Jordan University of Science and Technology

Faculty of Computer And I.T

Department Of Computer Engineering

Security and Network Management

CPE542 Project

Security over the RFID

By:
Mohammad H. Al Malkawi 20010171062

Ashraf M. Abussaud 20010171071

Handled to:
Dr. Loa’i Tawalbeh
# Table of Contents:

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents:</td>
<td>2</td>
</tr>
<tr>
<td>Table of Figures:</td>
<td>3</td>
</tr>
<tr>
<td>I. Introduction</td>
<td>4</td>
</tr>
<tr>
<td>II. RFID and its Applications:</td>
<td>5</td>
</tr>
<tr>
<td>III. RFID Security Issues:</td>
<td>8</td>
</tr>
<tr>
<td>III.a Privacy and Security Threats:</td>
<td>8</td>
</tr>
<tr>
<td>III.b Proposed Solutions</td>
<td>9</td>
</tr>
<tr>
<td>IV. RFID Right to Know Act of 2003</td>
<td>14</td>
</tr>
<tr>
<td>V. Future of RFID</td>
<td>15</td>
</tr>
<tr>
<td>VI. Conclusion</td>
<td>16</td>
</tr>
<tr>
<td>Appendix A: (RFID Right to Know Act of 2003)</td>
<td>17</td>
</tr>
</tbody>
</table>
Table of Figures:

Figure 1: RFID System ........................................................................................................... 5
Figure 2: RFID System Deployment .................................................................................... 7
I. Introduction

RFID (Radio Frequency IDentification) is one of recent advances in technology that was invented to replace the traditional Bar Codes which were used to identify products for more than 50 years. However, this technology has much wider potential use than Bar codes in identifying items and can be used in wider applications.

Basically, this technology uses small integrated microchips attached to antennas that are hidden in the items to be identified. Each chip carries a unique 96-bit ID that identifies the item. Each of these chips is connected to an antenna that senses electromagnetic energy that is generated by the RFID readers. In response to sensing this energy, the chip will transmit its unique ID to the reader device. The range of RFID operation is between 5 cm or less and 10 meters.

RFID is not simply a newer version of Bar Codes but much more than that, although it can virtually replace it. The two technologies differ in the following ways:

1. Bar Codes identify the category of a product (e.g. every family of optical mice from Microsoft holds the same Bar code that identifies the family not the specific optical mouse). However, RFID can identify each item by itself since it links every item with a unique ID and this can yield to privacy intrusion.

2. Bar Codes need a short-distance line of sight between the reader and the tag whereas in RFID the reader can read the tag from a distance without being noticed by the person carrying the RFID-tagged item.

3. Since Bar Codes do not transmit any electromagnetic energy they are safe for health. On the other hand, RFID might be harmful for health in the long run since there will be a continue exposure to electromagnetic energy.

RFID technology is deployed by major companies such as Phillip Morris and Wal-Mart. One of the famous products that carry RFID tags is the Gillette shaving razors. That encouraged more research on RFID research and development. Nowadays, it is possible to print the RFID chip and thus they can be hidden along with their antennas. Therefore, it is almost impossible for consumers to recognize that the items they buy are RFID-tagged or not.
II. RFID and its Applications:

RFID is not just a product that is deployed intensively in the market. RFID is a well-defined Technology that uses radio waves for Products Identification or even tracking of mobile products.

RFID like any other technology consists of:
- The Idea behind the Technology which is here the Radio wave usage.
- The Standards that control the RFID usage.
- The Theory behind the RFID which include: Low power consumption and the ability for mobile tagging.

Any deployed RFID system must consist of:
- RFID Database.
- RFID Reader Device.
- Multiple of RFID Tags.

![Figure1: RFID System.](image)

Recent reports on RFID systems showed that the technology has already been massively deployed throughout the US and much of the industrialized world. In November 2003, the executive vice president for Philips Semiconductors said that Phillips had shipped more than a billion RFID Devices to the US and the European market.

Some RFID researchers estimate that between 20 and 50 million Americans carry an RFID chip in their pocket every day - either in the form of a proximity card for entering buildings and garages or in an automobile key with an “immobilizer” chip embedded into the key’s plastic handle.
An RFID system can be deployed and used in variety of fields and application such as:

**Automobile immobilizers:**

In such a system we use an RFID tag as the car key and an RFID reader as the car key lock, thereby once you get near the car, the RFID recognition and authentication of your RFID tag will unlock the car.

These tags are usually programmed and set at the factory in a mode that will not let you to rewrite them in the field. We may have some versions which include cryptographic communications between the key and the reader. The Immobilizers can be used for these functions typically have a small read range (typically 5 cm) and operate in the low-frequency end of the electromagnetic spectrum (between 125 and 134.2 KHz), and costs a few dollars each.

