Running head: Security Concerns Surrounding RFID Technology

Security Concerns Surrounding RFID Technology

Andrew B. Koerner

University of Nebraska-Lincoln

Abstract

The ever-increasing expansion and integration of RFID into nearly all aspects of modern living gives rise to the inherent need for security. RFID has practical applications in logistics, product tracking, vehicle tracking, asset tracking and also Separation of Privileges to name a few. With the multitude of applications it is important to insure secure data transactions.

Security Concerns Surrounding RFID

Introduction

The predecessor to modern Radio Frequency Identification (RFID) first appeared in the advent of World War II. Then known as Identification Friend or Foe (IFF) it was used to positively identify aircraft, vehicles and forces. This technology was technically limited to only the positive identification of a friendly force by means of a transponder and was unable to identify a foe. Radio Frequency Identification technology has met practical application in many aspects of modern life. RFID technology has heavy use in logistics, tracking packages and company assets. Data loggers have also been equipped with RFID technology to track such thing as temperature, pressure etcetera.

The possible applications for RFID technology are limitless and exciting. RIFD technology is thought to be the barcode of the future (Dimitriou, 2008). The shear nature of RFID in the basis that it is wireless communication gives rise to the possibility of abuse by attackers. RFID technology enables the transfer of simple unique identification numbers or large amounts of dynamically generated data e.g., temperature data loggers will dynamically generate data. The security threats present by the transmission coupled with the enticing data content leaves RFID a likely and potential target for attack.

It is the scope of this paper to first outline the basic

functionality of a RFID enabled network. This includes necessary devices and basic network topology. Secondly, in the most basic application the protocol behind RFID communication and how it is conducted will be outlined. To understand the threats being faced by RFID technology the basic functionality and operation of RFID technology must first be understood. Finally, various possible threats will be discussed in length and attack scenarios will be presented.

RFID Primer

RFID transmission medium

RFID stands for Radio Frequency Identification and by name implements and relies on the radio band for the transmission of data. Radio refers to the electromagnetic spectrum lower then roughly 300 GHz and a wavelength of greater then roughly 1mm. Radio communication and data transmission occurs on a very broad spectrum however RIFD transmission medium resides within a few spectrums. The FCC within the United States and equivalent regularity commissions in other countries govern radio transmissions. Most RFID communication and transmissions occur in the kilohertz or radio Very High Frequency (VHF) Range from 30 MHz to 300 MHz.

RFID contains three general bands:

- Low Frequency (LF) @ 125 KHz – 134
- High Frequency (HF) @ 13.56 MHz
- Ultra High Frequency (UHF) @ 860 MHz – 930 MHz

There are however slight variations on frequency depending on

local sovereignty or governmental policy. Each band or frequency is unique in physical transmission properties and limitations. The physical properties of the band influence power transmission levels and device antenna geometry i.e., length, diameter and transmission range. The band and transmission properties of said band remain an important security topic because it is important to know the effective transmission range of a particular RFID device. Radio communications is inherently unpredictable; signals can be absorbed or reflected by various materials.

RFID Devices

RFID technology in the most basic sense is comprised of two devices The RFID Tag/Label and Interrogator/Reader. The RFID Tag is an electronic device containing an antenna, memory and has the ability to transmit or receive data. Tags come in three flavors or verities active, passive and semi-passive. Passive, the most inexpensive and widely used is powered by the radio waves created by the interrogator/reader. The principal used for power generation in a passive RFID chip is Near Field. Near Field by name implies that the RFID Tag must be near the reader (typically < 3m).

Passive RFID tags do not contain a power supply and thus require the presence of the electromagnetic field generated by the reader to power the device (See Figure 1). The second type of RFID tag is an active tag. Active tags are identical in makeup to the passive tag with the only disguising factor being

the integrated power supply. Active RFID tags have an integrated power supply and do not require the Near Field to operate. This enables the active tags to function at a much larger distance then that of the passive tags. Active tags are typically more expensive and only used for specialized applications (see Figure 2).

