Structure (Source:http://www.gtin.info/upc/)

This limitation can be overcome by using EPC or the ***Electronic Product Code***, which can store much more information, and is designed to serve as a unique global identifier for all physical objects. The EPC was developed by the Auto-ID Center as a global and open standard. Apart from a unique identification number for each item of the inventory, the EPC information can include additional information such as the date of manufacture, the product's origin, and its shipment destination, etc. The EPC structure is defined in the EPCglobal Tag Data Standard. It is a 96-bit number that consists of a header and three sets of data. The 96-bit EPC can support sufficient capacity for 268 million companies, thereby allowing each manufacturer to support up to 16 million object classes with 68 billion serial numbers in each class [18]. An example of a typical EPC code is shown in Figure 4.
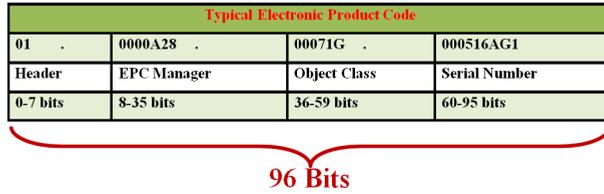
Typical Electronic Product Code			
01 .	0000A28 .	00071G .	000516AG1
Header	EPC Manager	Object Class	Serial Number
0-7 bits	8-35 bits	36-59 bits	60-95 bits

96 Bits

Fig. 4. EPC structure

Header: The header identifies the EPC version number, which identifies the type of EPC data to follow.

EPC manager Number: The second part of the number identifies the company or manufacturer of the item.

Object Class: The third part refers to the exact type of product and is functionally similar to a *stock-keeping unit (SKU).*

Serial Number: The fourth part is the item's unique identifier.

Apart from the data structure, the EPC also covers the air interface protocol and the network for getting tag information. It defines contents and encodings for all the different classes of transponders along with coupling, frequency, and communication protocols for Class 0 and Class I transponders [19].

5.2 RFID Air Interface Protocol

The Air Interface protocol is responsible for communication between the reader and the tags and manages modulation/de-modulation as well as collision avoidance for the transmitted data. The standard used with EPC Generation 2.0 protocols is the modified slotted ALOHA protocol, which is a random access protocol for sharing broadcast channel access among a number of users with relatively low throughput demand. Anti-collision methods may be designed for space domain, frequency domain, or time domain. Most RFID implementations employ time domain anti-collision, wherein fractional communications from the transponders are varied in time. Time domain anti-collision methods support both synchronous, as well as asynchronous schemes [20].

Popular RFID standards used for different applications are listed in Table 5:

Table 5. Popular RFID Standards

	Standard	Purpose or Application Area
1	ISO/IEC 18000	RFID for item management:
	Part 1	Generic parameters for air interfaces for globally accepted frequencies.
	Part 2	Parameters for air interface communications that are below 135 kHz.
	Part 3	Parameters for air interface communications at 13.56 MHz.
	Part 4	Parameters for air interface communications at 2.45 GHz.
	Part 5	Parameters for air interface communications at 5.8 GHz.
	Part 6	Parameters for air interface communications at 860–960 MHz.
	Part 7	Parameters for active air interface communications at 433 MHz.

Table 5. (continued)

	Standard	Purpose or Application Area
2	ISO 14223	RFID of animals – Advanced transponders.
3	ISO/IEC 14443	HF (13.56 MHz) standard for High FIDs for RFID-enabled passports under ICAO 9303.
4	ISO/IEC 15693	HF (13.56 MHz) standard for High FIDs that are widely used for non-contact smart payment and credit cards.
5	ISO 18185	Standard for electronic seals or "e-seals" for tracking cargo containers using the 433 MHz and 2.4 GHz frequencies.

