COMP 4905 – Honours Project

Threat Analysis of Development Frameworks for the EPCglobal Network

Author: Gilles Lafrance

Advisor: Dr. Michel Barbeau
Faculty: Science
Department: Computer Science
Date: April 9, 2008

Abstract

The introduction of RFIDs in the supply chain by the use of an Electronic Product Code (EPC) has recently brought a lot of attention concerning privacy and security. These concerns have been raised by many people including the discussions made in [17] pertaining to RFID exploits, viruses, and worms and [42] concerning ONS security. Without a proper analysis of these threats we cannot determine proper ways to defend against them. Recently a group of Carleton University associates have created a paper [1] analyzing the general overview of possible security threats to an EPC based RFID systems based on the STRIDE model and the methodology proposed by the European Telecommunications Standards Institute (ETSI). This analysis will be applied to various RFID frameworks to determine possible advances that can be introduced to deal with the numerous security and privacy issues. Throughout this paper we will discuss and apply this threat analysis to the open source frameworks known as Accada and Singularity with a main focus on Accada as it has been deployed as an open source platform used for research and development.

Acknowledgments

I would first like to thank the Carleton University associates that designed the threat analysis on which I based my research. This group includes Joaquin Garcia-Alfaro, Prof. Michel Barbeau, and Prof. Evangelos Kranakis. I would also like to give out a special thank you to Prof. Michel Barbeau for being my project supervisor and for introducing this subject to me as well as Joaquin Garcia-Alfaro for co-supervising and providing me with valuable research information and ideas.

Table of contents

List of Figures

List of Tables

Introduction

RFIDs have been around for many years and were first deployed in WWII as a means of identifying friendly aircrafts. Recently RFIDs have been introduced into the supply chain by the use of an Electronic product code (EPC) developed by the MIT Auto-ID Center and currently operated by EPCglobal Inc. This EPC is a unique number associated to an RFID tag that is placed on articles such as products and shipment pallets. Information pertaining to the actual product is not stored on the tags and is instead accessed through the EPC Information Services (EPCIS) network. Each company using the system has their own private database containing the information about their products. These private databases can then be accessed with limited privileges by partner companies requiring information on your merchandise. A standardized EPCglobal RFID system consists of 4 levels used to properly organize the reading and distribution of RFID data, these areas being the ID system, the Middleware, the Discovery Service and the Information Service. Each level is a collection of various hardware and software components. To begin we have the ID system which consists of

RFID tags, readers and the appropriate reader software. The ID system is the process in which RFID data is wirelessly accessed from the tags by the readers. From here the information is set to the Middleware where it is properly filtered and aggregated. Now that we have the EPC data we can access its valuable information by connecting to the Discovery Service and receive a URL used to access this data. This URL will grant us access to information regarding that product from the manufacturer's local EPCIS. The process of retrieving this information from a partner's EPCIS is known as the Information Service. With this newly acquired data we can now store it in our own local EPCIS.

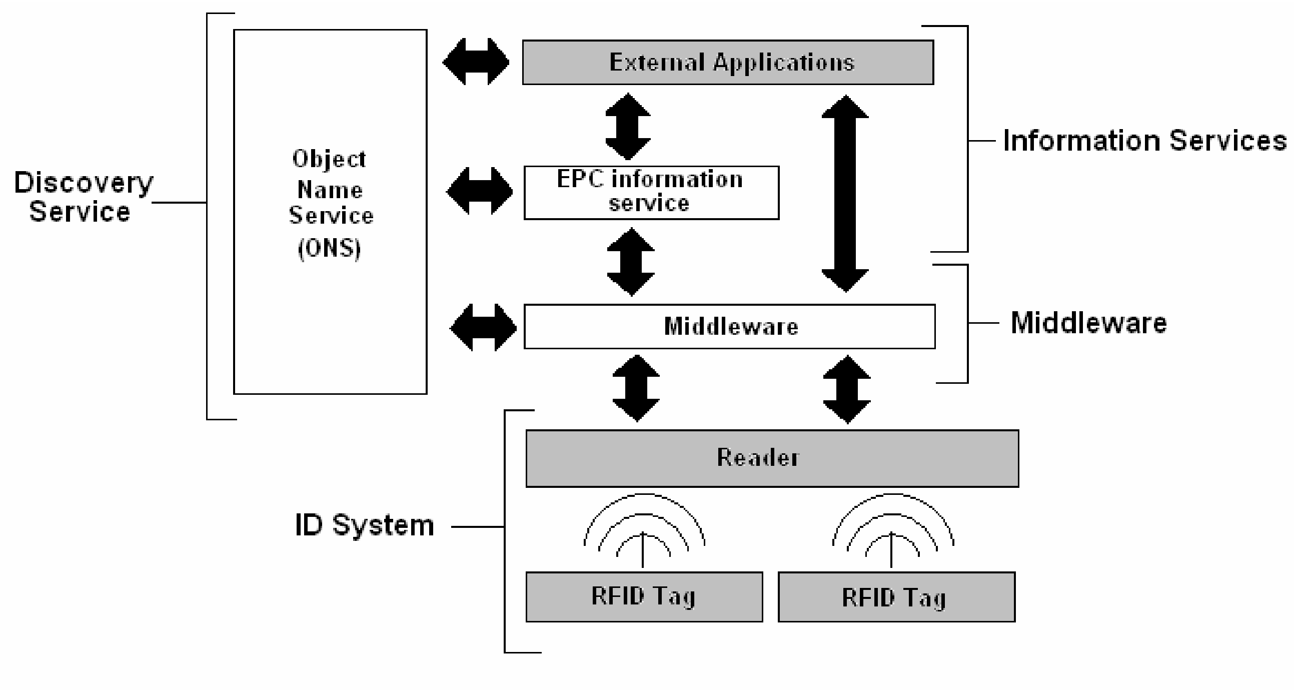

Figure 1: EPC network architecture [Diekmann et al., 2007]

RFID tags

A typical RFID tag consists of 3 parts, the antenna, the enclosure and the chip. The chip contains two types of memory: a non-volatile memory known as EEPROM stores information while the chip is not being powered, and volatile memory known as RAM is used during computation on the tag. Using the readers, the data stored on the tags can be access in two different ways depending on the type of RFID tag. There are three main types of RFID tags:

Passive Tags

The main feature of a passive tag is that it does not contain an internal source of power. This allows the size of the tag to be very small. Hitachi is the current leader in physical tag size with measurements of 0.05 x 0.05 millimeters. Power is obtained by the tag by collecting a very minute amount of energy from the radio frequency signal sent out by a reader. Returning a signal is done using a technique called backscattering where the signal received from the reader is modulated and reflected back to it. Therefore if a tags data needs to be wirelessly accessed one must be in range of a reader to power the tag. Passive RFID read distances range from about 10 cm to a few meters. Proximity cards, or commonly known as smart cards are an example of a low range passive tag. Longer range tags are being used in areas such as the supply chain by implementing EPC standards. The communication range of a passive tag depends on two factors: the need for a very strong signal to power the tag and the small amount of power available for the tag to respond to the reader. These two factors limit the range between reader to tag and tag to reader. Constraints such as these can cause problems within a dynamic operation. Consider a shipping container which just arrives and needs to access the RFID tag data. The reader will operate by connecting to each tag one-by-one. Not only will this increase the amount of time required to access every tag, but it will also increase the chance of interference. Since passive tag do not use internal batteries, are very limited in memory size, and are very small they are currently sold at a minimum price of 5 cents with a purchase of 100 million or more tags. The following figures are a few examples of passive tags:

