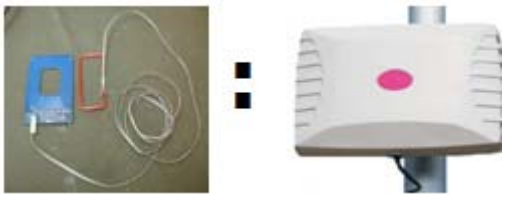

Figure 2: Antenna or Coil [16]

3.2Transceiver (with decoder)

The reader releases radio waves in ranges from one inch to 100 feet or more. The range depends on its output power and the radio frequency used [15]. When the RFID tag passes through the electromagnetic field it will then detect the reader's activation signal. [15] At this point the reader will decode the data programmed in the tag's circuit.[15] Finally, the data is passed to the host computer to be processed.

Figure 3: Transceiver with decoder [17,18]

3.3Transponder (RF Tag)

RFID tags are the heart of the RFID system because they store the information that describes the object being tracked.

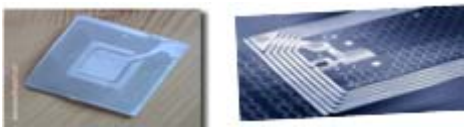

Figure 4: (Transponder) [19,20]

Tags are classified according to their abilities:
♦ Active
♦ Passive
♦ Read-Only
♦ Write-Once
♦ Read-Write

3.3.1Active Tags
Active Tag contains a battery that runs the microchip's circuitry. Active Tag is able to send a stronger signal to the reader due to battery. It allows a read range of about one hundred feet.

3.3.2 Passive Tags
Passive tags contain no batteries. Passive tags get power from a reader. Readers send electromagnetic waves that produce a current in the tag's antenna which then powers the microchip's circuits. [15]

3.3.3 Read-Only Tag
Read-only contain data such as tracking numbers. These tracking numbers are usually serialized and pre-written onto them by the tag manufacturer.[15] Read-only tags are usually the least expensive because information cannot be added onto them as they move through the supply chain.

3.3.4 Write-Once
Write-once tags allow a user to write information into the tag one time during the production. The information can be something like a batch or serial number.[15]

3.3.5 Read-Write
Full read-write tags allow for new data to be written to the tag as it is needed. These tags also allow for original data to be written over.

4. Difference between Bar Code and RFID

Table 1: Barcode Vs RFID

BAR CODE	RFID
Bar code reader requires a direct line of sight, using laser technology.	Reading is done automatically using RF waves.
Scan and read one tag at a time.	Scan and read multiple tags simultaneously.
Reading by bar code take much more time.	Reader can interrogate, or read tags much faster, appx. 23 tags per seconds.
Bar code don't have read /write memory.	RFID tag have read/write memory capability.
Human intervention is required to scan a barcode.	RFID tag can be detected hands off.
It should be visible on the product for scanning.	Tags can be concealed in any non metallic item.
The readability of bar code can be impaired by dirt, abrasion or packaging etc.	RFID tags are not affected by those condition.
Less read range in comparison to RFID.	RFID tag have a longer read range.
Technology is old and outdated. Less expensive. Ability hold limited data.	Scope for more advancement. More expensive. More data can be stored in an RFID tag. also facility to modifying it at later stage.

5. Communication Initiation

Tags and readers can initiate RF transactions in two general ways:

5.1 Reader Talks First (RTF)

In an RTF transaction, the reader broadcasts a signal that is received by tags in the reader's vicinity.[21] Those tags may then be commanded to respond to the reader and to continue transactions with the reader.

5.2 Tag Talks First (TTF)

In a TTF transaction, a tag communicates its presence to a reader when the tag is within the reader's RF field.[22] If the tag is passive, then it transmits as soon as it gets power from the reader's signal to do so. If the tag is active, then it transmits periodically as long as its power supply lasts. it is necessary to identify objects that pass by a reader, such as objects on a conveyer belt.[22]

Readers and tags in an RFID system typically operate using only RTF or only TTF transactions, not both types. Active tag TTF operation may be easier for an adversary to detect or intercept, because active tags send beaconing signals even when they are not in the presence of a reader. The adversary could eavesdrop on this communication without risking detection because in TTF transactions the adversary never has to send a signal to ascertain the tag's presence.