6. RFID APPLICATIONS

The phenomenal proliferation of RFID chips in such a short amount of time is testimony to the fact that they can be used in a wide variety of applications to streamline different processes thereby producing a tangible and cost-effective increase in efficiency. Common applications that are well suited for RFID system implementations include [21]:

(a) **Automotive Industry**
    i. Vehicle Immobilizers
    ii. Inventory Management
    iii. Agile and Flexible manufacturing
    iv. Product life cycle management

(b) **Cattle Ranching and Animal Tracking**

(c) **Health Care**
    i. Patient tracking
    ii. Tracking of high value pharmaceuticals
    iii. Resources management

(d) **Manufacturing Industry**
    i. Supply change management
    ii. Warehousing
    iii. Asset management
    iv. Inventory control

(e) **Marine Terminal Operation**
    i. Container tracking and handling

(f) **Defense**
    i. Logistics and Inventory control
    ii. Field Combat
    iii. Marking of high value assets as well as targets
    iv. IFF aircraft detection
    v. Reconnaissance

(g) **Payment Transactions**

(h) **Retailing**
    i. Inventory and shelf management
    ii. Point of Sale management
    iii. Information kiosk and customer service
    iv. Loss prevention

    v. Customer loyalty programs
(i) **Transportation**
   i. Electronic toll collection
   ii. Automatic vehicle identification
   iii. Fleet management
   iv. Car parking and access control
   v. Electronic vehicle registration
(j) **Casino Chip Tracking**
(k) **Library Management**
(l) **IDs such as EDL and Passports**
(m) **Human Implants using VeriChip**

7. RFID PRIVACY ISSUES

As RFID proliferation spreads to different application-area; coupled with an increase in news-reports documenting various security vulnerabilities in RFID systems, a concern about the privacy issues is bound to be there. With RFIDs being introduced in employee access cards, Federal Personal IdentityVerification cards, new passports as well as passport cards, national driver's licenses, credit cards, human implants (such as those implemented by the Baja Beach nightclub in Barcelona for the ease of payment for preferred customers), patient tracking systems, personal clothing items and handbags, pet-tracking implants with the owner's information, and other merchandise; the concern about surreptitious and unauthorized tracking of individuals seems well founded [22]. Since RFID tags embedded in merchandize remain functional even after the products leave the point of sale and are no longer required for supply chain management activities, the unrestricted universal read capability of the tags can be used to monitor the movements of the customer, especially if the data is used in conjunction with his / her credit card or merchant loyalty card when they are used for the financial transactions [23]. Privacy advocates from Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) has exposed instances when these "spychips" or RFIDs containing customer IDs were embedded in customer loyalty cards without disclosing the fact to the customers. CASPIAN also highlighted an incident where a manufacturer was using hidden cameras activated by RFID chips to track merchandise. This was supposedly done to deter shoplifting, but the tags remained readable even after a customer bought the product and took it home [24]. Also news articles, such as the one titled, "Wal-Mart Uses RFID to Track Underwear" do nothing to increase the common man's confidence in the extent to which RFID chips can be used for invasion of privacy [25].

8. RFID VULNERABILITIES

Common RFID vulnerabilities include RFID data skimming, tag killing, and susceptibility to a DoS attack. These vulnerabilities are described below:

8.1 RFID Card Skimming

One of the biggest vulnerabilities of RFID systems is the fact that anyone with access to a

suitable reader can capture the information stored on the ID. This act of surreptitiously grabbing personal information from a victim's financial transaction card or any RFID enabled ID is known as "electronic pick-pocketing."

8.2 Tag Killing

RFID systems that support read/write memory are susceptible to unauthorized tag killings from large distances using specially configured readers. This allows the attacker to alter the tag memory content without the owner's knowledge.

8.3 Susceptibility of the EPCglobal Network to DoS Attacks

The EPCglobal Network is used to share product information between different stakeholders in the RFID implementation and relies on the Electronic Product Code (EPC) of different items. The EPCglobal Network manages dynamic information such as data regarding the movement of each individual object throughout the product life cycle. This management of all the phases of the supply chain management is achieved by using the following components:

   i. Object Naming Service (ONS)
  ii. EPC Discovery Services
 iii. EPC Information Services (EPCIS)
  iv. EPC Security Services

The ONS service is used for the discovery of object information on the basis of an EPC and uses a mechanism that is similar to the Domain Name System for resolving IP addresses. The response sent to the requester is a URL or IP-address that is obtained from the database when the corresponding Electronic Product Code indicates a match. A similarity in a mechanism with the DNS implies similar vulnerabilities and susceptibility to similar threats such as Denial of Service attacks.

