RFID Usage Issues in the Supply Chain

Benjamin Khoo
School of Management, New York Institute of Technology
P.O. Box 8000, Old Westbury, NY 11568, U.S.A.
kkhoo@nyit.edu

Abstract—Soon RFID technology will be universal for tracking items, products, animals, shipments and even humans. The pervasiveness of RFID technology has given rise to a number of serious issues including security and privacy concerns. This paper will discuss current RFID usage issues and conduct a threat analysis of the RFID usage in the SCM processes then identify issues/risks and discuss how these issues can be resolved or risks can be mitigated.

I. INTRODUCTION

The advent and mass adoption of the Internet have caused a paradigm shift in the 21st century; not only in our everyday lives but also in the way business is conducted. Commerce and especially online commerce or eCommerce (electronic-Commerce) has exploded! The new online business paradigm is the “Customer is King” whereas the traditional business is based on the “Product is King” [1]. Today, there is more business conducted online than traditional face-to-face or pen-paper modes of doing business. Entrepreneurs, sensing the potential for profit taking, have increased their stakes in eCommerce by increasing their equity market capital by billions since the late 1990s. The resulting explosion of sales of consumer products has overloaded the supply, manufacturing and logistical resources of most businesses, depending on the type of products that are sold, this can be a nightmare, if not properly managed.

A supply chain is a network of value adding cells. There are two important aspects of the supply chain. Supply chain co-ordination incorporates the information links and decisions that determine the flow of materials and services in order to match supply with demand throughout the supply chain. Supply chain structure determines the location, capacity, connectivity and mission of the cells in the supply chain network. When the “Customer is King,” the market power shifts to the customer – customer centric solutions. Products and services will be customized. The supply chain (SC) provides the time, space, availability and logistics system to support the product development and manufacturing process, and the distribution to the customer. The SC processes include sourcing, procurement, conversion and logistics activities involving coordination and collaboration with partners, suppliers, intermediaries, third-party providers and customers. A good supply chain management (SCM) process will match the supply to the product of the demand and deliver to the customer in the fastest time at lowest costs. There are four critical success factors that enable the SCM: information of all real-time SC transactions, material flow of direct and just-in-time shipments, products with reduced economies of scale in production and decisions based on real-time reaction to contingencies [1]. Real-time tracking of items in the SC is crucial to the success of SCM.

Radio Frequency Identification (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 logistical overload [2] [3] [4]. RFID market watchers have predicted a market growth of 20.7% from 2008 to 2010 (http://www.researchandmarkets.com). In the near future, RFID technology will be universal for tracking items, products, animals, shipments and even humans. The pervasiveness of RFID technology has given rise to a number of serious security and privacy concerns.

There have been a number of published papers that discussed SCM frameworks [5][6][7] and others that surveyed RFID security and privacy issues [8][9][10][11][12]. This paper will take a different approach while extending this body of published literature by conducting a threat analysis of the RFID usage in the SCM processes then identify issues/risks and discuss how these issues can be resolved or risks can be mitigated.

This paper is divided into 5 sections. Section 1 is the introduction. Section 2 provides a survey of RFID usage in the SC. Section 3 will discuss current RFID usage issues and some possible solutions. Section 4 will conduct a threat analysis of RFID usage in SC processes and includes mitigating the associated risks based on accepted practices or guidelines (such as NIST800-98) [13] and ISO27001/2 (available for purchase at http://www.standards-online.net/InformationSecurityStandard.htm). This paper will conclude in Section 5 by analysing current efforts and future roadmaps to resolve these outstanding issues.

II. SURVEY OF RFID USAGE IN THE SC

The passive RFID tag is cheap, small and has an infinite shelf life. These qualities make it practical for the retail industry. RFID technology plays an important and very adaptable role in supply chain management. RFID usage in SCM will reduce the “bullwhip effect.” The movement and tracking of goods through the manufacturing and supply chain process is a complex procedure that presents
challenging management issues. RFID can remove blind spots from inventory and supply chain operations because it can be read through packaging, without concern to orientation, without direct line of sight between object and reader and can withstand exposure to dirt, heat, moisture and contaminants that make bar codes unusable. Manufacturers can improve visibility and confidence in their inventory and in so doing enable overall inventory levels, labor costs and safety stocks to be reduced by using the highly accurate, real-time and unattended monitoring capability of RFID to track raw materials, work-in-process and finished goods inventory [14].