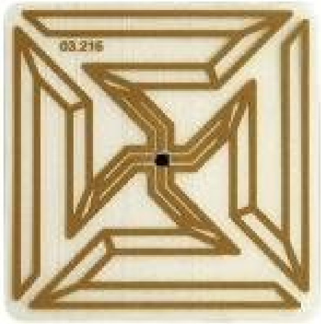

Figure 2

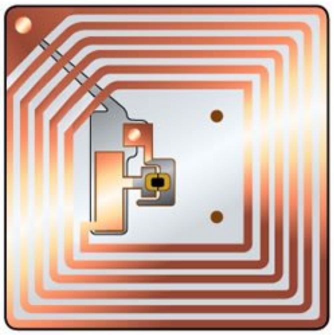

Figure 3

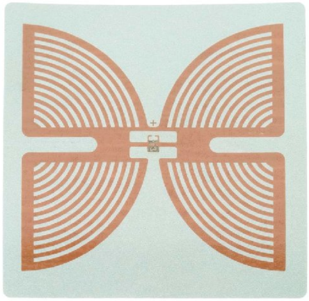

Figure 4

Active Tags

Unlike the passive tags, an active tag contains its own internal power source. This alone allows the tag to accomplish much more than a passive tag ever could. Having an internal power source however drastically increases size and cost of the tags. The factors that limit a passive tags range are nullified by the use of the internal power source in active tags. An active tag does not receive its power from a reader allowing the tag to operate by receiving very low level signals from the reader. Once the tag has received the signal from the reader it can respond with a high level signal using its own internal power. Not having these constraints eliminates many problems in a dynamic system because the reader does not have to access each tag one-by-one. Having an internal power source also increases the available read distance of the tags. An active tag's read range currently can operate at a range of around 100 meters or more.

Semi-passive tags

Similar to an active tag, semi-passive tags contain an internal source of power. However this power source is only used to power the chip and is not used to return a signal to a reader. To return a signal a semi-passive tag uses the same methods as a passive tag by backscattering the signal received from the reader. Another possible use of the internal power source is to store energy from the reader to be able to return a signal in the future.

EPCglobal Class 1 Generation 2 tag

In December 2004 EPCglobal approved the new RFID tag known as a Class 1 Generation 2 tag. This new tag has become the new standard for low cost RFID technology in the supply chain replacing the previous Class 0/1 and ISO tags. While improving on the features of previous tags the Class 1 Gen 2 tag is also designed to meet emerging Ultra High Frequency (UHF) regulations in various regions to accommodate the use in worldwide deployment.

Speed

Unlike previous tags which operate at a single communication speed a Class 1 Gen 2 tag has the ability to run at four different speeds. At top speed a Gen 2 system can theoretically read 1000 tags per second. However, achieving these speeds would require an area insulated from RF noise. By increasing the read speed we are also decreasing the reliability, therefore in areas with high RF noise we would use lower speeds in the range of 100 tags per second to increasing the read reliability.

Q protocol and Symmetry

A tag on the outer edge of a readers range will experience only short burst of power from the reader and can therefore make it very difficult to access. The Q protocol proven affective in previous Gen 1 tags addresses this issue by passing short simple queries between the tags and the reader. The reader begins by issuing a query and each tag responds with a randomly generated number. The reader then sends out an acknowledgment request using one tags random number. The tag holding the random number is now able to communicate with the reader. With this connection the reader can encrypt the commands by performing a bit-by-bit exclusive OR (XOR) using the random generated number issued between the tag and reader. Once the tag has been successfully read it is put in “sleep” mode until the reader has completed accessing the other tags. Every tag that is asleep is removed from the reader’s lists to allow easier access to the more difficult to read tags. Once every tag has been read a “wake-up” command is sent to each tag to reactivate them. In a typical Gen 1 system the sleep and wake-up commands are sent multiple times to increase the accuracy of the final inventory. To refine this process a Gen 2 tag uses a dual-state symmetry scheme. This allows a new inventory count to be created without the tags needing to be put to sleep or woken up. To accomplish this, the reader begins by setting each tag in state A. Once a tag has been read using the appropriate random number it is put in state B. Once a tag in state B has been read again it is put back into state A. Repeating this process of switching a tag between two states allows the reader to go through the entire inventory in a similar way to the previous method of multiple sleep and wake up calls.

Anti-collision with Multiple Readers

With the use of multiple readers many problems can arise. The first problem is known as the "dense-reader" problem. While a reader can output a powerful signal to a tag, the tag can only respond with a very minimal signal. Having too many readers communicating to various tags can drown out this faint signal response from a tag. To deal with this issue, Gen 2 tags new signaling mode isolates tag responses into a side channel that is easier to access. Using the Miller sub-carrier algorithm we can specify side channels of varying widths according to the overall noise conditions. This means that we can specify channels that are not being used by the reader and therefore will reduce the risk of interference. Gen 2 tags can also use FM0 which is a faster algorithm used in current ISO standards but is much more susceptible to interference.

Another problem that can arise is having two or more readers try to communicate with the same tag. The problems that we face here are concerning the state of the tag. As mentioned before, a tag will be in either state A or state B. If two readers are trying to read the same tag around the same time they will each change the tags state accordingly. Now both readers' inventory counts have been changed, and this is where the problem arises. With the use of the proper applications this problem can usually be avoided by allowing only one reader to access the tag; however Gen 2 has improved on this by introducing the use of sessions. A session accommodates the grouping of various readers according to how they are used. In other words, we can eliminate the confusion between various readers by grouping them by the type of reader and where they are used. For example, let's say a warehouse consists of two types of readers: mobile and stationary. Using sessions we group the stationary reader separate from the mobile readers. This will allow both reader types to initiate tag reads without accidentally changing the state of a tag currently used by another session.

Memory

An EPC tag's memory consists of four different memory banks. We consider each banks memory address to start at 00_h.

Reserved memory: If passwords are being uses then the kill and access passwords are stored here. The kill password is a 32-bit value stored between 00_h and $1F_h$ that is used to render the tag unresponsive once it is no longer needed. If no kill password is set then it operates as a zero-value password that is permanently read/write locked. The access password is also 32-bit value stored between 20_h and $3F_h$ used to gain access to the tag. If no access password is set it does the same as the kill password and sets itself to a zero-value password and is permanently locked. Unlike the access password, the kill password cannot run when it does not exist to eliminate wrongful termination.

EPC memory: the main parts of EPC memory are CRC-16 (16 bit cyclic redundancy check), PC (protocol-control) and EPC. The 16 bit CRC is used to protect the PC+EPC value by having the tag backscatter the CRC-16 during operation. At power-up of the tag the CRC-16 is computed on the PC+EPC values and stored in EPC memory 00_h to $0F_h$. The 16 PC bits contain physical layer information that is stored from

10_h to $1F_h$. The first five bits are used for the length of the PC+EPC value. Bits 15_h and 16_h are reserved for future use and are currently set to 00_2 for Class 1 tags. The final 9 bits consists of the numbering system identifier (NSI). The first bit at 17_h is used to identify whether or not it is an EPCglobal application. If this bit contains a logical 0 then it is seen as an EPCglobal application and bits 18_h to $1F_h$ are defined in the EPCglobal tag data standards. If bit 17_h contains a logical 1 then it is not an EPCglobal application and bits 18_h to $1F_h$ will contain the entire Application Family Identifier (AFI) defined in ISO/IEC 15961.

TID memory: Tag identifier (TID) memory contains an 8-bit ISO allocation class identifier at 00_h to 07_h. Anything above 07_h shall contain sufficient identification information to uniquely identify custom commands and optional features supported by the tag based on the class identifier. The remaining bits may also contain tag or vendor specific data such as a tags serial number. The TID memory is also linked with the EPC data in a manufacturer's EPCIS therefore making it impossible to switch the data between two tags.