The final type of RFID tag is the semi-passive RFID tag. Semi-passive tags are identical to passive tags with the only difference being onboard memory power supply. The semi-passive power supply only powers the memory the remaining circuitry is powered by the integrated resonant supply and the Near Field (see Figure 3).

The final device required to form an RFID network is the interrogator or reader. The interrogator is a radio transceiver and has the middleware, software that controls and interprets data presented from tags (see Figure 4).

RFID tags are capable of carrying bytes to megabytes of data depending on the application. Active tags are capable of carrying more data then that of passive and the primary reason for semi-passive tags is to increase the amount of data storage.

RFID tags are capable of carrying any data including SQL queries and product data. Electronic Product Code is a standardized means of unique identification to categorize and identify every physical object anywhere in the world and has 2^96 possible codes (see figure 4). EPC enabled RFID tags are known as EPC tags and hold a EPC compliant data payload.

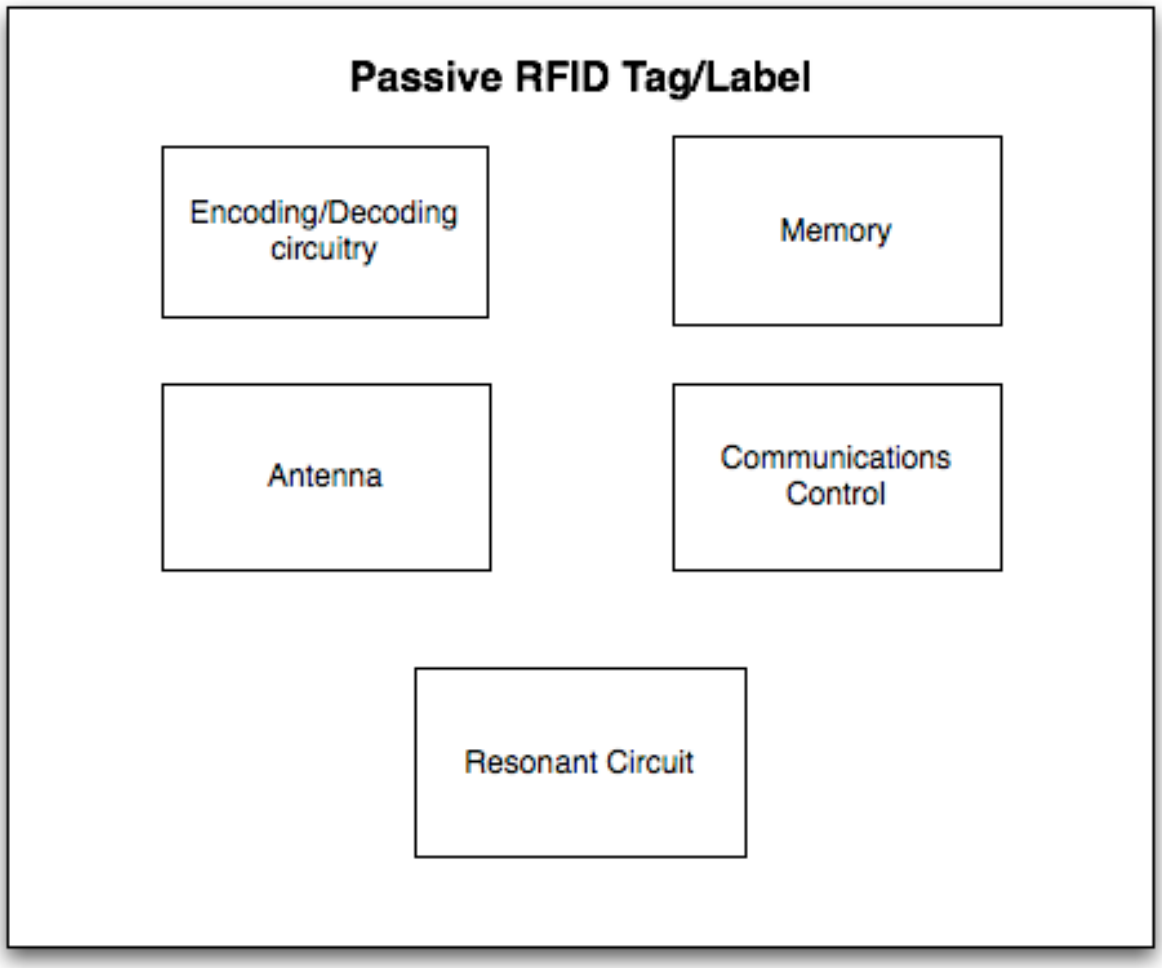
Passive RFID Tag/Label
Encoding/Decoding circuitry
Memory
Antenna
Communications Control
Resonant Circuit