6. RFID and Information Security

There are a number of serious security concerns that should be examined thoroughly before executing any widespread RFID deployment. Some common threats include: [23]

6.1 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.

6.2 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[23]. RFID cloning is also referred to as a, relay attack. [24]

6.3 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 .Such an attack on a Generation 1 RFID tag was demonstrated at the 2006 RSA Security annual conference.

6.4 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.[24]

6.5 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[24].

6.6 Real ID Act

The Real ID Act will require some type of electronic national identification card, most likely issued through state motor- vehicle agencies as a standardized driver's license. While the act does not require that the "machine-readable" technology will be RFID, all solutions currently being considered use RFID technology. The Real ID Act of 2005 was passed into law in May 2005 under the Emergency Supplemental Appropriations Act for Defence, the Global War on Terror, and Tsunami Relief. The Real ID act will directly affect state government and court systems with the implementation deadline now being moved back to December 2009.

7. Countermeasures / Precautions

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

7.1 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. Once the kill command has been executed there is no way to revive the tag's usability at a later stage.

7.2 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.[24]

7.3 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 [24]. The use of crypto- graphic protocols in conjunction with Challenge-response authentication systems or using "rolling code" schemes, wherein the tag identifier information changes after each scan, are some other ways to make RFID communication more secure.[24] Care should be taken not to transmit secret tag information over non-secure communication channels .

7.4 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.

7.5 Other Security Threats

Other security threats, such as SQL injection, cross site scripting, buffer overflow,[25] and glue code attacks can be minimized or eliminated by using the following countermeasures:

1) Strong input validation.
2) Good software design.
3) Proper filtering rules on the perimeter firewall that controls access to the middleware and end-user applications
4) Disabling scripts on the backend system.
5) Auditing buffer bounds and thoroughly checking for boundary condition errors.
6) Accepting cookies only from trusted sites.
7) Limiting account privileges for users that don't require full administrator access to the software component.

8. RFID Advantages

1) Accurate knowledge of who has and where the document is in real time.
2) Alarms if the document is copied or is not visible to the system for a set period of time.
3) Alarms if the document is in a wrong location.
4) Alarm if the document is removed from an office or building.
5) Ability to read stacked documents by any reader.
6) Although RFID has been slow to take off due to manufacturing problems and the subsequent costs, those problems have been overcome to a degree and have given the technology the chance to be implemented.
7) RFID in the Smart World is providing automatic identification across the board, from a cashless society, tracking of people, animals to assets and inventory.[26]
8) Applications are now available for IOS, Android and Windows smart phones.
9) Automatic secure document return
10) Retail Automation - in apparel, electrical goods and white goods, with auto inventory control for quantity and location, and auto Point of Sale. Retail applications today do not need dedicated mobile computers, smart phones and tablets are being implemented reducing cost and increasing user comfort.[26]
11) Asset management internal and external with tracking and security. For high security areas the integration of CCTV provides asset ID, user ID, location ID with immediate access to video for assurance.
12) Defence, Law Enforcement and Fire Fighting – asset management for arms ammunition, ordinance and accessories communications, batons, breathing equipment etc [26]. Real time automatic asset management for user issue and deployment.

9. RFID Problems

RFID problems can be divided into several categories:

a) Technical problems with RFID.
b) Privacy and ethics problems with RFID.