User memory: A tag may contain but does not always contain User memory. This allows for user-specific data storage. An EPCglobal application with user memory shall be encoded using the EPC standards defined in the EPCglobal Tag data standards and a non EPCglobal application with user memory shall store the Data Storage Format Identifier (DSFID) from 00_h to 07_h defined in ISO/IEC 15961. Anything above 07_h will be as define in ISO/IEC 15962.

The major risks associated with RFID

Business process risk: A direct attack on an RFID system could undermine the business processes originally intended to be enabled by the RFID system. In other words, a company whose main system relies on RFID for tracking will not be able to process orders and keep track of inventory in an orderly and timely fashion.

Business intelligence risk: If an attacker were to gain access to a companies RFID system, they could potentially access valuable information and use it against them. An example of this would be if someone were to gain access to Wal-Mart's RFID system. In theory the attacker may be able to gain information on the more expensive items that Wal-Mart carries. Using this information the attacker could then track down and steal the containers holding these multiple expensive items. Another option that an attacker has is to sell this information to a rival who can use it to their advantage.

Privacy Risk: Privacy is directed more towards an individual and there everyday lives. Information about a person or a group of people can be used by a company to market their product to the appropriate people. With RFID tags being hidden inside items such as clothing a company can scan someone's RFID tags without their knowledge and offer them products that relate to their style. Depending on the amount of privacy a person actually expects this can be seen as a great new feature or on the other hand an invasion of privacy. With the introduction of RFIDs into other items such as phones and car keys we may never know what kind of valuable personal information will be disclosed.

Externality risk: An RFID system could also bring risk to non-RFID systems that are networked with the system. Through the use of Internet Protocols (IP) and badly configured readers an attacker could gain access to computers and valuable information on the network. With this, the attacker could potentially gain power over the entire system.

STRIDE

To conduct our analysis we will be using the security threat model known as STRIDE: Spoofing identity, Tampering with data, Repudiation, Denial of service, and Elevation of privilege. Some threats can simply disrupt the inventory system and others can be used for personal gain.

Spoofing identity

Spoofing is when an attacker successfully poses as authorized user of this system. An RFID system can be susceptible to many different types of spoofing threats. Here are a few examples:

- An attacker spoofing one or more legal tags would disrupt the company's internal inventory. This would make the company assume that it has more stock than it actually has and would disrupt the internal shipping and receiving system.
- An attacker spoofing a legal reader however is much more significant threat because it could be use for personal gain. If the attacker were to perform an unauthorized inventory check they could offer the information to a competitor which can then use that to its advantage.

Tampering with data

Data tampering occurs when and attacker is able to create, modify or delete stored data. With the proper techniques data tampering in most cases can be avoided although system that do not implement them properly are still at risk. Here is a list of possible data tampering threats:

- If an attacker was able to modify the data of an EPC tag they would disrupt the internal system of a company.
- Adding tags to a company's inventory can have the same affect as spoofing a tag. Authentic tags could have been procured from another company selling the same item and used to disrupt the system.
- An Attacker that can gain access to the kill command of tags could simply destroy the information on every tag that it can access. Although this password would be very difficult to get, once they have it they could walk through a store or have a hidden reader periodically kill every tag it could access.
- Removing or physically destroying a tag is also seen as data tampering. If an attacker were to do this unnoticed they could easily walk out of the store with an RFID-less product, and would therefore not be detected.
- Because the wireless channel between tag and reader is seen as potentially insecure an attacker could modify the return signal from a tag. This will have the same affects as modify the data on a tag itself.
- If a product is off its warranty an attacker could modify the data on the tag or steal a tag from a similar product to reestablish the warranty or even refund.

Repudiation

Repudiation is when a user denies that a certain action was performed when there is no evidence to prove that in fact the action did occur. If there are no proper non-repudiation protocols introduced then the RFID system could be affected by threat such as these:

- Lack or proof to show that a tag has been read by a reader. A user could say that they have not received a shipment and blame either the manufacturer or the shipping company.
- The manufacturer of a certain product could deny having information on a product with a specific EPC number. This would allow the manufacturer to also deny services such as warranty, repairs, or return.

Information disclosure

Information disclosure occurs when information from a tag has been illegally accessed by an unauthorized user. In information disclosure the main threat is to ones privacy. Here is a list of possible threat affected by information disclosure:

- Someone walking down the street carrying RFID enabled products is illegally scanned to determine what these items are. With this kind of information an attacker could pick out people carrying certain products for various reasons. One of these reasons could be for company marketing. If an attacker working for a designer clothing company discovers that someone is wearing a lot of their products, they would know to target them with product opportunities over say someone wearing simple jeans and t-shirt. This could also be done inside a retail store by installing a reader at the entrance. When the user walks they are offered various deals on similar products by an employee or by looking at an LCD screen.

- Walking around carrying RFID enabled devices could make it a lot easier for someone to steal what they want from you. Consider someone walking around with an expensive RFID enabled product in their pocket such as a phone or car keys. An attacker could then target that specific person and steal from them.
- Just like spoofing a reader, if tag information is disclosed in a warehouse an attacker could sell this information to a competitor.

Denial of Service

A Denial of Service attack (DoS) is when an attacker successfully manages to deny services to an authorized user. There are many ways this can be done and it is not always easy to prevent against. Here are some examples of possible DoS attacks:

- Devices known as blocker tags are used to disrupt the signal between tag and reader. Using one of these devices the reader cannot access the information on a tag and the person holding the blocker tag can freely walk out of a store carrying items that have been blocked from the reader.
- Using a type of metal enclosure known as a faraday cage an attacker can easily shoplift items by insert them inside this enclosure and simply walking out the store. The faraday cage is used to block incoming and outgoing signals from a tag.

- Tags have a very weak return signal when they are talking to a reader. If an attacker was able to broadcast a more powerful signal they could potentially drown out the weak tag signal.
- An RFID system is also susceptible to traditional internet DoS attacks against the servers gathering EPC data from the readers and against ONS.

Elevation of privilege

Elevation of privilege defines a threat where an unauthorized user or a user with very little privileges elevates their status on the system to grant them access to areas that they were previously unauthorized to go. Here is an example:

- An attacker or unauthorized user that raises their status to system administrator can have total control over a system and can add malicious code or delete valuable information.

Threat Analysis

In our security analysis we will be following the evaluation functions proposed by Michel Barbeau and Christine Laurendeau in [2] and modeling after the results found in [1] in relation to two open source RFID frameworks known as Accada and Singularity. These evaluation functions are based on the methodology proposed by the European Telecommunications standards (ETSI) with a few modifications.

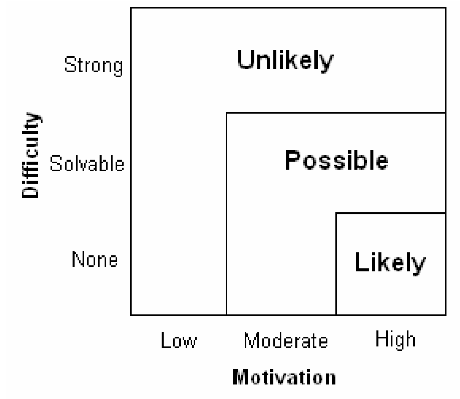

Figure 5: Likelihood of threat [Barbeau and Laurendeau 2007]

Figure 5 is used to determine the likelihood of a threat. This is done by looking at the motivation of the attacker and the technical difficulties that an attacker must overcome. The motivation of an attacker is defined as the motivation needed to carry out the attack path, whether it is “low”, “moderate”, or “high”. The difficulties associated with the attack are evaluated as “none” in which very little work is required, “solvable” where moderate amount of work is required to overcome obstacles, and “strong” where the difficulties are seen as very complicated and close to impossible. Using the determined likelihood we can move on to the next evaluation function to determine the risk of the threat.