Figure 1

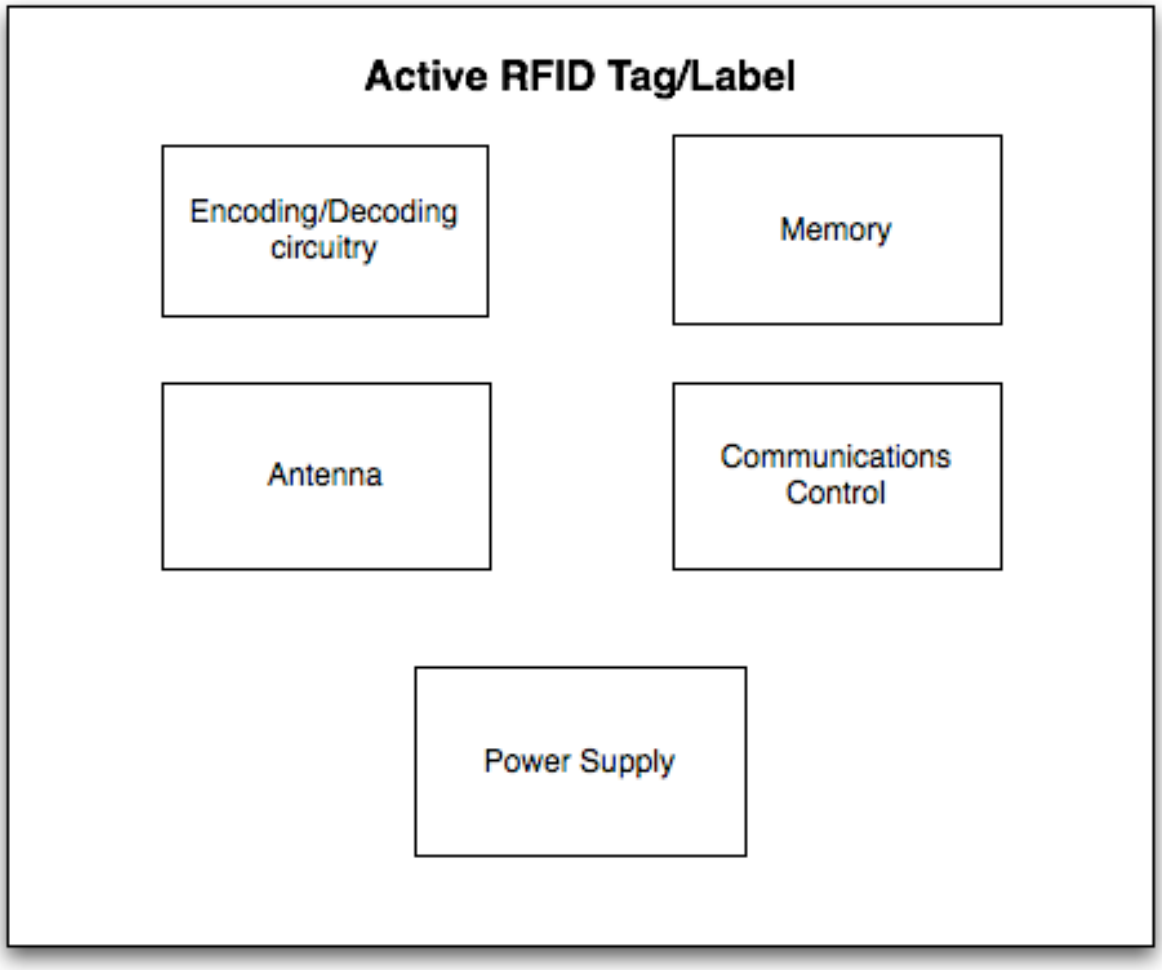
Active RFID Tag/Label
Encoding/Decoding circuitry
Memory
Antenna
Communications Control
Power Supply