Using RFID, inventory can be updated in real time without product movement, scanning, or human involvement. Fully automated systems allow inventory status to be determined and shipping and receiving documents can be generated automatically. The system could also trigger automatic orders for products that are low in inventory. RFID enables a level of logistics management way ahead of previous supply chain technologies, allowing managers to save money by addressing inefficiencies they may not have known existed. RFID will fundamentally transform the way information about products, equipment, animals and even people is gathered and analyzed in real time, providing new business opportunities. Traditional supply chain models are rife with waste. That is why inventory reductions and cost savings are still the number one Return on Investment (ROI) objective of supply chain initiatives [15].

A key advantage of RFID tags is the ability to provide visibility of the entire supply chain-monitoring inventory, transit times and locations, material content and quality. An organization has limited ability to plan and react to changes in its supply chain if it does not have visibility of the processes. Thus, providing a clear, unobstructed view of operations up and down a supply chain is critical for success. Increased visibility results in greater access to information about inventory, orders, shipments and invoices whether in a single-enterprise or a multi-enterprise supply chain. Globalization, outsourcing and compressed product lifecycles, as well as the shifting competitive dynamic from enterprise to supply chain, has created a need for increased accountability. Companies need a view into fragmented business processes, and they need a way to manage numerous disparate sources of information [16]. Better visibility leads to better responsiveness in the supply chain. This is achieved by optimizing channel and customer demand responses based on historical and real-time data analysis. RFID enables this data to be collected in real time while having lower operator cost. This real time operational data enables organizations to respond ahead of events affecting the supply chain. Company supply chains are thereby enabled to respond synchronously to changes in demand [7][17].

Various types of tags serve different environmental conditions. For example, tags suited to cardboard cases containing plastic items may not be ideal for wooden pallets, metal containers or glass. Tags can be as small as a grain of rice, as large as a brick, or thin and flexible enough to be embedded within an adhesive label. Paper-thin labels are referred to as "smart labels," and they usually serve single-use applications, such as case and pallet identification. Printer/encoders produce smart labels on demand, encoding the tag while printing text and/or a bar code on the outer label. Smart labels will satisfy most RFID compliance tagging requirements for cases and pallets [4].

There are several types of readers that can be incorporated into supply chain operations, portable readers integrated with handhelds, readers mounted on vehicles/forklifts, and fixed readers on dock doors and portals. A very useful adaptation is installing RFID readers on forklifts. This enables fewer readers to cover a facility. Additionally, their portability enables them to go wherever the demand is.

RFID systems can also function simultaneously with wireless networks, and are often integrated with wireless LANs to exchange data with host computer systems—Wi-Fi LANs do not cause interference for RFID systems [18][19].

One of the main benefits of using RFID in the supply chain for inventory tracking is that it collects information and provides visibility in environments where there were no previous tracking. Manufacturers, distributors, logistics providers and retailers all use RFID for inventory applications. RFID technology is now being embedded in 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. Well-developed systems can share the same tags to reduce implementation costs [7].

Readers covering warehouse racks, shelves and other storage locations automatically record the removal of items and update inventory records [20]. Misplaced items or those urgently required to complete an order, fixed-position readers or a worker with a mobile computer and RFID reader could automatically search for the item by reading for its specific ID number. Readers could be set to sound alarms or send notification if items are placed in unauthorized areas of the facility or removed from storage without prior approval to secure inventory from theft and diversion. Direct store delivery (DSD) and other remote sales and service personnel could take advantage of RFID readers integrated with mobile computers to quickly and accurately count inventory held in stores or in the vehicle. The automated counting would save significant time in the field, enabling representatives to visit more customers in a day. For field service applications, permanent asset tags applied to equipment could store its ID, configuration and service history information to ensure accurate and appropriate service is performed in the field where access to a central records database may be unavailable [21].