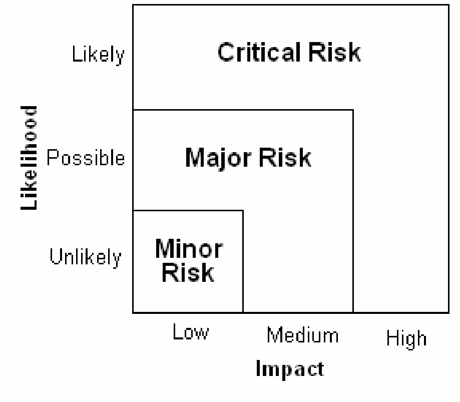

Figure 6: Risk evaluation function [Barbeau and Laurendeau 2007]

With the evaluation function shown in Figure 6 we can determine the risk of the threat by looking at the likelihood we previously obtained from Figure 5 and the impact this threat would have on the system. The measurements of the impact are evaluated as "low" where the attack results in small outages, "medium" if these outages create minimal financial losses, and "high" if a large financial loss is noticed while outages are occurring more often and affecting many users.

In our evaluation we have assumed that the attacker is working from the outside with no physical access to the components or the RFID infrastructure involved. However, this doesn't stop the attacker from having information on both the components and infrastructure being used. To conduct this analysis we will discuss the techniques used by the two frameworks followed by an overall threat analysis at each step in the architecture. These steps being ID system, Middleware, Discovery Service, and Information Service

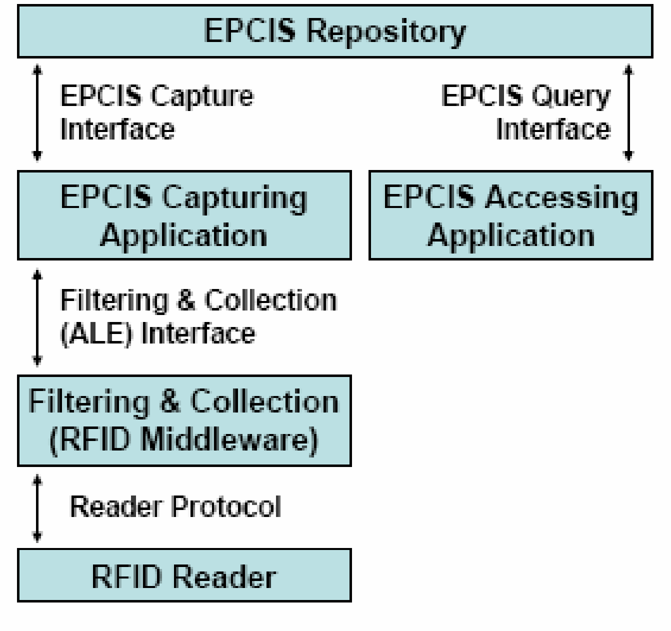
EPCIS Repository
EPCIS Capture Interface
EPCIS Query Interface
EPCIS Capturing Application
EPCIS Accessing Application
Filtering & Collection (ALE) Interface
Filtering & Collection (RFID Middleware)
Reader Protocol
RFID Reader

Figure 7: Accada architecture

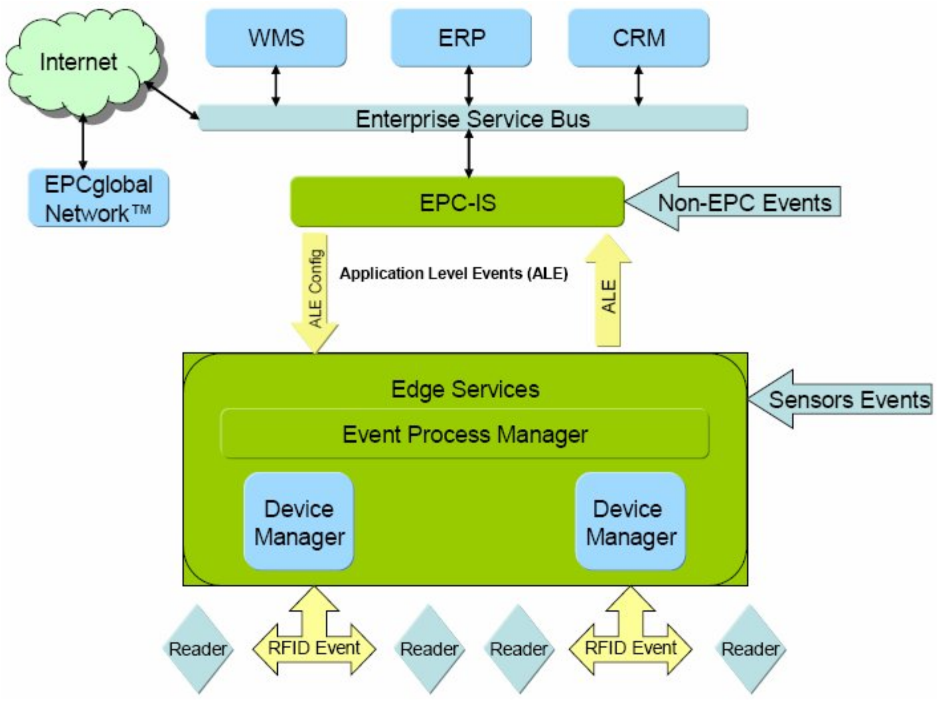

Figure 8: Singularity architecture

ID System

Accada: Reader module

The reader module that has been developed for Accada was designed based on the specifications in the EPCglobal Reader Protocol. The EPCglobal Reader protocol specifies current requirements that must be satisfied by the reader module. These requirements mainly consist of data dissemination, filtering, aggregation, writing to tags, and external triggers. Not only does the reader implement the mandatory features it also implements those that are seen as optional. Optional features added in the Accada reader are virtual tag memory service (VTMS), the adaptive filters to compute the aggregates, and the surrogate mode. The virtual tag memory service developed is used to facilitate the interaction between tag and reader by eliminating RFID inconveniences such as limited memory size and limited read range. To operate the

VTMS the host needs to simply provide key-value pairs to a set of tags. The reader then looks at the VTMS to determine the proper memory block to write to. If the tag write succeeds a backup copy of the data is stored in the VTMS. Now that we have a backup copy we only need to access the tag when we need to write to it or kill it. If writing to the tag fails due to lack of power the key-value pair is stored in the VTMS for a later time when the tag comes back into reader range. However if writing to the tag fails because of lack of memory then the reader will receive and error message and will store the key-value pair in the VTMS. The adaptive filters are used to smooth out the noise from the collected RFID data and to help deal with false negative reads. When implementing the reader module we can proceed in three different ways: First, by the use of an integrated computer containing the needed software known as a surrogate. Using the surrogate method we can easily deal with multiple readers and those that have proprietary message transport bindings and limited resources. Another method is to have the software embedded on the reader itself. Finally for testing purposes we can also currently avoid the need of reader hardware with simulation software. The EPCglobal Reader Protocol implemented by Accada abstracts from the EPCglobal Air Interface Protocol because it allows the application developer to be shielded from RF communication details. Although this has its disadvantages by preventing the use of the advanced features of an air interface. Features specific to an air interface include the denser reader mode introduced with the Class 1 Gen 2 tags. The EPCglobal Reader Protocol currently allows access to a tags memory however it is not possible to perform command such as read, write and kill without the use of an application.