Figure 2

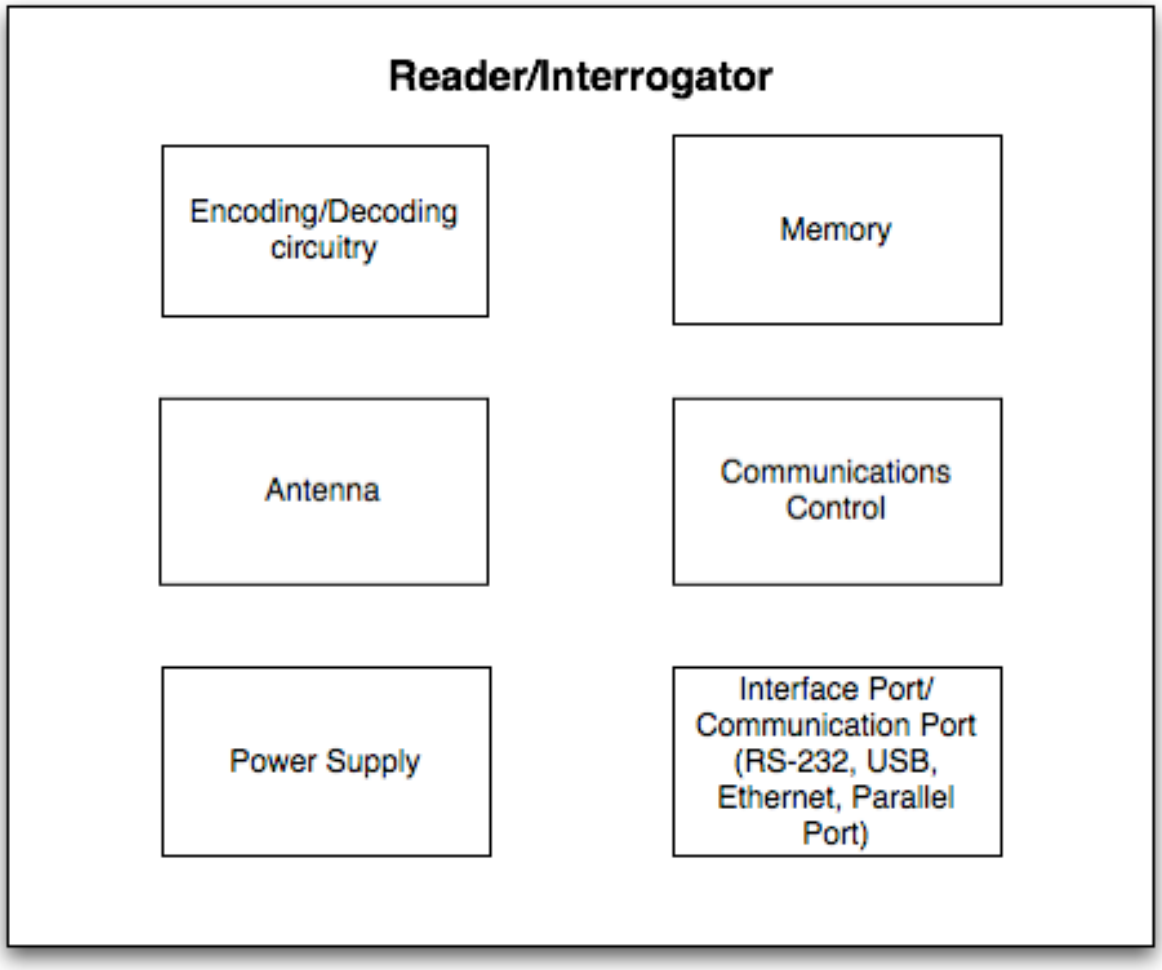
Reader/Interrogator
Encoding/Decoding circuitry
Memory
Antenna
Communications Control
Power Supply
Interface Port/ Communication Port (RS-232, USB, Ethernet, Parallel Port)