8.4 Documented Hacks

Documented hacks for spoofing / cloning have highlighted vulnerabilities in almost all popular RFID implementations, including Chris Paget's cloning of the **Western Hemisphere Travel Initiative (WHTI)** compliant documents, such as the passport card and **Electronic Driver's License (EDL);** compromising the **VeriChip, MIFARE Classic card, Oyster card;** the cracking of the RFID encryption on an **American Express credit card** using an 8 USD reader, which is easily available on eBay, and the hacking of the Texas Instruments **RFID Digital Signature Transponder (DST) used in ExxonMobil SpeedPass systems,** etc. [26, 27, 28, 29]. In December 2007, a demonstration at the 24th Chaos Communications Congress (24C3) in Germany highlighted vulnerabilities of the ubiquitous MiFare Classic RFID chip by reverse-engineering the underlying Crypto-1 cipher. To make matters worse, it has been shown that it is possible to recover secret keys in mere minutes on an average desktop PC [30].

9. RFID SECURITY ISSUES

There are a number of serious security concerns that should be examined thoroughly before executing any widespread RFID deployment. Some common threats include:

9.1 RFID Spoofing

The process of unauthorized capturing of RFID tag information, including its unique tag ID (TID), and the retransmitting of this information to a reader thereby fooling it into believing that the data is coming from a legitimate transponder is known as, RFID spoofing. There have been numerous demonstrations that show the ease with which this can be done given the right equipment [31].

9.2 Tag Cloning

When RFID spoofing is done coupled with replicating the original form factor of the tag to give an identical product, the RFID tag is said to have been cloned. RFID cloning is also referred to as a, relay attack.

9.3 Side Channel Attacks

Rouge RFID readers can sniff RF communications between authorized tags and readers and might use confidential information that was obtained for carrying out industrial espionage or other illegal activities [32]. Such an attack on a Generation 1 RFID tag was demonstrated at the 2006 RSA Security annual conference.

9.4 RFID Viruses and Worms

Since RFID systems rely on middleware top communicate with business applications and backend databases, they are susceptible to malware attacks by hackers just as any other software based solution. It has been demonstrated that by merely scanning an infected RFID tag, it is possible to compromise the system's security and cause malicious pre-programmed damage to the backend database of an RFID implementation. Once the system has been compromised, the malware's payload can be designed to spread the damage by infecting other tags. Based on the propagation vector that is used, RFID malware can be classified as an RFID worm or RFID virus [33].

9.4.1 RFID Worm
An RFID worm is a malware that propagates using network connections by exploiting online RFID services, as well as via RFID tags. The RFID middleware server gets compromised when a legitimate RFID server is tricked into downloading and executing a malicious code. The compromised middleware server then unwittingly propagates the infection by replacing legitimate tag data with a malicious code.

9.4.2 RFID Virus
An RFID virus is a self-replicating malware that does not require a network connection for propagation. Once a tag with a specially crafted code is able to infect the backend software of

Fig. 5. A virus infected RFID chip (Source: http://www.rfidvirus.org/index.html)

the RFID implementation, the middleware can be used to churn out infected tags, which in turn have the capacity to infect the middleware layers of the same software in different geographic locations when these infected tags reach a new location and are scanned by the system.

9.5 SQL Injection

SQL Injection is an attack technique that exploits the vulnerability of database security by injecting a specific code to gain access to the underlying database. If incorrect input is not filtered properly, an attacker can cause real damage to the RFID database using malicious SQL commands.

9.6 Cross -Site Scripting

XSS is a web application vulnerability that allows the embedding of form input with malicious scripts. By injecting a client-side script into web pages, attackers can bypass client-side access control mechanisms and if this website is a necessary part of an RFID implementation, the attackers can compromise the RFID backend system.

9.7 Buffer Overflow

It is possible to exploit poorly written middleware code that doesn't dynamically check the data capacity of the tags to send irregular amounts of data to the reader and cause a buffer overflow that may either crash the RFID system or compromise some part of it that can be used for launching other attacks such as SQL injection to disrupt the integrity of the database.

9.8 Glue Code

A glue code is a code that is primarily used to "glue together" different parts of code to make different modules or components compatible with each other, but that does not specifically contribute towards a specific functional requirement. Glue code attacks focus on targeting various types of interfacing codes where there is a greater probability for introducing data format errors and thus crash the system. A typical RFID implementation uses a glue code to interface the RFID readers with the middleware or other end-user applications and is thus susceptible to glue code attacks.