Singularity: Device Manager

Included in the Singularity framework is a Device Manager (DM) which is used in a similar way as the Accada Reader module. The Device Manager is used to configure and manage reader devices. When the Device Manager initializes it will determine what physical devices it is responsible for and will configure them accordingly. Supported by this framework is the "logical reader" aspect which combines readers from different areas into one that will send reader events to the middleware process known as the Event Manager. Unlike Accada, Singularity does not support the VTMS service; therefore security features facilitated by the VTMS will not be relevant to the Singularity framework.

ID System Threats

Because the communication channel between tag and reader is potentially seen as an insecure connection we can assume that many threats associated to RFID will take place here. To begin our security analysis let us look at the causes and effects of the first threat of the STRIDE model.

Spoofing

With the new Class 1 Gen 2 tags explained above a few new security features have been added including the CRC-16 and the 16 bit pseudo random number. However without the available on-chip memory we cannot apply stronger cryptographic functions such as MD5 or SHA-1. In current EPC Class 1 Gen 2 tags the security used is a simple XOR function between the access password and the pseudo random number shared between tag and reader. By eavesdropping on the signals we can determine the access password from the random number and the XOR function that we have intercepted. Therefore as discussed in the spoofing threats, a malicious reader that successfully breaks the Class 1 Gen 2 tags security can impersonate a legal reader. Although the EPC data on a tag seems to be meaningless to an average person, a rival company or thief could use this information to their advantage. With this unauthorized reader we can also copy tags that have been scanned. We can therefore rank the motivation of such a threat as "high" because the attacker can sell this information for personal gain. We can also rank this as a "solvable" problem since it is theoretically possible to determine the access password of a tag. The impact of such a "possible" threat can be seen as "high" resulting in a "critical" risk.

Tampering with data

For tampering of data we will be looking at the data stored on a tag and the data transmitted from tag to receiver. The first thing that an attacker would need to do in order to affect the data that is stored and shared is to determine the 32-bit PIN access password. By eavesdropping on the wireless connection an attacker can determine the pseudo random number and the XOR encrypted access password shared between tag and reader. Using these two values the attacker can easily determine the access password of the tag. Now that the attacker has the access password to a tag, using a Class 1 Gen 2 reader they can access, delete, or modify information from the tag. Possible exploits that could be taken advantage of in this case can either be used to disrupt the company's internal system or could also be used for personal gain. Disrupting the company's internal system can be done by simply modifying or deleting the data from EPC tags that can be accessed. This is not seen as a big problem since there is minimal financial loss caused by the disruption in the business process. However, if an attacker were able to determine one products access password and another products kill password they could easily use that to their advantage to steal from the company. If one of these products is much more expensive then the attacker can simply use the cheaper tag on the more expensive item. This is easier said than done because we cannot simply switch the EPC data between the two tags. This is because of the unique tag information stored in the locked TID memory. The TID memory once written cannot be modified, therefore making it impossible to switch EPC data between two tags. The "easiest" way to do this would be to just switch the RFID tags in the same way barcodes have been switched for years. However this does not seem very practical and it would be very easy to get caught. Therefore what we would need to do is determine the access password to the cheaper product that we will be "purchasing" and the kill password to the product we will actually be getting. Obtaining the access password can be done in different ways depending on the mechanism used to scan the RFID tags. One way would be to bring the product up to a check out counter or price check where they will be accessed by readers. Another way would be to determine the access password when the shipment arrives at the store. This would also be a good time to determine the kill password of the other product because this requires a power analysis of the tag as discussed in [30]. Now that the attacker has the passwords that he needs he can begin by creating a copy of the less expensive products tag. Using this newly made tag the attacker can attach it to the expensive product and kill its actual tag. All the attacker needs to do now is purchase his product with the fake RFID tag. Once the company realizes what has happened the attacker will be long gone. Another way to kill a tag that is much easier then determining the kill password is to use a device known as a RFID-Zapper which has recently been demonstrated in [37]. This method uses a strong electromagnetic field to destroy a tag indefinitely. Seeing as this method is a lot easier to accomplish than finding the kill password we will use this technique as a means of killing the tags in our evaluation. The results concluded by [1] indicate that the motivation of an attacker to perform a data tampering attack on the ID system is moderate because the attacker would simply be disrupting the company's business process, however with the aforementioned tag switching attack the motivation towards such an attack increases to "high" because the attacker will now have some personal gain in doing such an attack. The technical difficulties are easier said than done to overcome because they include the determining the access password and killing a tag. However this is still theoretically possible and therefore the difficulty is seen as "solvable". With these findings the result shows the likelihood to be "possible". Moving on to the impact related to this type of threat we can say that it has a "high" affect on the company's business operation while having substantial financial losses. Therefore we can conclude that this threat is a "critical" risk and should be dealt with appropriately.

Repudiation

Currently due to the lack of non-repudiation protocols in the EPCglobal network infrastructure used by Accada and Singularity a company can easily deny that a shipment has arrived. The only evidence that can be used is a time stamp, but indeed this is not proof. We can see that this can easily be used for financial gain therefore the motivation towards such a threat is seen as "moderate". The only difficulty that we will face in this situation is the laws that will be broken. Therefore that clearly makes this a "solvable" threat. This threat will also have a "medium" impact because there will be some financial and disruption to the system. Since Accada and Singularity have not been able to improve on the repudiation threat at the ID system level we are still faced with the results found in [1] that the likelihood would be "possible" and the risk would be "major".

Information disclosure

As shown in the spoofing threat, by eavesdropping is it theoretically possible to retrieve EPC data through the wireless connection between tag and reader. In other words this is a disclosure of information. Seeing as the effects of this threat are very similar to that of a spoofing threat we can say that they share the same results.

Denial of Service

As shown in the tampering with data threat it is theoretically possible to determine the access password by simply eavesdropping on the connection between tag and reader by determining the XOR function and the pseudo-random number. Also, again according to [30], we can theoretically determine the kill and access password by doing a power analysis. With these passwords we can do similar things to disrupt the internal system. Using the kill password we can simply connect to various tags and send the kill command. Using the access password we can also do a similar type of attack by removing all the available data from the tag. Both of these methods will deny readers from accessing the tags because according to the readers the tags are no longer there or they do not contain any EPC data.

The next method proposed in [1] is to use an RFID jamming attack where a powerful transmitter would broadcast strong signals on the same frequency as the tags. As mentioned this type of attack is possible and is not very difficult to do, however with such a powerful emitter there is a good chance FCC laws will be broken. Therefore we suggest a similar mechanism known as RFID blocker tags. Currently RSA has discussed in [16] two methods in which a blocker tag can be used. The two methods are based on the types of singulation known as ALOHA and tree-walking. The Q protocol supported by Class 1 Gen 2 and applied by Accada and Singularity is a type of ALOHA singulation. A general RFID blocker tag simulates all the possible RFID tags and this causes collisions between the legal tags and the blocker tag simulating it. In consequence this renders all the tags inaccessible. A blocker tag can also be made to simulate a specific tag if information from the tag is previously known. Therefore using a blocker tag an attacker can successfully deny access to all or specific tags without breaking any current laws.

As mentioned before, determining the access password is theoretically possible as well as creating a Blocker tag. This implies that in a general RFID framework the difficulties towards this threat are “solvable”. However, with the virtual tag memory service (VTMS) employed by Accada these DoS threats will create very minimal affect on the system. As soon as a tag is entered into the system it is stored in the VTMS. If information is needed from a tag and the tag is not in the vicinity of the reader then the information is simply retrieved from the VTMS. The only time the DoS attacks will have an effect on the system is when a reader tries to write to a tag and in this case the information will be stored in the VTMS for later use when the tag is back in range.