Figure 3

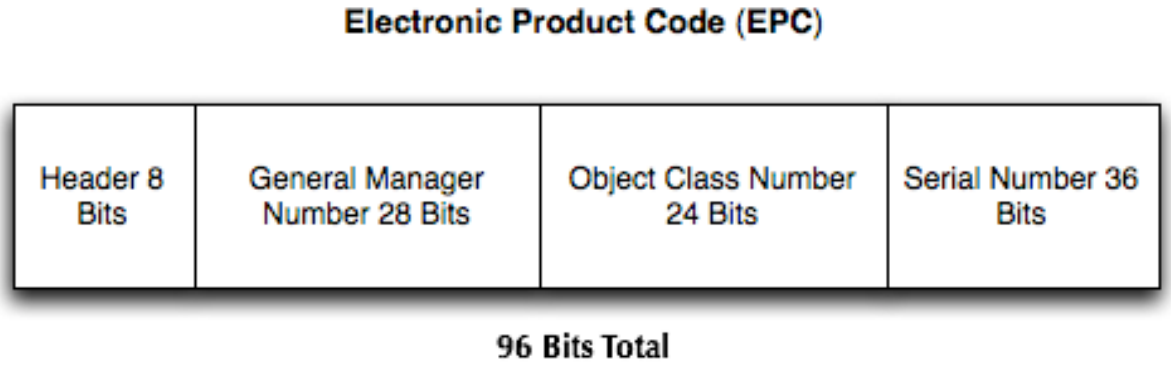
Electronic Product Code (EPC)
Header 8 Bits
General Manager Number 28 Bits
Object Class Number 24 Bits
Serial Number 36 Bits
96 Bits Total

Figure 4

The RFID Network

An RFID network is comprised of four main parts. The RFID reader/interrogator is responsible for sensing the presence of a RFID tag and querying the data. The second element of an RFID network is the middleware.

The middleware is a software layer responsible for interpreting data presented from a tag. Such responsibilities include: input sanitation, resource allocation and data processing. The backend/middleware layer can do all of the tasks listed and more depending on the particular application. The middleware is also responsible for database CRUD and running queries against the database. The database element to an RFID network is responsible for storing additional data pertaining to an RFID tag. An example of data that could be stored being product data. The product id number is received by the reader/interrogator and a query is formed by the middleware. If the product ID = 101 an example query submitted could look like “Select * From Products Where id = ?”. Subsequently the submitted query would look like “Select * From Products Where id = 101” and the database could respond with product data that could include product name, expiration date etcetera.

The final necessary element of an RFID network is the tag/label. The tag/label is responsible for storing data pertaining to the object in which the tag represents. Examples of this could be a passport, NUID card, pet id chip, product

identification tag and many other possible applications. The tag/label can store a simple identification number or megabytes of complex data. Refer to (Figure 5) for an illustrated diagram of RFID network architecture.