9.1Technical problems with RFID

9.1.1 Problems with RFID Standards

RFID has been implemented in different ways by different manufacturers; global standards are still being worked on. It should be noted that some RFID devices are never meant to leave their network (as in the case of RFID tags used for inventory control within a company). This can cause problems for companies. Consumers may also have problems with RFID standards.[27]

9.1.2 RFID systems can be easily disrupted

RFID systems make use of the electromagnetic spectrum (like Wi-Fi networks or cell phones), they are relatively easy to jam using energy at the right frequency. Although this would only be an inconvenience for consumers in stores (longer waits at the checkout), it could be disastrous in other environments where RFID is increasingly used, like hospitals or in the military in the field.[27]

9.1.3 RFID Reader Collision

Reader collision occurs when the signals from two or more readers overlap. The tag is unable to respond to simultaneous queries. Systems must be carefully set up to avoid this problem;[27] many systems use an anti-collision protocol and it is also called a singulation protocol. Anti-collision protocols enable the tags to take turns in transmitting to a reader .Reader collision occurs in RFID systems when the coverage area of one RFID reader overlaps with that of another reader.[27] This causes two different problems:

9.1.3.1 Signal interference

The RF fields of two or more readers may overlap and interfere. This can be solved by having the readers programmed to read at fractionally different times. This technique (called time division multiple access - TDMA) can still result in the same tag being read twice

9.1.3.2 Multiple reads of the same tag

The problem here is that the same tag is read one time by each of the overlapping readers. The only solution is to program the RFID system to make sure that a given tag (with its unique ID number) is read only once in a session.

9.1.4 RFID Tag Collision

Tag collision occurs when many tags are present in a small area; but since the read time is very fast, it is easier for vendors to develop systems that ensure that tags respond one at a time.[27] Tag collision in RFID systems happens when multiple tags are energized by the RFID tag reader simultaneously, and reflect their respective signals back to the reader at the same time. This problem is often seen whenever a large volume of tags must be read together in the same RF field.[27] The reader is unable to differentiate these signals; tag collision confuses the reader. Different systems have been invented to isolate individual tags; the system used may vary by vendor. For example, when the reader recognizes that tag collision has taken place, it sends a special signal (a "gap pulse"). Upon receiving this signal, each tag consults a random number counter to determine the interval to wait before sending its data.[27] Since each tag gets a unique number interval.

9.2 Security, privacy and ethics problems with RFID

9.2.1 The contents of an RFID tag can be read after the item leaves the supply chain

An RFID tag cannot tell the difference between one reader and another. RFID scanners are very portable; RFID tags can be read from a distance, from a few inches to a few yards. This allows anyone to see the contents of your purse or pocket as you walk down the street. Some tags can be turned off when the item has left the supply chain.[27]

9.2.2 RFID tags are difficult to remove

RFID tags are difficult to for consumers to remove; some are very small (less than a half-millimetre square and as thin as a sheet of paper) - others may be hidden or embedded inside a product where consumers cannot see them. New technologies allow RFID tags to be "printed" right on a product and may not be removable at all .

9.2.3 RFID tags can be read without your knowledge

Since the tags can be read without being swiped or obviously scanned (as is the case with magnetic strips or barcodes), anyone with an RFID tag reader can read the tags embedded in your clothes and other consumer products without your knowledge. For example, you could be scanned before you enter the store, just to see what you are carrying.

9.2.4 RFID tags can be read a greater distances with a high-gain antenna

For various reasons, RFID reader/tag systems are designed so that distance between the tag and the reader is kept to a minimum [27]

9.2.5 RFID tags with unique serial numbers could be linked to an individual credit card number

At present, the Universal Product Code (UPC) implemented with barcodes allows each product sold in a store to have a unique number that identifies that product.

10. Conclusion

The use of RFID technology is increasing across a range of different industries, the associated security and privacy issues need to be carefully addressed. Some low cost passive and basic tags cannot execute standard cryptographic operations like encryption, strong pseudorandom number generation, and hashing. Some tags cost more than basic RFID tags and can perform symmetric-key cryptographic operations. Organisations wishing to use RFID technology need to therefore evaluate the cost and security implications as well as understand the limitations of different RFID technologies and solutions. Important aspect of RFID security that of user perception of security and privacy in RFID systems. As users cannot see RF emissions, they form their impressions based on physical cues and industry explanations. RFID will come to secure ever more varied forms of physical access and logical access.