10. COUNTERMEASURES / PRECAUTIONS

The threats and vulnerabilities inherent in RFID systems described above can be minimized to a great extent by employing the following countermeasures:

10.1 Faraday Cages

Faraday cages or meshes or shields use containers that are coated with certain metals that don't allow RF waves to pass through. Good examples include the use of credit card shielding sleeves or passport shielding cases such as those shown in table 6.

Table 6. RFID Shields

RFID Smart Card Shielding sleeve[34]	
RFID Passport shielding case[35]	
RFID Shielding Flipside Wallet [36]	

10.2 Kill Command

The kill command is a feature built into the RFID transponder that can be activated by a reader by transmitting an access code or PIN at the point of sale to make the tag unreadable [37]. Once the kill command has been executed there is no way to revive the tag's usability at a later stage.

10.3 Sleep Command

Unlike the kill command, the sleep command de-activates the RFID transponder only temporarily. For using the tag again it needs to be activated physically. As a security feature, it can't be re-activated remotely without the user's knowledge.

10.4 Encryption

Using encryption is a good way to secure the contents of the data that is transmitted so that even if an unauthorized person eavesdrops on the communication, the cipher text would not reveal meaningful information unless the key has also been compromised. The use of cryptographic protocols in conjunction with Challenge-response authentication systems or using "roll-

ing code" schemes, wherein the tag identifier information changes after each scan, are some other ways to make RFID communication more secure. Care should be taken not to transmit secret tag information over non-secure communication channels [38].

10.5 Clipped Tags

The Clipped Tag is an RFID tag that allows a consumer to tear off a portion of the tag after an item has been purchased. Produced as a collaborative effort by IBM and MarnlenRFiD, this helps in increasing consumer privacy, as once the antenna is clipped the distance from which the tags can be read is reduced drastically. Figure 6 shows an example of the clipped tags.
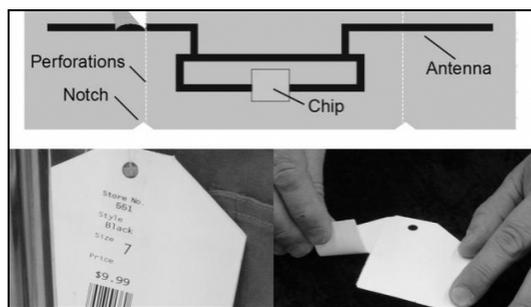

Fig. 6. Clipped Tags (Source:[39]:http://www.gizmag.com/go/5865/)

10.6 Blocking

A possible solution is introducing a blocker tag and extending the tag data structure format to handle a privacy bit that can be turned on or off like the kill command only when the reader has the appropriate access code or PIN [40].

10.7 Reduction of the Transmission Range

An easy solution to prevent unauthorized eavesdropping is to limit the transmission range of the tag to just a few centimeters. However, this method does not provide very strong security against determined eavesdroppers.

10.8 Randomization

One solution is to store a sufficiently large random number as the tag ID of a write-once read-only tag and the mapping of this number for the product information should be handled by a secure database so that even if the ID information is compromised, it doesn't reveal any meaningful information without access to the backend database [41].

10.9 EPC Gen 2 Standards

Using the *EPCglobal UHF Class 1 Generation 2* standard provides slightly more secure communications than Generation 1 standards, as it supports a memory-locking feature that can only be accessed by using the appropriate password. Though this prevents unauthorized altera-

tion of the memory, it is not fully secure, as the password is sent to the tag by the reader using the same channel as the secure data, thereby rendering it susceptible to password breaking attacks. Security is provided by encoding data transmitted by the reader using a 16-bit random number as communicated by the tag to the reader. This implementation assumes that strength of the backscattered signal as transmitted by the tag is not sufficient enough to be eavesdropped on by unauthorized entities. However, it has been shown that technologically, this assumption does not hold true. Plus, it also adds an overhead in the backend database management system [42].

10.10 RFID Enterprise Application Framework based on Kerberos

Another implementation that may be used to enhance security in dynamic RFID application environments is the proposed Enterprise Application Framework that is based on Kerberos and abstract business processes that includes a standard communication protocol and diverse security functions [43].