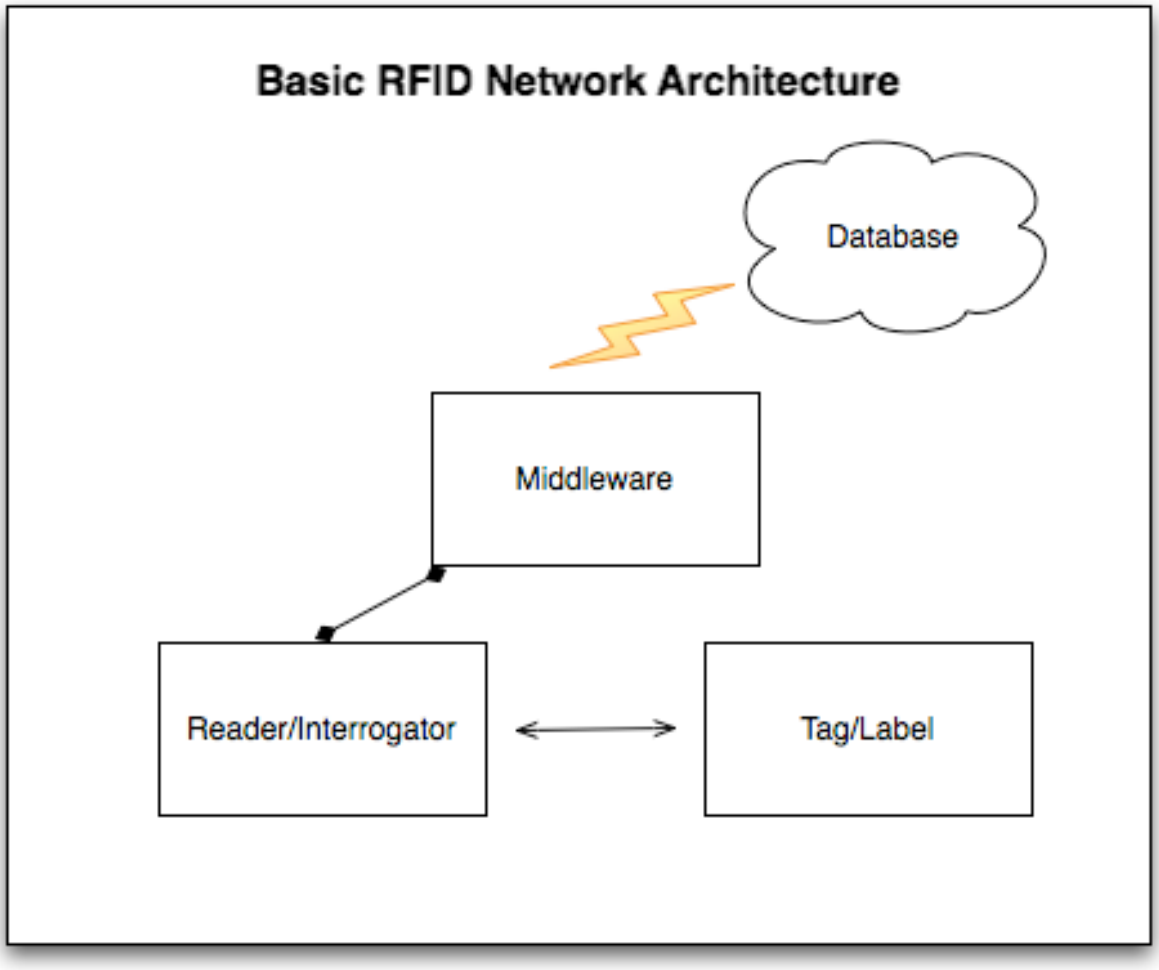
Basic RFID Network Architecture
Database
Middleware
Reader/Interrogator
Tag/Label

Figure 5

Network architecture for passive, semi-passive and active RFID tags is identical however the limiting factor being the effective range of the tag from the reader. Passive tags must be within the Near Field and store markedly less data then active or semi-passive tags. The range of the Near Field of a particular RFID network is determined by the frequency or band that the network is function on refer to (Figure 6) for an illustrated example of active verses passive RFID network.

