Security Risk Analysis of RFID Technology

Benjamin Khoo1, Peter Harris2, Stephen Hartman3

1, 2, 3, 4 School of Management, New York Institute of Technology
P.O. Box 8000, Old Westbury, NY 11568, U.S.A.
1 kkhoo@nyit.edu, 2 pharris@nyit.edu, 3 shartman@nyit.edu

Abstract—Most of the sources of security and privacy issues in RFID technology arise from the violation of the air interface between a tag and its reader. This paper will approach the security risk analysis process from the perspective of the RFID tag life cycle, identify the tag usage processes, identify the associated vulnerability and threat to the confidentiality, integrity and availability of the information assets and its implications for privacy, and then mitigate the risks.

I. INTRODUCTION

Business enterprises and even governments have looked upon the emerging Radio Frequency Identification (RFID) technology as a possible silver bullet in the application of pervasive and ubiquitous computing [1] [2]. RFID is a wireless Automatic Identification and Data Capture (AIDC) technology that operates without human intervention. Manufacturers and distributors look to RFID as a saviour in handling the impending logistical overload [3] [4] [5]. In fact, the retail industry (with such major retailers like Walmart and Tesco in the US, and Britain’s Mark & Spencer and Germany’s Metro Group) is the initial driver of RFID adoption. Recently with the push by Wal-Mart and the US Department of Defense to use RFID tags in their supply chain, RFID has re-gained the limelight. Recently RFID market watchers have predicted a market growth of 20.7% from 2008 to 2010 (according to reports published by http://www.researchandmarkets.com).

Today RFID technology is used in many applications: manufacturing, healthcare, transport and logistics, defence and other industries. Soon RFID technology will be universal for tracking items, products, animals, shipments and even humans. Associated with the integration of RFID technology in business and in the day-to-day life of consumers are various security and privacy concerns [6] [7] [8] [9] [10].

The prominence that businesses and governments have placed on RFID technology in electronic article surveillance, cashless payment from credit cards (Smart cards) and public transportation tickets (Mifare) to consumer devices (such as EZpass and Speedpass), healthcare (tracking items, drugs and patients) and e-government (such as e-driver’s license and ePassport) [11] necessitate a closer examination of the security and privacy risks associated with this technology. The potential to reduce purchase anonymity, embedded tags in products that can reveal sensitive information, violations of location privacy with no-contact, non-line-of-sight through non-conducting material such as cardboard or paper, fast read rate at a distance of up to a few meters and invisible identification which can be done indiscriminately has raised privacy concerns.

There have been a number of published papers that surveyed RFID security and privacy issues. This paper will take a different approach while extending this body of published literature by conducting a security risk analysis based on the RFID tag life cycle then discuss how these risks can be mitigated.

This paper is divided into 5 sections. Section 1 is the introduction; the security risk analysis will begin with an overview of the RFID mechanism in Section 2. Section 3 will review current RFID security and privacy issues and proposed solutions. Section 4 will conduct the security risk analysis and discuss the various issues of RFID security and privacy that includes mitigating the associated risks based on accepted practices or guidelines (such as NIST800-98) [12]. This paper will conclude in Section 5 by analysing current efforts and future roadmaps to resolve these outstanding issues.

II. RFID MECHANISM

A basic RFID infrastructure consists of 3 major components: (1) tags, (2) a reader and its antenna, and (3) middleware application software. RFID tags are transponders that contain a chip and an antenna. The antenna receives radio signals from the readers while the chip is used to respond to the signals and store information. Current tags are small enough to be embedded into physical objects for identification and tracking. Tags can be read only, write once/read many times or read/write capable [13]. RFID readers are electronic interrogators that emit and receive radio signals through their antennas. They capture data stored and may overwrite the data on the tags. They are also responsible for the information flow between the tags and the host system via the middleware [14]. There are 2 main types of RFID tags – active and passive tags. The active tag requires a power source which makes it more costly and larger. It is not practical in the retail industry. It operates at 455 MHz, 2.45 GHz or 5.8 GHz and has read ranges from 20 to 100 meters. The passive tag, on the other hand, is cheap, small and has an infinite shelf life. These qualities make it practical for the retail industry. It operates at...
128 KHz, 13.6 MHz, 915 MHz or 2.45 GHz and has read ranges from a few inches to 30 feet. There are 2 fundamental design approaches used in passive tags – the near field which uses the magnetic induction and far field which uses electromagnetic wave capture [15] [16]. Figure 1 show the near field mechanism that is used in passive RFID tags.