10.11 RFID Security Framework for Smart Home Environments

Futuristic smart home environments that envisage network and RFID enabled devices such as refrigerators, music systems, air-conditioning systems, mobile RFID-enabled smart phones, kitchen appliances, and other household gadgets are leaving the realm of science fiction and becoming a reality. These smart home networks are susceptible to their own security threats and vulnerabilities. A proposed "Security Framework for RFID-based Applications in Smart Home Environment" deals with tag locking and other strategies to provide authentication and data confidentiality, as well as integrity [44].

10.12 RFID Security for Ubiquitous Computing Environments

RFID is an integral part of the ubiquitous network computing environment and apart from the traditional focus on an RFID reader system and tag-based security, the practical usefulness of low-priced RFID tags can be increased with the help of a proposed security service that not only ensures availability but also provides for "forward channel security" and "secure status-acquisition technology" [45].

10.13 Other Security Threats

Other security threats, such as SQL injection, cross -site scripting, buffer overflow, and glue code attacks can be minimized or eliminated by using the following countermeasures:

   i. Strong input validation
  ii. Good software design
 iii. Proper filtering rules on the perimeter firewall that controls access to the middleware and end-user applications
  iv. Disabling scripts on the backend system
   v. Auditing buffer bounds and thoroughly checking for boundary condition errors
  vi. Accepting cookies only from trusted sites
 vii. Limiting account privileges for users that don't require full administrator access to the software component.

11. CONCLUSION

While the list of applications that may be streamlined or optimized using RFID implementations keeps on growing every day, it is also true that newer exploits keep demonstrating again and again that RFID in its current form is certainly not secure enough to deal safely with transactions involving sensitive personally identifiable and financial information. Though it is safe to say the technology has matured enough to be used in inventory management throughout the supply chain, toll-gate payment systems, high value asset tracking for defense applications, animal tracking, casino management, and automobile security; it would not be wise to completely rely on RFID based solutions for carrying out financial transactions and using ID documents embedded with RFID chips unless better safeguards are implemented to ensure foolproof security. While many of the security concerns can be handled by using existing technology, one of the biggest challenges is the general lack of awareness about the various RFID security issues.

REFERENCES

[1]   Finkenzeller, Klaus, *RFID Handbook*, John Wiley & Sons, Chichester, West Sussex England, 2003, pp.4.

[2]   Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.37.

[3]   Finkenzeller, Klaus*, RFID Handbook*, John Wiley & Sons, Chichester, West Sussex England, 2003, pp.5.

[4]   Newitz, Annalee, "The RFID Hacking Underground", Wired Magazine, http://www.wired.com/wired/archive/14.05/rfid_pr.html

[5]   Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.99.

[6]   Jerry Banks, David Hanny, *Manuel Pachano, Les Thompson, RFID Applied*, Wiley, 2007, pp.12.

[7]   Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.89.

[8]   Jerry Banks, David Hanny, *Manuel Pachano, Les Thompson, RFID Applied*, Wiley, 2007, pp.73.

[9]   Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.69.

[10] Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.91.

[11] http://www.rfid.averydennison.com/products.php#2

[12] Finkenzeller, Klaus, *RFID Handbook*, John Wiley & Sons, Chichester, West Sussex England, 2003, pp.13-20.

[13] Glover, Bill and Himanshu Bhatt*, RFID Essentials*, O'Reilly Media, Sebastopol CA, 2006, pp.72.

[14] "A Summary of RFID Standards", http://www.rfidjournal.com/article/view/1335/2

[15] Jerry Banks, *David Hanny, Manuel Pachano, Les Thompson*, RFID Applied, Wiley, 2007, pp.81.

[16] Jerry Banks, *David Hanny, Manuel Pachano, Les Thompson*, RFID Applied, Wiley, 2007, pp.112.

[17] Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.25,132

[18] RFID: The Next Generation Auto-ID Technology, http://www.mwjournal.com/Journal/RFID_Next_Generation_Auto_ID_Technology/AR_7232/

[19] Glover, Bill and Himanshu Bhatt, *RFID Essentials*, O'Reilly Media, Sebastopol CA, 2006, pp.72.

[20] Sweeney II, Patrick J., *RFID for Dummies*, Wiley Publishing, Hoboken NJ, 2005, pp.100.