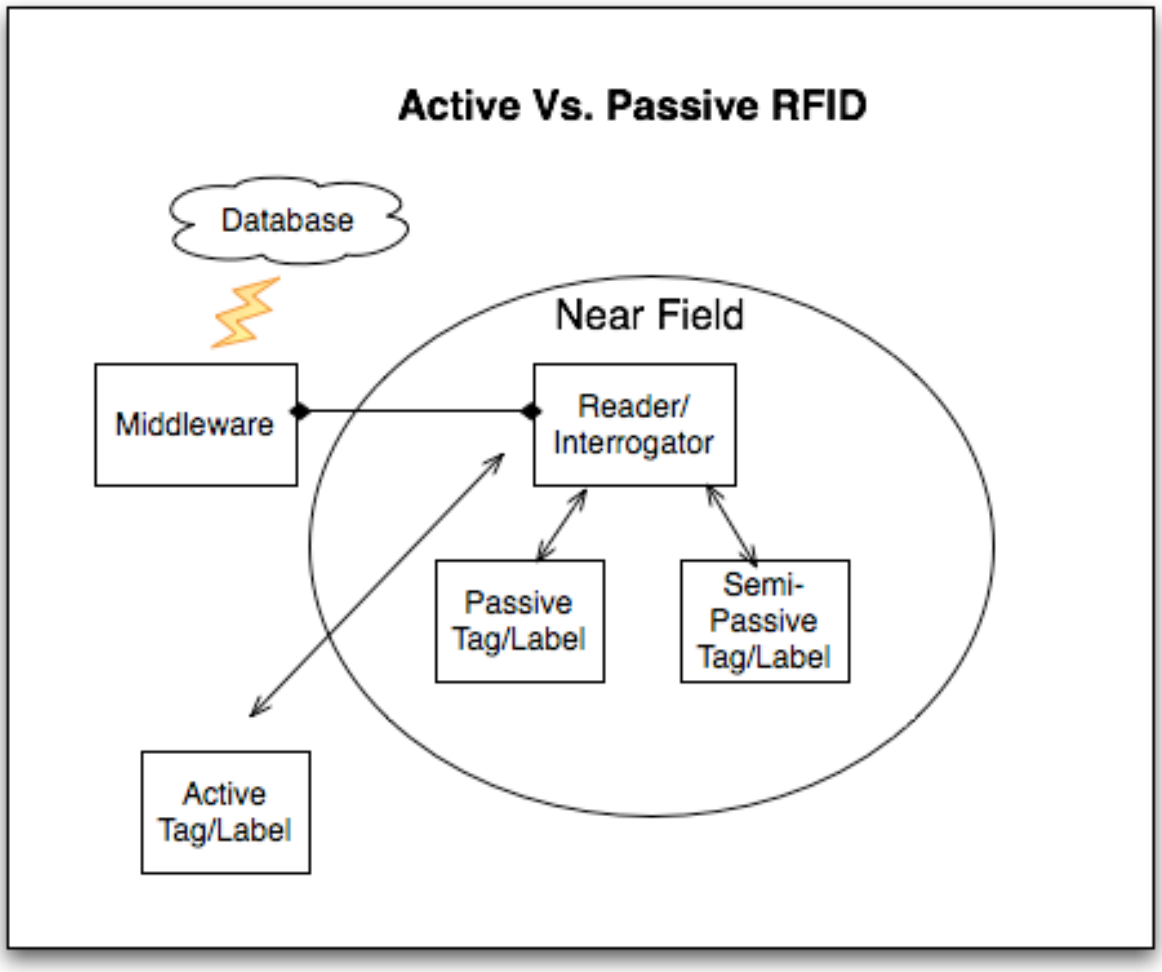
Active Vs. Passive RFID
Database
Near Field
Middleware
Reader/
Interrogator
Passive
Tag/Label
Semi-
Passive
Tag/Label
Active
Tag/Label

Figure 6

Communication Exchange

In brief the RFID communication exchange begins with a read cycle or dis. Read cycles occur faster then data is needed. A read cycle is when all tags within the vicinity of the RFID reader/interrogator are queried. Read cycles occur at a relative high frequency and under most applications an RFID tag must be present within range of the reader for several cycles before acknowledgement. Once acknowledged the reader sends out a query for each read cycle the tag is present for. The RFID tag then responds with a payload of data. RFID tags can respond with different data for subsequent read cycles. Depending on the number of cycles present the tag could present different data for each cycle.

RFID Security

Types of Attacks

In RFID technology there are two broad categories of security attacks. The first category of attack is a direct alteration or manipulation of data within the database. This can be accomplished by compromising the middleware. The second class of attack aims solely on the alteration of data on a tag. This can be for the intention of cloning a tag, inserting data on a tag or deleting data on a tag. With this class of attack the data within the database is uncompromised, left unaltered and intact.