The rationale for adopting the EPC Global architecture is to facilitate sharing of information between SC participants resulting in full visibility throughout the SC. The EPC Network standard defines the RFID infrastructure
The Electronic, Author Pointer facility of the Domain through use of tracking. For this reason, RFID
and the local Object products/service groups while marked
- into pallets at the Supplier Warehouse (location#1)

RFID tags are extremely flexible and are being
- integrated in a wide range of asset management, inventory
control, and general supply chain operations relatively
inexpensively. The benefits are enormous and provide clear
visibility to the entire supply chain process.

III. RFID USAGE ISSUES

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. RFID technology needs to
support data sharing and transfer between different
locations/organizations that are partners in the SC. They are
different from the traditional assets in a threat analysis
scenario because they are “carriers” of the information assets
that are useful in the case of tracking. For this reason, RFID
have to support two important features: transfer of ownership
and multiple authorisations [25]. RFID tags contain two types
of data – static and dynamic data [26][27]. Static data pertains
to commercial entities and products/service groups while
dynamic data applies specifically to individual items. There
are two types of dynamic data – instance and temporal data.
Instance data include the serial number and the date of
manufacture while the temporal data are all captured through
EPC-tag readings – observations, containment and location
changes of objects. An RFID system will have several
interacting entities: Objects – all EPC-tagged objects, such as
cases, pallets and trucks in Figure 2(a); Readers – which are
tagged with EPC code, such as readers 1, 2, 3 and 4 (marked
with circles in Figure 2(a); Locations – used to represent
where an object is and is also associated with a owner; and
Transactions – business transaction in which EPC is involved
e.g. check-out [25].

![Figure 2. An RFID-Enabled Supply Chain Management System](image)

Each product item/case is EPC-tagged. The cases are then
packed onto pallets at the Supplier Warehouse (location#1)
where both the cases and pallets are auto-scanned by
reader#1. Then at the warehouse exit or loading zone, the
pallets are loaded onto trucks where both the pallets and
trucks are auto-scanned by reader#2. The truck then departs
through a pre-defined route (location#2). At the entry or
loading zone of the Retail Store (location#3), all the pallets
are unloaded from the truck and all the cases unloaded from
the pallets. All the cases, pallets and truck/s are auto-scanned
by reader#3 and stored. The cases are later auto-scanned by
reader#4 at the register when purchased by customers
(location#4). The dynamic interactions between these entities

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 1.

![Figure 1. A block diagram illustrating how the different ISO standards apply](image)

In short, RFID tags are extremely flexible and are being
integrated in a wide range of asset management, inventory
control, and general supply chain operations relatively

References [15] and [17] describe the RFID infrastructure or the Electronic
Product Code (EPC) network as comprising five layers: (1) The lowest layer is the RFID tags containing the EPC code,
which starts as a 64-bit to 128-bit identifier. 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. once it is attached to a physical
object, product or item. (2) The second layer consists of
RFID readers that identify any EPC tag within its
interrogating field (based on the RFID Air-Interface and
RFID protocols that specify details such as anti-collision
techniques), reads the EPC tag and forwards information to
the SAVANT. (3) The SAVANT is the middleware system
located between readers and the application systems (AS),
that act like wrappers in data integration systems. It is
responsible for data filtering, aggregation and interacts with
the EPC Information Service (EPC-IS) and the local Object
Name Service (ONS) based on configured business rules. (4) The
EPC-IS is the gateway between any requester of
information and the firm’s AS and internal databases. (5) The
local ONS is an authoritative directory of information sources
available in order to describe all EPC tags used in a supply
chain. The ONS is essentially a look-up service that maps the
EPC to a Unique Resource Locator (URL) that describes the
item represented by the EPC. The design of the ONS service
uses the Naming Authority Pointer facility of the Domain
Name Service [22][23][24].
generate events and state changes. The state changes are object location change and object containment relationship change (In addition, can include a reader location change, if the reader is moved to a new location.) Location change can be owner change as well. The events changes are observations, when readers interact with tags on objects and transacted items, when the tag on an object participates in a transaction. Queries to a RFID data management system are of two types: “Object Tracking” which is tracking the change history of RFID objects including missing objects and “Object Monitoring” which monitor the states of RFID objects and the RFID system. Current RFID data management systems only manage and store events while the state information is implicit and has to be derived. Thus, searching for state information is very complicated [25].