Therefore if the information is removed or if the kill command has been sent out to the tags the readers will notice that they can know longer see them. Eventually someone will realize that these tags have not been around for awhile and will begin investigating. Once they determine that the tags have been disabled they can easily resolve the issue. Therefore this increases the difficulty of a DoS attack over other frameworks. In other words we can reset the difficulty back to "strong" using the Accada framework. Seeing as an attacker will not have any financial gain with this type of threat we can set the motivation to "low". With a "low" impact to the system we can conclude this to be a "minor" risk with the determined likelihood of "unlikely".

Elevation of privilege

EPC tags do not carry information regarding privileges like some other RFID devices such as passports. Since an attacker does not have physical access to the system this could create a great deal of problems with elevation of privilege in the ID system of a supply chain RFID framework. In this case we will look at possible programming flaws in the reader through the wireless connection to hopefully change the configurations to support different RFID tags. Seeing as this is almost impossible to do without a physical connection we can see that the results determined correlate with those found in [1] with motivation = "low", difficulty = "strong", likelihood = "unlikely", impact = "low", and risk = "minor".

Threat	Motivation	Difficulty	Likelihood	Impact	Risk
Spoofing of identity	High	Solvable	Possible	High	Critical
Tampering with data	High	Solvable	Possible	High	Critical
Repudiation	Moderate	Solvable	Possible	Medium	Major
Information disclosure	High	Solvable	Possible	High	Critical
Denial of service	Moderate	Solvable	Possible	Medium	Major
Elevation of privilege	High	Strong	Unlikely	High	Critical

Table 1: ID system threat analysis

Middleware

Accada: Filtering and Collection Middleware module

Once a reader captures proper tag data it notifies the middleware so that it can perform the proper steps of filtering and collection. Here we will have multiple readers sending data to the middleware to properly aggregate the data from all the readers to eliminate redundant reads and to perform various types of filtering. In other words the middleware will create a single interface for multiple readers to connect to. This allows applications to create a standing query and subsequently subscribe to it. A standing query is simply a query that is repeated multiple times over a period of time. Using the subscription to this query we configure the readers according to the EPCglobal Reader Protocol. With this readers can determine whether the RFID data is significant to an application. Once a reader captures data that is relevant it notifies the middleware which combines all data retrieved from readers according to the pre-determined standing query schedule of the subscribed applications. Using this method allows the readers to efficiently use the available bandwidth by increasing the sampling rate when targeting a specific group of tags or by turning off a reader's connection completely to transfer the available bandwidth to another reader. The interface used between the filtering and collection middleware and the next step towards the EPCIS module is known as an Application Level Event (ALE) interface. The ALE standard defined by the EPCglobal is used to create XML reports based on the activity made by the EPC tags. These XML reports contain a high-level description of what operations to perform and EPC tag information such as the duration of activity and company product information used for grouping. The current company or one of their partners then sends this information to the EPCIS module to store it for later use.

Singularity: Event Process Manager

Singularity's middleware filtering and data collection is similar to Accada and is known as the Event Process Manager (EPM). Between the DM and EPM is the Service Component Bus (SCB) which deals with the subscription of the events that the EPM will handle. Events are transferred between the DM and the EPM by notifying the EPM through the Message Space. From here the EPM filters the events received from the DM and can publish them to the EPCIS.

Middleware threats

Unlike the other three processes, the middleware does not have any outside connection without through one of these mentioned processes. The main threats associated to the middleware are concerning the available filtering and collection utilities. Possible security holes were recently discovered by students at the Vrije University in Amsterdam and they are discussed in [17]. These possible threats involve exploits such as buffer overflows and SQL injections along with other threats including RFID worms and viruses. These threats utilize the available memory on a tag to insert malicious code used to do a variety of hostile acts on the system. Let us first begin with possible exploits starting with SQL injections. The statement "SQL injection" clearly depicts that this is some way of introducing SQL code into the information stored on an EPC tag. This is usually done by including a ";" somewhere in the data. An example of this at the stage of inserted the EPC data in the SQL database would be a command such as this

```
INSERT INTO EPCISlibrary VALUES ( '%id%', '%data%')
```

where the data value looks something like "apples'); -insert SQL code-"

This will force the database to complete the two SQL commands separated by the semicolon. Even with very little available memory on a tag, an attacker could insert commands such as

```
drop table <tablename>
```

which will delete the entire SQL database. Another possible exploit is found in middleware designed using languages such as C and C++ and is known as a buffer overflow. An RFID tag contains information regarding the amount of information stored on the tag. By changing this information using illegitimate readers and tags a legal reader could accidentally read in more data than expected causing a buffer overflow. This buffer overflow will cause the unexpected data to overwrite on top of previous data stored on the tag. By included shell commands into this unexpected data an attacker can theoretically take control of a system.

Using these exploits and known holes in widely-used network services an attacker can theoretically propagate RFID viruses and worms throughout the system. A virus spreads by attaching itself to a tag, entering the system and extending itself onto new tags. Unlike a virus, a worm is self-replicating over both RFID tags and network holes and does not require user activity to spread.

Although these threats seem to be of a great concern, the minimal amount of available memory on Gen 2 tags limits the possibility of such attacks. Distributed RFID frameworks such as Accada and Singularity also tend to take care of these issues during the filtering process. In the case of a buffer flow, Accada and Singularity cannot be infected since they are written in java which is completely invulnerable to such a threat. Databases systems such as MySQL and Oracle also support their own SQL injection filtering techniques. An example of this is the mysql_real_escape_string() command used by MySQL which detects unwanted characters that would cause an SQL injection. The motivation of an attacker towards carrying out such an attack can be seen as "high" because with the proper commands or malware they could take control of the entire system, however from a technical stand point this is pretty much impossible when using an RFID framework that complies with EPC standards. Although the impact of such a threat could be seen as "high" we simply cannot declare this as a critical risk because of the implemented filtering techniques and the unlikely ability to overcome them. Therefore we declare this as a "minor" threat.

Discovery Service

Currently Accada and Singularity do not have a discovery service implemented into their framework, however future releases will most likely integrate this service using the Object Name Service (ONS). The basic operation of ONS is to determine a URL which allows a partner company to access EPC data from a retailer or manufacturer using the information stored on an EPC tag in URI form. ONS is a subset of functions of the Domain Name service (DNS) and therefore will also have the same known security vulnerabilities. Since ONS is used by all frameworks in pretty much the same way, the examination of Discovery Service threats in [42] are general to all RFID frameworks. Therefore the following threat analysis of the discovery service will be a brief overview with a few added threat possibilities. We encourage the reader to refer to [1] and [42] for a more elaborate explanation.

Discovery Service threats

Spoofing

The two options available for a spoofing attack are impersonating an external application or to imitate the ONS/DNS server. The main objective here is to obtain valid URLs to determine what products are certain company has. If an attacker seized valid URLs they could sell the information to a rival company or thief. Therefore we can rank the motivation of such an attack as “high” as well as a “possible” likelihood since the technical difficulties are “solvable” using known DNS security flaws. The impact of such an attack can be seen as “high” since this will cause financial loss from a thief and it could also give the advantage to a competitor eventually resulting in loss of revenue. Therefore the resulting risk is seen as “critical” and should be dealt with appropriately.

Tampering with data

An attacker may try to tamper with data by attempting to impersonate an ONS/DNS server by intercepting queries to a legitimate company’s server and respond with false URLs. Sending the false information to the company will result in a loss of trust between the two partners. The difficulties associated with this threat are seen as “solvable” using known exploits such as hijacking or manipulation of queries and offers the attacker a “moderate” motivation resulting in a “possible” likelihood. The impact is seen as “medium” since the company will be providing company information to an illegitimate user using the false URLs. Along with this the reputation of the company will be affected causing this threat to be considered as a “major” risk.