Figure 1. Near-field power/communication mechanism for RFID tags operating at greater than 100 MHz (from Roy Want, “An Introduction to RFID Technology,” IEEE Pervasive Computing, vol.5, no. 1, pp. 25-33, January-March 2006).

Figure 2 show the far field mechanism that is used in passive RFID tags.

Figure 2. Far-field power/communication mechanism for RFID tags operating at greater than 100 MHz (from Roy Want, “An Introduction to RFID Technology,” IEEE Pervasive Computing, vol.5, no. 1, pp. 25-33, January-March 2006).

The passive Ultra High Frequency (UHF) RFID technology operating from 860 MHz to 960 MHz offers the best read range read rate performance, readability through a wide range of materials, and at a very cost-effective manner; as a result, it is the most prevalent technology across all industries. RFID devices are classified into categories, for example Class 1 Generation 1 devices do not have security features while the Class 1 Generation 2 devices have security features like authentication and encryption. For a more complete classification, see the paper by Phillips, et al [17]. The communication between readers and tags at the air interface (EPCglobal Class-1 Generation-2 protocol) and the way the data are processed at various stages are defined by the EPCglobal and International Standard Organization (ISO) standards. This is illustrated in Figure 3.

RFID tags have advantages over bar codes in that:

1. It does not require line-of-sight access.
2. The read range is larger.
3. Tag readers can communicate with multiple tags simultaneously.
4. The tags can store information [18].
5. The tags can be read through non-conducting materials such as cardboard and paper.
6. The tags can be read at a much faster rate [19].

As a result of the benefits of RFID, it is currently used and will be used in more applications in the future. RFID technology is now being embedded in various business processes such as operations management where it is used in asset management, tracking components, work-in-progress and manufactured products; logistics where items are tracked from the inventory or store through the shipment to the retailer; customer service where items are traced to customers to validate defective items that are returned or that are for repairs. RFID information systems typically consists of the tag identification (with verification) and wireless flow of data from the tag to the reader through application middleware (SAVANT) to the enterprise information system and may be transmitted via inter-enterprise systems to an external information system. The pervasiveness of RFID technology has given rise to a number of serious security and privacy concerns. Associated with these concerns, Garfinkel proposed a consumer’s bill of rights (http://www.technologyreview.com, October 2002). See Figure 4.
The RFID Bill of Rights addresses the most obvious RFID abuses

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

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first class RFID alternatives: consumers should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag’s "kill" feature.
4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where and why an RFID tag is being read.

Figure 4. The Consumer’s RFID Bill of Rights as proposed by S. Garfinkel.

The subsequent EPCglobal guidelines for the use of RFID (http://www.epcglobalinc.org/public policy/public policy guidelines.html) were developed to alleviate some of these concerns but did not go far enough.

III. LITERATURE REVIEW

A number of security researchers have published papers surveying the latest development in this area [9] [19] [20]. Most of the sources of security and privacy issues arise from the violation of the air interface between a tag and its reader. EPCglobal created the Object Naming Service (ONS) as a public lookup system for EPC tags. Currently, this is localized but in the near future an RFID infrastructure proposed by Verisign called EPC Discovery Service will create a unified view of EPC tags across organizations.

References [9] and [21] examine various approaches to protect privacy and ensure integrity in RFID technology. It describe a number of security researchers have published papers surveying the latest development in this area [9] [19] [20]. Most of the sources of security and privacy issues arise from the violation of the air interface between a tag and its reader. EPCglobal created the Object Naming Service (ONS) as a public lookup system for EPC tags. Currently, this is localized but in the near future an RFID infrastructure proposed by Verisign called EPC Discovery Service will create a unified view of EPC tags across organizations.