[21] Jerry Banks, David Hanny, *Manuel Pachano, Les Thompson, RFID Applied*, Wiley, 2007, pp.297-363.

[22] "Are RFID Chips a Personal Security Risk?", http://www.smartertravel.com/travel-advice/are-rfid-chips-personal-security-risk.html?id=2672576

[23] http://www.spychips.com/index.html

[24] Garfinkel, Simon and Beth Rosenberg, *RFID Applications, Security, and Privacy,* Addison-Wesley, 2006, pp.63.

[25] http://barcodereader.systemid.com/index.php/2010/09/24/wal-mart-uses-rfid-to-track-underwear/

[26] http://cq.cx/verichip.pl

[27] http://www.engadget.com/2008/03/19/rfid-credit-cards-easily-hacked-with-8-reader/

[28] http://www.youtube.com/watch?v=vmajlKJlT3U

[29] http://www.youtube.com/watch?v=NW3RGbQTLhE

[30] http://www.computerworld.com/s/article/9069558/How_they_hacked_it_The_MiFare_RFID_crack_ explained

[31] RFID: Cloning vs. Spoofing, Bert Moore, http://www.aimglobal.org/members/news/templates/ template.aspx?articleid=1564&zoneid=24

[32] http://www.thingmagic.com/rfid-security-issues

[33] http://www.rfidvirus.org/

[34] http://www.idstronghold.com/Secure-Sleeves-for-ID-Payment-Cards-IDSH1003-001-/productinfo/ IDSH1003-001/

[35] http://www.pacsafe.com/www/index.php?_room=3&_action=detail&id=150

[36] http://www.vagabondish.com/flipside-rfid-protected-wallet/

[37] Jerry Banks, David Hanny, *Manuel Pachano, Les Thompson, RFID Applied*, Wiley, 2007, pp.276.

[38] Garfinkel, Simon and Beth Rosenberg, *RFID Applications, Security, and Privacy,* Addison-Wesley, 2006, pp.297.

[39] http://www.gizmag.com/go/5865/

[40] Jerry Banks, David Hanny, *Manuel Pachano, Les Thompson, RFID Applied*, Wiley, 2007, pp.279

[41] Garfinkel, Simon and Beth Rosenberg, *RFID Applications, Security, and Privacy*, Addison-Wesley, 2006, pp.343.

[42] Garfinkel, Simon and Beth Rosenberg, *RFID Applications, Security, and Privacy*, Addison-Wesley, 2006, pp.342.

[43] Kyuhee An, Kiyeal Lee, and Mokdong Chung, "Design and Implementation of an RFID-based Enterprise Application Framework based on Abstract BP and Kerberos", *International Journal of Information Processing Systems*, Vol.2, No.3, December, 2006.

[44] Divyan M. Konidala, Daeyoung Kim, Chan Yeob Yeun and Byoungcheon Lee, "Security Framework for RFID-based Applications in Smart Home Environment", *Journal of Information Processing Systems,* Vol.7, No.1, March, 2011.

[45] Dae-Hee Seo and Im-Yeong Lee, "A Study on RFID System with Secure Service Availability for Ubiquitous Computing", *International Journal of Information Processing Systems,* Vol.1, No.1, 2005.

Amit Grover holds a Master of Science degree in Informatics (Cyber-Security) from the University of Nevada, Las Vegas and another M.S. degree in Computer and Information Science from East Tennessee State University along with a Bachelor's Degree in Mechanical Engineering.He has played an instrumental role in the development, implementation and commissioning of a variety of Defense related IT applicationsand has worked on interfacing Information Systems on board warships, submarines and UAVs (Unmanned Aerial Vehicles).

Hal Berghel, PhD, is currently Professor of Computer Science at the University of Nevada Las Vegas where he has previously served as Director of the School of Computer Science, Founding Director of the School of Informatics, and Associate Dean of Engineering. He also founded the Identity Theft and Financial Fraud Research and Operations Center and the Center for CyberSecurity Research. His most recent teaching and research responsibilities deal with digital security, computer and network forensics, and cyber warfare. He has contributed hundreds of articles to the professional literature, and has been the recipient of numerous grants in support of his research. He is a Fellow of both the Association for Computing Machinery and the Institute for Electrical and Electronics Engineers, and serves both associations as a Distinguished Visitor.