**Payment systems:**

We can use the RFID tags as credit card. They will act like payment identifiers that contain a unique serial number related to a bank account. These tags will be identified to an appropriate tag reader which in turn sends the serial number over a network to a remote computer that debits the value from the customer’s account depending on the customer’s receipt.

This technology is used in Speedpass pay-at-the-pump system (Speedpass is developed by Texas Instruments) and in Mobil stations in the mid-1990s. Several years ago, the European Central Bank suggested considered embedding RFID tags into currency.

**Inventory management:**

The RFID tags can be attached to every item in the warehouse, each RFID will contain a unique serial number that completely identifies its item thus the inventory management is just one RFID reader that will read all the tags and add them to the Inventory Database. It can be added easily to monitor the movement of tags either entering or leaving the warehouse and it will update the warehouse inventory Database.

DHL used such a system by individually serialized tracking items by tags that are already being attached to some consumer packages and then used to track packages as they get on the truck, travel by boat, arrive in a foreign country, leave the boat, enter the supply chain, travel through distribution, and eventually reach their DHL Delivery destinations.

RFID Tags can also assure that products produced and sold in one market are not illegally diverted to another. Further, smart shelves equipped with RFID readers could integrate with inventory systems, tracking all merchandise and alerting store
personnel when items are out of order. RFID tags might even be used after the sale, for example, to ensure that consumers actually bought them.

There are also a lot of applications such as:

- Libraries (Santa Clara Library, University of Nevada, etc.)
- Anti-counterfeiting
- Pets identification
- Recycling Monitoring.
- Sensor networks (Michelin’s tyres, etc.)
- Localization of people (Amusement parks, etc.)

As we have seen above RFID as technology can be called a gift because it will make our life easier and smother, thus it was mapped to many applications. But like any other reliable systems the RFID system must support an acceptable degree of security in the users and the system sides i.e. the system Database must be secure to any outside intrusion and the users must interact with the system in a secure manner, which assure that no other third part can spoof on it.

In this manner we can develop an RFID system which is secure and reliable even though that the RFID by inheritance was designed for purposes which may invade our privacy directly in certain aspects like tracking and remote recognition and identification.

Finally, this paper will focus in the on RFID as technology and how to develop a secure RFID system even if it is aimed for tracking or Identification.
III. RFID Security Issues:
III.a Privacy and Security Threats:

Although RFID technology has provided us with many security benefits such as key-less entry systems, it is vulnerable to many privacy and security threats. For this technology to succeed and gain universal deployment, these threats must be addressed. RFID systems rely on RF communication which doesn’t require a line of sight communication. Therefore, the person carrying an RFID-tagged item can not physically stop communication with the tag and can’t even notice that such communication is taking place.

The RFID tags must not identify their holders because people’s privacy is the most important consideration. Also, the RFID tags should not send any meaningful information to unauthorized RFID readers. When discussing the security issues related to RFID technology, one must remember that the RFID tags have limited capabilities due to their low-cost design and thus they suffer from limitation in their crypto capabilities since most encryption and authentication algorithms are computationally-intensive.

By far, no RFID security breach is recorded even though that it has been used in many products such as the shaving blades of Gillette. However, there are many potential privacy and security violations that might be exploited by attackers to compromise systems’ security and invade people’s privacy.

One basic problem with current tags is that they can not distinguish between authorized and unauthorized readers so they respond to every reader. Another problem is that the readers can not distinguish between tags they are authorized to identify and those they are not. These two problems challenge the privacy and security of RFID technology and require implementing authentication algorithms.

Most of the privacy threats result from associating unique-ID tags with a person’s identity. So, when an individual buys an item that has an RFID tag the individual’s identity is linked to the serial number of the RFID tag. So, such an individual can be monitored and the individual’s locations can be determined by a spying agency by knowing this association between the individual and RFID-tagged item. Although the exact identity of the individual is not known by one association, this method exposes so much information about the customers and their preferences such as the product types and their prices. So, a thief carrying an unauthorized RFID reader can know the value of the items that a person is carrying and if the monetary value of the items is high, the thief might attack this person.

As an individual buys more RFID-tagged items these information are associated with his/her identity in some spying agents’ database. Suppose that the individual discards one of these items and someone else picks it up and perform a crime with it. The identity of the person associated with this item will still be that of the original owner who would then be faced with the investigation authorities and will be accused for committing
the crime. This problem is due to the association between the individual and RFID-tagged items.

One more threat, known as the cloning threat, is that it is theoretically possible to clone an RFID tag. This is a serious problem because RFID tags are currently used in key-less entry systems and some payment cards so by cloning an RFID tag the attacker can impersonate the victim and get access to the victim’s properties and bank accounts.

On the corporate level, the attacker can compromise the corporate infrastructure if the attacker knows that the corporate infrastructure is dependent on RFID for critical operations. The attacker jams the radio frequency signals in the RFID band and this is a Denial-of-Service (DoS) attack that can bring the whole system down.