Reference [19] presented a brief summary of relevant standards for RFID technology, provided a technical overview of the state of the art and analysed the proposed solutions. It describes the RFID Interface including the various modes of communication between the reader and the tag. The relevant standards are then identified for the physical and link layers that covers the air interface, anti-collision protocol, communication protocol and security features. Contactless integrated circuit cards are defined by ISO7810 where ISO10536 are for cards that operate at < 1 centimetre, ISO14443 are for cards that operate at ~ 10 centimetres and have a microprocessor, and ISO 15693 are for cards that operate at > 1 meter and do not have microprocessor. ISO11784, ISO11785 and ISO14223 define the standards for tagging animals in the 135 KHz range. The communication protocol ISO14223 is similar to that of ISO18000-2. ISO18000 defines the air interface, collision detection mechanism, and the communication protocol. ISO18000-1 describes the reference architecture while parts 2 to 7 specify the system for the different frequency bands. The Electronic Product Code (EPC) network is made up of five elements: the EPC is a 96-bit field made up of 4 fields – version number, domains, object classes and individual instances, an identification system which is made up of RFID tags and readers using protocols similar to ISO15693 and ISO18000-3 for Class 1 tags in the HF band, the Savant Middleware which provide the services between the readers and the back-end system, and the ONS which provides a service similar to the Domain Name Service (DNS). There are two main issues – privacy and location privacy; other issues include physical attacks, Denial of Service (DoS) like signal jamming of RF channels, counterfeiting where the tag is manipulated to change the identity of an item, spoofing where an attacker successfully impersonate a tag (also called man-in-the-middle attack), eavesdropping where attackers are able to intercept and read messages and traffic analysis where messages are intercepted and analysed to extract patterns from the communication. Solutions that had been proposed includes: the Kill command, the Faraday Cage Approach where the tag is isolated from any electromagnetic waves, the active jamming approach where the RF channels are jammed with corresponding public key. It also discusses the proxying approach where a privacy-enforcing device is used. The Watchdog tag has a device that detects the transmission of readers in close proximity and captures the information of these readers such as the identifiers. The RFID Guardian searches for the tags around and managing access to it by means of authenticating the readers trying to access the tags. A blocker tag is able to stimulate the full spectrum of possible tags; this makes it difficult for a reader to know which tag it really is. The blocker tag can be programmed to generate only a given subset of possible identifiers, this way, security zones can be implemented for different blocker tags. However, the presence of malicious blocker tags can interfere in the operation of the RFID protocols, for example, at check-out counters.

References

[19] Reference [19] presented a brief summary of relevant standards for RFID technology, provided a technical overview of the state of the art and analysed the proposed solutions. It describes the RFID Interface including the various modes of communication between the reader and the tag. The relevant standards are then identified for the physical and link layers that covers the air interface, anti-collision protocol, communication protocol and security features. Contactless integrated circuit cards are defined by ISO7810 where ISO10536 are for cards that operate at < 1 centimetre, ISO14443 are for cards that operate at ~ 10 centimetres and have a microprocessor, and ISO 15693 are for cards that operate at > 1 meter and do not have microprocessor. ISO11784, ISO11785 and ISO14223 define the standards for tagging animals in the 135 KHz range. The communication protocol ISO14223 is similar to that of ISO18000-2. ISO18000 defines the air interface, collision detection mechanism, and the communication protocol. ISO18000-1 describes the reference architecture while parts 2 to 7 specify the system for the different frequency bands. The Electronic Product Code (EPC) network is made up of five elements: the EPC is a 96-bit field made up of 4 fields – version number, domains, object classes and individual instances, an identification system which is made up of RFID tags and readers using protocols similar to ISO15693 and ISO18000-3 for Class 1 tags in the HF band, the Savant Middleware which provide the services between the readers and the back-end system, and the ONS which provides a service similar to the Domain Name Service (DNS). There are two main issues – privacy and location privacy; other issues include physical attacks, Denial of Service (DoS) like signal jamming of RF channels, counterfeiting where the tag is manipulated to change the identity of an item, spoofing where an attacker successfully impersonate a tag (also called man-in-the-middle attack), eavesdropping where attackers are able to intercept and read messages and traffic analysis where messages are intercepted and analysed to extract patterns from the communication. Solutions that had been proposed includes: the Kill command, the Faraday Cage Approach where the tag is isolated from any electromagnetic waves, the active jamming approach where the RF channels are jammed with corresponding public key. It also discusses the proxying approach where a privacy-enforcing device is used. The Watchdog tag has a device that detects the transmission of readers in close proximity and captures the information of these readers such as the identifiers. The RFID Guardian searches for the tags around and managing access to it by means of authenticating the readers trying to access the tags. A blocker tag is able to stimulate the full spectrum of possible tags; this makes it difficult for a reader to know which tag it really is. The blocker tag can be programmed to generate only a given subset of possible identifiers, this way, security zones can be implemented for different blocker tags. However, the presence of malicious blocker tags can interfere in the operation of the RFID protocols, for example, at check-out counters.
radio signals to isolate the tag from any electromagnetic waves, the blocker tag, the RFID Bill of Rights which is offered to companies to adopt and the use of cryptography, hash functions and authentication schemes to secure the data.