References

[1] RFID-Based Students Attendance Management System Arulogun O. T., Olatunbosun, A., Fakolujo O. A., and Olaniyi, O. M.
[2] A Survey Paper on Radio Frequency IDentification (RFID) Trends Christoph Jechlitschek, christoph.jechlitschek@gmx.de
[3] http://www.uk-automation.co.uk/blog/radio-frequency-identification-for-home-automation/
[4] http://merlin360.co.uk/rfidoverview.html
[5] http://electronicsforu.com/electronicsforu/circuitarchives/view_article.asp?sno=1375&title%20=%20RFID+Technology+for+Building+Access+Control&id=12043&article_type=8&b_type=new
[6] Robin G. Qiu, " Rfid-Enabled Automation In Support Of Factory Integration," Robotics And Computer-Integrated Manufacturing, Volume 23, Issue 6, Dec. 2007, Pages 677-68.
[7] Sangkeun Yoo, Junseob Lee, Yongwoon Kim, And Hyungjun Kim, "An Integrated Mobile Rfid Service Architecture Between B2b And B2c Networks," 9th Ieee International Conference On Advanced Communication Technology, Volume 1, Feb. 2007, Pages 90–93.
[8] Pala, Zeydin And Inanc, Nihat, "Smart Parking Applications Using Rfid Technology", 1st Annual Rfid Eurasia, Sept. 2007, Pages 1–3.
[9] Min, Zhang, Li Wenfeng, Zhongyun Wang, Li Bin And Xia Ran, "A Rfid-Based Material Tracking Information System", Ieee International Conference On Automation And Logistics, Aug. 2007, Pages 2922–2926.
[10] Karen Coyle, "Management Of Rfid In Libraries," The Journal Of Academic Librarianship, Volume 31, Issue 5, Sep. 2005, Pages 486-489.
[11] Andrea Cangialosi, Joseph E. Monaly, And Jr., Samuel C. Yang, "Leveraging Rfid In Hospitals: Patient Life Cycle And Mobility Perspectives", Ieee Communications Magazine, Volume 45, Issue 9, Sep. 2007.
[12] George Adams, "Pharmaceutical Manufacturing: Rfid – Reducing Errors And Effort," Filtration & Separation, Volume 44, Issue 6, July- August 2007, Pages 17-19.
[13] May Tajima, "Strategic Value Of Rfid In Supply Chain Management," Journal Of Purchasing And Supply Management, Volume 13, Issue 4, December 2007, Pages 261-273.
[14] A. Sagahyroon, A. R. Al-Ali, F. Sajwani, A. Mehery And I. Shahin "Assessing The Feasibility Of Using Rfid Technology In Airports", Proceedings Of The Rfid Eurasia 2007 Conference, Istanbul, Sept. 2007.
[15] www.slideshare.net/PeterSam67/presentation-9-rfid
[16] gaorfid2.en.supplierlist.com/
[17] www.tagsense.com/ingles/products/product_mw.html
[18] www.intermec.com/services/...services/software_consulting/
[19] http://www.rolitec.ch/kompetenzen/rfid/.
[20] https://www.google.com/search?tbm=isch&oq=&gs_l=&q=transponder%20rfid
[21] http://itlaw.wikia.com/wiki/Reader_Talks_First
[22] http://itlaw.wikia.com/wiki/Tag_Talks_First
[23] Journal of Information Processing Systems, Vol.7, No.4, December 2011 http://dx.doi.org/10.3745/JIPS.2011.7.4.561 561 A Survey of RFID Deployment and Security Issues Amit Grover* and Hal Berghel*
[24] December 12, 2011 A Survey of RFID Deployment and Security Issues Amit Grover, Hal Berghel Identity Theft and Financial Fraud Research and Operations Center (www.itffroc.org)
[25] A Survey of RFID Deployment and Security Issues Amit Grover* and Hal Berghel*
[26] www.aiti.gov.bn/downloadables/.../RFID%20Presentation.ppt
[27] http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20
[28] www.infosec.gov.hk/english/technical/files/rfid.pdf
[29] Rfid Journal The World's Rfid Authority. April 2, 2008. Http://Www.Rfidjournal.Com/
[30] What Is Rfid? Online. 2 April 2008. Http://Www.Technovelgy.Com/Ct/Technology Article.Asp?Artnum=1