Given the type of data RFID tags are capable of storing under the proper application a RFID network can be subject to

SQL(Structured Query Language) injection attacks. A SQL injection attack would fall under the first category of attacks with the intention of altering the database. This form of attack is possible by weaknesses within the middleware specifically involving input validation and sanitation.

Suppose the middleware formulates a SQL query for an item as follows “Select * From Products Where id = ‘<RFID tag data>’” and middleware fails to properly sanitize the RFID tag input data. The RFID tag scanned holds the following data ”101'; Drop Table Products; --”. The resulting query submitted to the database by the middleware would be “Select * From Products Where id = ‘101'; Drop Table Products; --’”. The compromised query would result in a table being dropped within the database making the data inaccessible. This example is overly simplified however under the same methodology an attack could be orchestrated in this manner. The prevention of this type of attack occurs at the middleware level with thoroughly checking and sanitizing input data.

A second form of RFID attacks known as cloning or spoofing of tags effectively creates an identical tag. This would be advantageous for Elevation of Privileges or Masquerading types of attacks. Tag spoofing would fall under the second class of RFID attacks by manipulation of data on a tag. Cloning product tags could result in the attacker being awarded a lesser value for an item in a retail environment.

A possible example, a retail electronics store has a coffee maker priced at $20.00 and an alarm clock priced at $10.00. A

would-be attacker could clone the contents of the RFID tag on the alarm clock and place it on the coffee maker. The attacker then would be awarded the lesser value of $10.00 for the more expensive item. Implementing hashing, encryption and intelligent middleware filtering can effectively squelch this form of attack. In the previous example the alarm clock was cloned with proper middleware filtering this could be prevented. If there is a sensor or RFID reader on the shelf sensing the presence of the alarm clock and said attacker tries to buy that alarm clock a flag should be thrown. The alarm clock cannot be in two locations at once. This is a simple countermeasure to prevent the cloning of RFID tags in this particular application.

RFID networks are subject to Denial of Service attacks. This form of attack could be manifest by flooding a reader with data. The data could be invalid or bad data but the intent is to overload the reader with illegitimate tags/data such that legitimate data cannot be read. If a large number of tags with bunk data are all presented with a short timespan the result could be a crashed system.

Attack Scenarios

Scenario 1:

- Joe Blow is a UNL student with a valid NUID card.
- Joe has a friend named Darth that is not a UNL student and does not have a valid NUID card.
- Joe Blow is registered in the College of Engineering and thus his card is valid to gain access to the engineering

building.

- Darth uses a RFID reader to gain the data on Joe's card without Joes knowledge.
- Darth then uses that data to create a copy of Joe's NUID card.
- Darth now has access to the engineering building effetely applying Elevation of Privileges.

Scenario 2:

- Tom Foolery is an employee for a local food distribution center.
- Tom is responsible for managing inventory.
- Wile on break Tom replaces a legitimate RFID tag on an item with a malware infected RFID.
- The malware tag utilizes a known flaw in the input sanitation within the middleware to preform a SQL injection attack.
- The result being inaccessible data and halted distribution.

Conclusion

RFID technology is increasing in application. The advent of faster more secure RFID networks the practical uses of RFID technology will increase. Security is an important concern when dealing with the transmission of data. The necessary countermeasures and precautions required to ensure security are

application specific and must be considered. When designing a RFID network application specific risk and threat assessment must be given thought.

References

Thornton, F, Haines, B, M., A, Bhargava, H, Campbell, A, & Kleinschmidt, J. (2006). Rfid security. Syngress Media Inc.Kleinschmidt, J. (2006). Rfid security. Syngress Media Inc.

Dimitriou, T. (2008). RFID Security and privacy. (2008). Rfid security: techniques, protocols 57 and system-on-chip design. Athens, Greece: Springer Science+Business Media, LLC.

Thompson, D.R., Chaudhry, N., & Thompson, C.W. (n.d.). Rfid security threat model. Unpublished manuscript, Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas. Retrieved from http://comp.uark.edu/~drt/index.php