Reference [20] takes a slightly different approach by conducting a technical assessment of the RFID communication link layers. The communication link can be divided into 3 layers as illustrated in Figure 5.

![Figure 5. Layers of an RFID System](image)

The Application Layer handles user-defined information, for example identifiers. The Communication Layer defines how reader and tag communicate. The Physical Layer specifies the physical requirements such as frequency, data encoding, modulation and so on. Techniques used in the physical layer includes: killing the tag and reducing the read range by reducing the size of its antenna. Techniques used in the communication layer include: singulation protection to guarantee the communication between the reader and many tags and the Noisy Tag Protocol (NTP) [22] where another tag nearby is used to generate random “noise” at the same time that a legitimate tag is communicating with the reader. Techniques used in the Application layer include: the Message Authentication Codes (MAC) where the identifier on the RFID µ-chip is encrypted (the identifier is known only to the manufacturer and clients), the Physical Unclonable Functions (PUF) circuit acts as a hardware decoded secret key for the RFID tag, the Distance Bounding Protocol to ensure the proximity of a device, Trusted Computing where the reader design has to be changed to include additional security modules, Re-encryption of Tags[9] and Pseudonym Protocol[9].

III. SECURITY RISK ANALYSIS

This paper will approach the security risk analysis process from the perspective of the RFID tag life cycle, identify the tag usage processes, identify the associated vulnerability and threat to the confidentiality, integrity and availability of the information assets and its implications for privacy, and then mitigate the risks based on accepted practices (for example NIST800-98).

The RFID infrastructure is derived from the EPC Network standard (http://www.epccglobalinc.org/home). Reference [27] succinctly describes it as follows:

“It is composed of five components: (i) the EPC code, which starts as a 64-bit to 128-bit identifier. Once it is incorporated into an RFID chip (also called an EPC tag) and attached to a physical object, product or item, it can provide information such as the manufacturer, the product category and size, the date when the product was made, the expiration date, the final destination, etc. (ii) The RFID reader identifies any EPC tag within its interrogating field, reads the EPC tag and forwards information to the SAVANT. (iii) The SAVANT is the middleware system located between readers and the application systems (AS). Based on configured business rules, it is responsible for data filtering and aggregation and interacts with the EPC Information Service (EPC-IS) and the local Object Name Service (ONS). (iv) The EPC-IS is the gateway between any requester of information and the firmware’s AS and internal databases. (v) The local ONS is an authoritative directory of information available in order to describe all EPC tags used in a supply chain.”

RFID devices are used for tracking and transfer of data at different stages or locations to different “owners” in an open system for later processing. They are different from the traditional assets in a risk analysis scenario due to the fact that they are “carriers” of the information assets that are useful either because the information is processed directly or indirectly as in the case of tracking. For this reason, RFID have to support 2 important features: transfer of ownership and multiple authorisations.

The RFID tag life cycle approach is used because unlike other devices the tag data can change over time; there are different “owners” and variations in the tag usage depending on the phases yet the commonality is the air interface where most of the vulnerabilities reside.

Reference [23] presented a typical RFID Tag Life Cycle (RTLC) as consisting of 4 phases:

1. Supply Chain Management, where the tag delivers a unique identifier called electronic product code (ePC) (http://www.epcglobalus.org/dnn_epcus/Standards/EPCGlobal Standards/tabid/185/Default.aspx) that is used for tracking items through the final manufacture, inventory, storage, distribution, location and transfer of “ownership” processes.

2. In-Store and Point-of-Sales, where the tags may be used for verification and prevent counterfeit, track the product and also monitor consumer interaction with the product and if a credit card is used for purchase, the product can be associated with the consumer for purchase services. (After the purchase, the tag can be removed or “killed” but this will prevent post-purchase services such as access to product support, warranty services, and other services in phases 3 and 4.)

3. Customer Control and after Sales Services, (if the tag is live) the tag can be used as an enabling technology for intelligent applications (for example, an intelligent refrigerator
with a reader can flash a message if the date on tagged food items have expired), after sales service where the ePC can be used for verification.

4. Recycling and Waste Management where the ePC can be used to sort recyclable materials and identify manufacturers of items that contain hazardous materials.

The RTLC applies to most current commercial usage of RFID technology – the production of goods for sale. Even though other RFID applications (like eHealth, ePassports, Mifare cards, Smartcards, EZPass, SpeedPass, etc) tags have a different tag life cycle yet the threat model derived from the communication mechanism analysis of the tag life cycle in phases 2 and 3 are also applicable here.