If we were to consider similar attacks discussed in the middleware threats we can see that with these false URLs an attacker could theoretically inject an SQL command into the false EPC data which will later be store in the database or possibly create a buffer flow. Although this seems possible, as explained before the filtering mechanisms used in an EPCglobal standardized framework tend to deal with these types of threats as well having software written in a language unaffected by buffer overflows like java.

Repudiation

With the very limited amount of tracing and auditing services an attacker could potentially perform illegal operations on the ONS/DNS server of a company through an external application. We can rate the motivation of such a threat as “moderate” because now the attacker could offer these services to partners or customers of the company. This results in a “possible” likelihood based on the fact that the difficulties associated with this threat are “solvable”. This will also have a “medium” impact on the company resulting in “major” risk.

Information disclosure

As previously discussed in the spoofing threat impersonating an external application or imitating the ONS/DNS server is a “solvable” difficulty through known DNS flaws. Therefore by seizing valid URLs an attacker can gain access to EPC information of that company. The motivation behind such an attack is “high” since obtaining information is the main reason this threat is taking place. The information will allow the attacker to have some financial gain by selling it to a competitor rendering this a “possible” threat. This disclosure of information will have a “high” impact classifying this as a “critical” risk.

Denial of Service

Known security flaws in DNS make the difficulty of a DoS attack “solvable”. Seeing as this is fairly simple to overcome, the motivation towards such an attack is “moderate” if this DoS attack is performed by someone working for a competitor. This will have a “medium” impact on the company based on possible small financial loss and the disruption on discovery services. This results in a “possible” attack with a “major” risk.

Elevation of privilege

Possible elevation of privileges threats involve SQL injections or buffer overflows using illegitimate URLs as mentioned above. Although the technical difficulties are still seen as “strong” to overcome the motivation would be considered as “high” because the attacker can benefit from having more access to the system in multiple ways. The impact is considered as “high” because unauthorized users will be granted access to valuable business information and also possible to take control over the entire system. Although with an “unlikely” possibility of performing elevation of privileges we can still rank this as a “critical” risk and must be dealt with accordingly.

Threat	Motivation	Difficulty	Likelihood	Impact	Risk
Spoofing of identity	High	Solvable	Possible	High	Critical
Tampering with data	Moderate	Solvable	Possible	Medium	Major
Repudiation	Moderate	Solvable	Possible	Medium	Major
Information disclosure	High	Solvable	Possible	High	Critical
Denial of service	Moderate	Solvable	Possible	Medium	Major
Elevation of privilege	High	Strong	Unlikely	High	Critical

Table 2: Discovery service threat analysis

Information Services

Accada: EPCIS module

The EPC Information Services (EPCIS) is responsible for receiving application specific RFID data and translating it into the proper business events and by making these events available. The EPCIS is made up of 3 different parts: A capturing application used to interpret the captured RFID data from the filtering and collection middleware, an EPCIS repository to store all the EPCIS events, and an accessing application to retrieve EPCIS events from the repository.

EPCIS capturing application

The role of the capturing application is to collect unidentified RFID data. The capturing application also has the responsibility of organizing each unidentified RFID data that has been captured into one single EPCIS event. Implementations of the capturing application can be done in various ways depending on the need for accessing business information from the collected RFID data. For example consider a retail store that just received the new shipment of sneakers that they were waiting for. The capturing application would receive the sneaker RFID data but would not know what to do with it. If the sneaker manufacturer trusts the retailer they will be granted access to historical data through their accessing application by first determining the relative URL address through ONS. Accada has chosen to create a simple capturing application which does not receive external data from partnered companies and therefore does not use ONS. However in future Accada release they plan on integrating this service. Accada's capturing application allows for multiple subscriptions to one or more filtering and collection instances. For each type of subscription a simple template will be made to transform every ALE event from the filtering and collection middleware into a single EPCIS event that will later be stored in the relational database through the EPCIS repository. Accada has facilitated the use of the capturing application by providing a graphical user interface

EPCIS repository

In simple terms, the EPCIS repository is used to store EPCIS events that have been captured. This is done by creating an EPC compliant network interface between the relational database and the capturing and accessing applications. The interfaces used by the repository are the capturing and query interfaces. The capturing interface provides a path to transfer EPCIS events between the capturing application and other roles that require it such as the EPCIS repository and the internal/external accessing applications. This is done by using a TCP/HTTP connection between the capturing application and the repository to transfer information. The query interface is used to transfer queries between the EPCIS repository and internal/external accessing applications and returns the results. This is done by using a SOAP protocol between the two to pass and return the needed information. Both interfaces also use a TCP/HTTP connection for the notification channel. Currently Accada uses MySQL as means to create their relational database which is linked to the EPCIS repository.

EPCIS accessing application

The accessing application is the main software that carries out the overall business processes such as shipping and receiving, warehouse management, and relaying historical EPCIS data to partner companies. Since this is not a part of the general middleware it is not included in the Accada software, however it can be implemented. If there is trust between two companies they may grant minimal access to each others accessing application. With this, proper EPC business information can be accessed and can be applied to the internal EPCIS repository. As previously described in the discovery service we access the company's external application by first obtaining the address as to where this information is stored through ONS. Using this address we can access all the needed information associated with the EPC information from the partner's repository. Accada has included a client graphical user interface for easy access to the implemented accessing application.

Singularity: EPCIS

Singularity's EPCIS runs in a similar way to Accada by receiving the captured EPC information from the EPM through standard web-services like SOAP. The added feature included in Singularity is known as an Enterprise Service Bus (ESB). This ESB encapsulates the EPCISs of an enterprise to allow access throughout the system. Therefore a company that consists of multiple retail stores and/or multiple manufacturing buildings can then access EPCIS information from any location.

EPCIS threats

In the case of information service Accada, Singularity and other RFID framework support bindings such as SOAP/HTTP are used for authentication and authorization. This process includes authenticating the identity of the application issuing or requesting EPCIS data and from here we can authorize the application to access the information relevant to them. Although the bindings are supported by current RFID frameworks, EPCglobal leaves them as an optional feature and therefore do not need to be implemented. As mentioned by [1], without properly identifying applications accessing EPCIS information from the database we open the possibility to the previous threats occurring. Therefore in a worst case scenario our threat results will correlate with those found in the Discovery service.

Threat	Motivation	Difficulty	Likelihood	Impact	Risk
Spoofing of identity	High	Solvable	Possible	High	Critical
Tampering with data	Moderate	Solvable	Possible	Medium	Major
Repudiation	Moderate	Solvable	Possible	Medium	Major
Information disclosure	High	Solvable	Possible	High	Critical
Denial of service	Moderate	Solvable	Possible	Medium	Major
Elevation of privilege	High	Strong	Unlikely	High	Critical

Table 3: Information service threat analysis

Conclusion

By continuing with research development and adopting current features available to these frameworks we hope to apply the RFID technology to the supply chain and other areas with minimal risk to companies and end users. Recent research regarding security and privacy of RFID systems has brought great improvements towards real world applications. Implementations of various cryptographic algorithms such as SHA-256, SHA-1, MD5, AES-128, and ECC-192 have all been discussed in [6] to deal with the tag and reader relationship security issues. Solutions towards the Discovery service include such things as DNSSEC, TLS/SSL and VPNs.

In the near future RFID tags will be implemented into various items not only to be used to identify the product but also to offer ingenious services to the user. Imagine in a few years going over to your fridge and having it remind you that you are out of milk or buying a casserole dinner equipped with an RFID tag containing cooking instructions that can be appropriately handled by your oven or microwave. All of these innovative ideas are not too far off, we simply need to consider the risks involved and strategize ways to counteract against them.