Despite its promises, RFID faces some challenges. In the RFID system, data points can add up fast. RFID has the potential to generate large amounts of data. There are many discrepancies in the data collected in the RFID system. The RFID data management system will need flexible rules to organize, filter and cleanse input data so that irrelevant data will not overload the system. It is important to integrate a data-quality program that profiles RFID data. In order to optimise the benefits from RFID, organizations must integrate RFID data into existing enterprise resource planning, customer relationship management and supply chain management applications. The real value of RFID technology is in exploiting the RFID data to optimise processes and relationships in the supply chain. As RFID data flows across the extended supply chain, participating organization will need new requirements for creating and sharing detailed RFID information. The organizations’ IT system will need to be flexible enough for a variety of processes and protocols. The introduction of RFID technology into the supply chain requires process reengineering in three areas: package, business site and network [28].

The increased integration of RFID technology in businesses and in the day-to-day life of consumers with 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 [8][9]. To alleviate some of these concerns, the EPCglobal developed guidelines for the use of RFID technology (http://www.epcglobalinc.org/public policy/public policy guidelines.html) but these guidelines did not go far enough.

There are two main privacy issues – personal and location privacy. Solutions that had been proposed includes: killing a tag (which can be executed with a 32-bit PIN) by disabling it at the point-of-sale counter, temporarily disabling a tag (putting a tag to sleep) then transmitting a PIN to awaken it, changing the tag identifier over time, relabeling tags, minimalist cryptography where tags contain a small collection of pseudonyms and releasing a different pseudonym on each reader query, re-encryption of tags in banknotes and universal re-encryption where the cipher-text is re-encrypted without knowledge of the corresponding public key, the Faraday Cage Approach where the tag is isolated from any electromagnetic waves, the active jamming approach where the RF channels are jammed with 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 [12].

IV. THREAT ANALYSIS

This paper will conduct a threat analysis of RFID usage in SC processes and includes mitigating the associated risks based on accepted practices or guidelines (such as NIST800-98) [13] and ISO27001/2 (available for purchase at http://www.standards-online.net/InformationSecurityStandard.htm). ISO27001 provides guidelines on the structure and controls required to implement an Information Security Management System (ISMS). ISO27002 provides the Code of Practice for Information Security Management.

Threats to RFID systems typically take place at the air interface. A number of security researchers have published papers surveying the latest development in this area [10] [12] [29][30]. References [10], [18], [30], [31] and [32] discussed a number of the major threats and examined various approaches to protect privacy and ensure integrity in RFID technology. Rogue readers can intercept and read tag information. Reader authentication can be used to allow only authorised readers to read the tag information. Eavesdropping happens when attackers secretly monitor the communication between the tag and the reader. Large read range has also opened up opportunities for eavesdropping by rogue readers. Authentication of distance is used to secure the tag by minimizing the read distance to a few millimetres. 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. 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. 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. Clandestine tracking and inventorying due to embedded tags in items that supports invisible identification,
which can be done indiscriminately, can reveal sensitive information, and violates location privacy with no contact and is non-line-of-sight. 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. 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. Physical tag destruction is when a tag is physically destroyed like microwaving in an oven or hitting it with a hammer. A summary of the threats and approaches to mitigate the risks from the threats is given in Table 1.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Reading</td>
<td>Reader authentication</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Encrypting the data, shielding the tag or</td>
</tr>
<tr>
<td></td>
<td>limit the tag-reader distance</td>
</tr>
<tr>
<td>Relay Attack</td>
<td>Using short range tags, shielding the tag</td>
</tr>
<tr>
<td></td>
<td>or implementing the distance bounding</td>
</tr>
<tr>
<td></td>
<td>protocol</td>
</tr>
<tr>
<td>Replay Attack</td>
<td>Encrypting the data, shielding the tag or</td>
</tr>
<tr>
<td></td>
<td>limit the tag-reader distance, tag</td>
</tr>
<tr>
<td></td>
<td>authentication</td>
</tr>
<tr>
<td>Tag Cloning</td>
<td>Tag authentication</td>
</tr>
<tr>
<td>Tracking People</td>
<td>Low range tags or shielding tags,</td>
</tr>
<tr>
<td></td>
<td>authenticating the readers or disabling</td>
</tr>
<tr>
<td></td>
<td>the tags</td>
</tr>
<tr>
<td>Blocking, Jamming</td>
<td>Detect early and localize, take</td>
</tr>
<tr>
<td></td>
<td>appropriate action</td>
</tr>
<tr>
<td>Tag Destruction</td>
<td>Use protective material</td>
</tr>
</tbody>
</table>