It is important to have an overview of the RTLC processes and the entities that interact with the tag [23] to conduct a security risk analysis. The tag will be embedded on the product by the manufacturer. The distributors (storage and transfer) that transport the products to the retailers will rely on the tags for logistical management. The retailers will use the tags to verify the product and prevent counterfeit, and for tracking and managing inventory, and can monitor customer interaction with the product (through the embedded tag) and the product can be associated with the consumer for purchase services at the point-of-sales counter. The after sales service providers will use the tag for verification and warranty services, and tracking product history. The infrastructure service providers will link the ePC to the manufacturer or retailer databases where detailed information is stored. The consumer who buys the product may benefit from intelligent interaction with the product (through the embedded tag) and the product can be associated with the consumer for purchase services at the point-of-sales counter. The after sales service providers will use the tag for verification and warranty services, and tracking product history. The infrastructure service providers will link the ePC to the manufacturer or retailer databases where detailed information is stored. The consumer who buys the product may benefit from intelligent applications enabled by the embedded RFID tag. The waste manager will use the tags to sort the waste materials and levy charges to the manufacturers (derived from the ePC) based on the type (hazardous, recyclable or garbage) and the volume of materials.

The NIST800-98 [12] guideline categorises RFID risks into 4 categories:

1. Business Process (BP) Risk - where a direct attack on the RFID system components will undermine the business processes it was designed to enable.
2. Business Intelligence (BI) Risk – where a competitor could gain unauthorised access to the RFID-generated information and use it against the company.
3. Privacy (P) Risk – where personal or private information in an RFID system is used for purposes against privacy regulations or laws. A person in possession of a RFID tag can also risk being tracked.
4. Externality (EX) Risk – where the RFID system could pose a threat to non-RFID networks, systems, assets or people. There are 2 types: Hazards of Electro-magnetic Radiation and Computer Network Attacks.

The NIST800-98 guidelines list various factors that will influence the risk level. The risk level is directly dependent on the impact to the business and the probability of occurrence. There are standard matrices of 3x3 (high, medium or low) or 5x5 (very high, high, medium, low or very low) tables to evaluate the risk level based on the probability versus impact. The NIST800-98 document also provides risk mitigation guidelines based only on the risk category. Unfortunately, this document did not conduct any threat analysis; neither was there a threat list.

Threats to RFID systems typically take place at the air interface. Reference [24] discussed a number of the major threats. Eavesdropping happens when attackers secretly monitor the communication between the tag and the reader. This can be mitigated by encrypting the data, shielding the tag or limit the tag-reader distance, however attacker can use a non-standard reader to extend the distance. Relay attacks is done using a fake tag to communicate with the real reader and a fake reader to communicate with the real tag. The information obtained by the fake reader is passed to the fake tag which then communicates with the real reader. This can be mitigated by using short range tags, by shielding the tag or implementing the distance bounding protocol. Rogue readers can intercept and read tag information. Reader authentication can be used to allow only authorised readers to read the tag information. When attackers make a duplicate tag based on a real tag after gaining unauthorised access to the real tag is called tag cloning. The duplicate tag can be used to gain unauthorised access to confidential information or make an electronic transaction. Tag cloning can be mitigated using tag authentication. Tags can also be used to track people who have in their possession a RFID tag by rogue readers and eavesdropping devices. This can be mitigated by using low range tags or shielding tags, authenticating the readers or disabling the tags. Replay attack happens when attackers eavesdrop on the communication between a tag and reader, and then use a cloned tag to repeat the authentication sequences. This can be mitigated using the same countermeasures for eavesdropping and tag cloning. Physical tag destruction is when a tag is physically destroyed like microwaving in an oven or hitting it with a hammer. Blocking is when attackers use a blocker tag to stimulate the existence of many tags and cause a denial of service as the reader tries to interrogate these non-existence tags. Jamming means paralysing the communication system by generating radio noise at the same frequency as that of the system. Blocking and jamming devices can be detected early and localize so that appropriate actions is taken.