References:

[1] Garcia-Alfaro, J., Barbeau, M., and Kranakis, E., Analysis of threats on EPC based RFID systems, *Carleton University*, *School of Computer Science*, 2007.

[2] Laurendeau, C. and Barbeau, M. Threats to Security in DSRC/WAVE. In: *5th International Conference on Ad-hoc Networks (ADHOC-NOW)*, 2006.

[3]Lehtonen, M., Michahelles, F., and Fleisch, E., Trust and Security in RFID-Based Product Authentication Systems, IEEE SYSTEMS JOURNAL, VOL. 1, NO. 2, DECEMBER 2007

[4] Floerkemeier, C., Roduner, C., and Lampe, M., RFID Application Development with the Accada Middleware Platform, IEEE SYSTEMS JOURNAL, VOL. X, NO. X, DECEMBER 2007

[5] Floerkemeier, C., Roduner, C., and Lampe, M., Facilitating RFID Development with the Accada Prototyping Platform, *Institute for Pervasive Computing*, *Department of Computer Science*, 2007

[6] Feldhofer, M., Wolkerstorfer, J., Strong Crypto for RFID Tags – A Comparison of Low-Power Hardware Implementations, *Institute for Applied Information Processing and Communications*, *Graz University of Technology*, IEEE, 2007

[7] EPC Information Services (EPCIS) Version 1.0.1 Specification, working draft, September 2007. [Online]. Available: http://www.EPCglobalinc.org/

[8] EPC - The Application Level Events (ALE) Specification, Version 1.1, Part I and II, September 2007. [Online]. Available: http://www.EPCglobalinc.org/

[9] The EPCglobal Architecture Framework version 1.2, September 2007. [Online]. Available: http://www.EPCglobalinc.org/

[10] EPCglobal Tag Data Translation (TDT) 1.0 Ratified Standard Specification., Jan 2006, [Online]. Available: http://www.EPCglobalinc.org/

[11] Low Level Reader Protocol (LLRP), Version 1.0.1., august 2007, [Online]. Available: http://www.EPCglobalinc.org/

[12] EPC Radio frequency identity protocols Class-1 Generation 2 UHF protocol for communications at 860 MHz - 960 MHz, version 1.1.0, [Online]. Available: http://www.EPCglobalinc.org/

[13] Reader Protocol Standard, Version 1.1, June 2006. [Online]. Available: http://www.EPCglobalinc.org/

[14] Ranasinghe, D., Cole, P. Confronting Security and Privacy Threats in Modern RFID Systems, *School of Electrical and Electronic Engineering, The University of Adelaide Auto-ID Lab*, 2006

[15] Konidala, D., Kim, W., and Kim, K., Security Assessment of EPCglobal Architecture Framework, *Auto-ID Labs White Paper WP-SWNET-017, 2007*

[16] Juels, A, Rivest, R., Szydlo, M., The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, *RSA Laboratories and Laboratory for Computer Science, MIT, 2003*

[17] Rieback, M. R., Crispo, B., and Tanembaum, A. S. Is your Cat Infected with a Computer Virus? In: *4th Ann. IEEE Int'l Conf. on Pervasive Computing and Communications (PERCOM)*, pp. 13–17, Italy, 2006.

[18] Sarma, S., Weis, S., and Engels, D., RFID Systems and Security and Privacy Implications, *Auto-ID Center*, 2003

[19] Ham, Y., Kim, N., Pyo, C., and Chung, J., A Study on Establishment of Secure RFID Network Using DNS Security Extension, *2005 Asia-Pacific Conference on Communications*, Perth, Western Australia, 3 - 5 October 2005.

[20] Brock, D., The Electronic Product Code (EPC) : A Naming Scheme for Physical Objects, *MIT auto-id center*, January 1, 2001

[21] The EPCglobal Network™ Demonstration, *EPCglobal Inc*, 2004

[22] Lee, H., and Kim, J., Privacy threats and issues in mobile RFID, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), 2006

[23] Brock, D., The Physical Markup Language: A Universal Language for Physical Objects, *Auto-ID Center*, 2001

[24] Organisation for Economic Co-operation and Development, RADIO FREQUENCY IDENTIFICATION (RFID): A FOCUS ON INFORMATION SECURITY AND PRIVACY, *DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY*, Jan 2008

[25] Ranasinghe, D., Engels, D., Cole, P., Low-Cost RFID Systems: Confronting Security and Privacy, *Auto-ID Labs*, 2006

[26] Floerkemeier, C., and Lampe, M., RFID middleware design – addressing application requirements and RFID constraints, *Institute for Pervasive Computing Department of Computer Science, 2006*

[27] Rose, T., Singularity Architecture, *I+konect*, Jan 12, 2006

[28] Rose, T., Singularity Middleware Design, *I+konect*, Jan 12, 2006

[29] Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., and Ribagorda, A, RFID Systems: A Survey on Security Threats and Proposed Solutions, Computer Science Department, Carlos III University of Madrid, 2006

[30] Oren, Y. and Shamir, A. Power analysis of RFIDtags. In: *Rump session of Advances in Cryptology*, *CRYPTO'2006*, 2006. [Online]. Available: http://www.wisdom.weizmann.ac.il/yossio/rfid/

[31] Haver, T., Security and Privacy in RFID Applications, *Master of Science in Communication Technology*, June 2006

[32] Smith, R., RFID: A Brief Technology Analysis, CTOnet.org, 2004

[33] Rieback, M., Simpson, P., Crispo, B., Tanenbaum, A., RFID malware: Design principles and examples, *Pervasive and Mobile Computing 2*, 2006

[34] Sachs, K., Guerrero, P., Cilia, M., RFID Seminar, *TU Darmstadt Dept. of Computer Science*, 2006

[35] Karthikeyan, S., and Nesterenko, M., RFID Security without Extensive Cryptography, *SASN'05*, November 7, 2005

[36] Thompson, D., Chaudhry, N., and Thompson, C., RFID SECURITY THREAT MODEL, *Department of Computer Science and Computer Engineering University of Arkansas*, 2003

[37] RFID zapper, [Online], https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html

[38] Thompson, D., Chaudhry, N., and Thompson, C., RFID Technical Tutorial and Threat Modeling Version 1.0, *Department of Computer Science and Computer Engineering University of Arkansas*, December 8, 2005

[39] Grunzke, R., Risk Analysis of the applied RFID System, Computer Science C-level thesis, Karlstad University, 2007

[40] Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J., and Song, S., AN APPROACH TO SECURITY AND PRIVACY OF RFID SYSTEM FOR SUPPLY CHAIN, *IBM China Research Lab*, 2004

[41] Juels, A, Minimalist Cryptography for Low-Cost RFID Tags, *RSA Laboratories*, 2003

[42] Fabian, B., Gunther, O., and Spiekermann, S., Security Analysis of the Object Name Service, *Institute of Information Systems Humboldt-University Berlin*

[43] Kost, S., An introduction to SQL injection attacks for Oracle developers, *Integrity*, 2007

[44] Choi, S. and Poon, C., An RFID-based Anti counterfeiting System, *IAENG International Journal of Computer Science*, Feb 2008

[45] Vajda, I., and Butty´an, L., Lightweight Authentication Protocols for Low-Cost RFID Tags, *Department of Telecommunications Budapest University of Technology and Economics*, 2003

[46] Vaudenay, S., RFID Privacy based on Public-Key Cryptography, *EPFL CH-1015 Lausanne*, *Switzerland*, 2007

[47] Cole, P., Ranasinghe, D., Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting, *Springer-Verlag Berlin Heidelberg*, 2008

[48] http://www.accada.org/

[49] http://singularity.firstopen.org/