Table 1. Summary of Threats and Risk Mitigation Approaches.

The NIST800-98 [13] guideline categorises RFID risks into four categories:
1. Privacy (P) Risk is when 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.
2. Business Intelligence (BI) Risk is when a competitor could gain unauthorised access to the RFID-generated information and use it against the company.
3. Business Process (BP) Risk is when a direct attack on the RFID system components will undermine the business processes it was designed to enable.
4. Externality (EX) Risk is when the RFID system could pose a threat to non-RFID networks, systems, assets or people.

In general, the RFID system components are: tag, air-interface, reader, network and back-end. A threat can attack one or more of these components. As a result of the proliferation of threats to the RFID data, it is important to protect the confidentiality (C), integrity (I) and availability (A) of the data. Threats to RFID data can have three types of effect on the CIA of the data. The relationship between the threat, affected RFID components, effect on the data and the risk category is illustrated in Table 2.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Affected RFID Component</th>
<th>Effect on the data</th>
<th>Risk Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Reader</td>
<td>Tag, Air-Interface, Reader</td>
<td>C</td>
<td>BI</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Tag, Air-Interface</td>
<td>C</td>
<td>BI, P</td>
</tr>
<tr>
<td>Relay Attack</td>
<td>Air-Interface</td>
<td>C, I</td>
<td>BP, EX</td>
</tr>
<tr>
<td>Replay Attack</td>
<td>Tag, Air-Interface</td>
<td>C, I</td>
<td>EX, P</td>
</tr>
<tr>
<td>Tag Cloning</td>
<td>Tag, Air-Interface</td>
<td>C, I</td>
<td>BP</td>
</tr>
<tr>
<td>Tracking People</td>
<td>Tag, Air-Interface</td>
<td>C</td>
<td>BI, P</td>
</tr>
<tr>
<td>Blocking</td>
<td>Air-Interface</td>
<td>A</td>
<td>BP</td>
</tr>
<tr>
<td>Jamming</td>
<td>Air-Interface</td>
<td>A</td>
<td>BP</td>
</tr>
<tr>
<td>Physical Tag Damage</td>
<td>Tag</td>
<td>A</td>
<td>BP</td>
</tr>
</tbody>
</table>

Table 2. Threat Analysis Matrix of a RFID System. The effects are: C = View confidential data, I = Manipulate data, A = Data not available.

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.

V. CONCLUSION

RFID will fundamentally transform the way information about products, equipment, animals and even people is gathered and analysed in real time, providing new business opportunities. RFID technology enables an organization to reengineer its business processes to increase its efficiency that results in lower costs and increase its effectiveness. Companies that implement the appropriate business processes to leverage the data collected by RFID and its conversion to information and intelligence will accelerate its benefits. However, 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. Some experts believe RFID will be one of a set of technologies representing a new way of doing business brought about by convergence in which computing, communications, and interactivity are available in most places through a world of wireless, sensors, and network computing. RFID has the potential to enable machines to identify objects, understand their status, and communicate and take action if necessary, to create “real time awareness.” Future research will be based on such an autonomous interaction between entities directed towards an “Internet of Things.”

REFERENCES


[16] Ibid, p. 8