The RFID Tag Life Cycle, the typical business processes and tag usage in each phase, the interacting entities, the associated threat/vulnerability and Risk Mitigation can be summarized as illustrated in Table 1.
<table>
<thead>
<tr>
<th>Business Processes</th>
<th>Interacting Entities</th>
<th>Threat/Vulnerability</th>
<th>Risk Category</th>
<th>Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supply Chain Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Manufacturing Process (tagging)</td>
<td>Manufacturer (within company premises)</td>
<td>Eavesdropping</td>
<td>BI</td>
<td>Encrypting the data, shielding the tag or limit the tag-reader distance</td>
</tr>
<tr>
<td>Product Movement/Transfer</td>
<td></td>
<td>Tag Cloning</td>
<td>BP</td>
<td>Tag authentication</td>
</tr>
<tr>
<td>Inventory Storage</td>
<td></td>
<td>Replay Attack</td>
<td>EX</td>
<td>Encrypting the data, shielding the tag or limit the tag-reader distance, tag authentication</td>
</tr>
<tr>
<td>Inventory Location</td>
<td></td>
<td>Rogue Reading</td>
<td>BI</td>
<td>Reader authentication</td>
</tr>
<tr>
<td><strong>Product Distribution/Transport</strong></td>
<td>Distributors (outside company premises)</td>
<td>Relay Attack</td>
<td>BP</td>
<td>Using short range tags, shielding the tag or implementing the distance bounding protocol</td>
</tr>
<tr>
<td>Warehouse/Product Storage</td>
<td></td>
<td>Tracking</td>
<td>BI</td>
<td>Low range tags or shielding tags, authenticating the readers or disabling the tags.</td>
</tr>
<tr>
<td>Warehouse/Product Location</td>
<td></td>
<td>Blocking, Jamming</td>
<td>BP</td>
<td>Detect early and localize, take appropriate action.</td>
</tr>
<tr>
<td><strong>Ownership Transfer</strong></td>
<td>Distributors/ Retailers</td>
<td>Eavesdropping</td>
<td>BI</td>
<td>Encrypting the data, shielding the tag or limit the tag-reader distance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tag Cloning</td>
<td>BP</td>
<td>Tag authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replay Attack</td>
<td>EX</td>
<td>Encrypting the data, shielding the tag or limit the tag-reader distance, tag authentication</td>
</tr>
<tr>
<td><strong>In-Store and Point-of-Sales</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Verification</td>
<td>Retailer</td>
<td>Eavesdropping</td>
<td>BI</td>
<td>Encrypting the data, shielding the tag or limit the tag-reader distance</td>
</tr>
<tr>
<td>Inventory Store Storage</td>
<td></td>
<td>Jamming and Blocking</td>
<td>BP</td>
<td>Detect early and localize, take appropriate action.</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td>Tracking</td>
<td>P</td>
<td>Low range tags or shielding tags, authenticating the readers or disabling the tags.</td>
</tr>
<tr>
<td>Display Shelf Item Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer-Product Interaction</td>
<td>Consumer</td>
<td>Blocking</td>
<td>BP</td>
<td>Detect early and localize, take appropriate action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tracking</td>
<td>P</td>
<td>Low range tags or shielding tags, authenticating the readers or disabling the tags.</td>
</tr>
<tr>
<td><strong>Customer Control and after Sales Services</strong></td>
<td>After Sales Service Provider/ Retailer</td>
<td>Tag Destruction</td>
<td>BP</td>
<td>Use protective material</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tracking</td>
<td>EX</td>
<td>Low range tags or shielding tags, authenticating the readers or disabling the tags.</td>
</tr>
<tr>
<td><strong>Recycling and Waste Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sort Waste Material</td>
<td>Waste Manager</td>
<td>Tag Destruction</td>
<td></td>
<td>Use protective material</td>
</tr>
<tr>
<td>Identify Manufacturer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
As RFID technology continues to evolve, more features will be added to the system. At the same time, more vulnerabilities/threats will be discovered; however this will drive the RFID researchers to come up with enhanced designs to mitigate the security and privacy risks.

IV. CONCLUSION

The current Class 1, Gen 2 tags have security features added and have enhanced the security of the RFID system. The wide range of applications of RFID technology with the different tag types also implies that there will be a wide range of design, security and privacy issues. Some applications are better suited for RFID technology whereas others are not. It is important to know the difference. RFID technology is great for tracking and keeping stock of items or animals but if this is applied to humans there have to be laws and regulations to govern its operation and strong enforcement or audit to ensure compliance as it can be so easily abused. Businesses and consumers are still concerned with the no-contact, non-line-of-sight operation of this invisible technology. It is important to eliminate people’s fears and concern before the RFID technology is wholly accepted. Thus, for RFID technology to meet the pervasive and ubiquitous computing expectations, issues with the technological and social problems will have to be resolved. The technology problems have to do with finding solutions or schemes that will bring benefits and yet protect the consumer’s security and privacy. The social problems have to do with educating the masses about the potential benefits with a guaranteed level of security and privacy.

REFERENCES