Another security violation is possible by impersonation of tags. An authorized reader tries to read an RFID-tagged item but the response is received from the attacker’s tag. This violation is possible if the information sent by the tag is static since it will be easier to break by the attacker. For example, an attacker in a supermarket can buy expensive items with an impersonated tag that has a lower-price entry.

If the transmission between the tag and the reader is not secured by encryption then eavesdropping becomes possible by regular wireless Sniffers. This is a major problem if the serial number associated with a tag is static.

III.b Proposed Solutions

The following is a list of proposed solutions for the RFID technology privacy and security issues:

1. Tag Deactivation

This method works by killing the tag at the point of sale to prevent tracking holders of the RFID-tagged item. The reader at the checkout point sends a KILL (also known as Self Destruct) command to the tag to destroy the tag permanently. The basic principle behind this is that killed tags can not communicate with readers and thus can not violate the individual’s privacy.

Tag deactivation definitely protects customers’ privacy but has several problems. First of all, it is not suitable within a supply chain because the tag will be read at multiple stages of the chain – it can be used at the end of the chain only. Also, tags might have a value to customers after the point of sale. For instance, these tags allow item returns easily. Major companies are currently producing products to assist blind people in identifying RFID-tagged items contents in the home so items tags should not be killed for these products to work. Moreover, sophisticated RFID-enabled consumer appliances are already in the market – there are refrigerators that can identify expired food items by
scanning the items’ tags. One more example is the libraries that have started using RFID tags to identify their books (e.g. San Francisco Public Library) can not use this method because if the tag is deactivated when a book is checked out it can not be reactivated it when it is checked in.

2. User Intervention

In this method the user must press a button on the tag to authorize the RFID reader to scan it. This method clearly solves the unauthorized readers’ issue and thus eliminates spying. However, eavesdropped on authorized scan is still possible. Also, this method is not possible within a supply chain since no user-intervention is possible. It also makes the operation of the system more complicated.

3. Encryption

Cryptographic algorithms can be used to encrypt a tag’s serial number and store the encrypted serial number in the tag’s microchip. However, there are some issues that must be examined. Firstly, for this method to work the key management and distribution must be defined and designed carefully. Secondly, the encryption method doesn’t solve the tracking problem because the ciphertext of the serial number is unique and can identify the holder.

Encryption can help in authenticating the reader if public-key algorithms were used. The tag will communicate with the reader by encrypting its serial number with the public key of the authorized reader so the reader can decrypt the serial number only if it has the privilege to do so by using the appropriate private key. However, since this requires a lot of computations it is very difficult to carry out on cheap RFID tags. As emphasized earlier, the market demands using low-cost RFID tags to make this technology gain wide deployment.

Private-key algorithms can be used to do the encryption but they will complicate the operation since distributing the private key is a practical challenge and is vulnerable to many attacks.

4. Tag Passwords

Every tag has a password and will not send its serial number until it receives the correct password from the reader. The problem here is that the reader can not know which password to send because it does know the identity (serial number) of the tag! However, this method can be effective if a group password is used. For instance, a shop can make all its items’ tags have the same password so only the shop’s readers can communicate with these items successfully. This way the customer’s privacy is protected because no other reader on the way home can track the customer. But if the tag needs to be read by different readers as the case of the blind-assistant then this method will not work.
5. Tag pseudonyms

In this method a tag has a set of uncorrelated serial numbers and the tag would cycle through them after each communication with the reader. This method makes the unauthorized reader’s job more difficult because the unauthorized reader can not know that these serial numbers belong to the same tag or not. Only the authorized reader has a list of the tag’s serial numbers. Attackers can read the same tag a large number of times to make it go over all its serial numbers. However, this type of attack can be prevented by making the tag change its serial number periodically (e.g. every 10 minutes) rather than immediately after the read operation is completed. This makes it almost impossible for the attacker to obtain all the serial numbers of a tag in a reasonable amount of time.

6. Blocker Tags

This method doesn’t modify the contents of the tags. It creates an unsuitable environment for RFID readers. The block tag is a specially design RFID tag that prevents unauthorized readers to read tags.

If more one tag transmits its serial number to the reader at the same time a collision will occur and the reader will not be able to read any of the serial numbers and basically this is the idea used by the Blocker Tags. So, a blocker performs a Denial-of-Service (DOS) attack to prevent all RFID readers from reading any tag in the Blocker tag protection zone. A Blocker tag makes the readers think that all possible tags in the world are present besides them and that makes them fail to operate. Therefore, a blocker tag can be carried by a customer who wants to protect the RFID-tagged items that he/she is carrying from being read.

The bad thing about this method is that a thief carrying a Blocker tag can compromise a shop’s security and steal items without being caught since the RFID-readers will not be able to detect the unchecked-out stolen items when the thief leaves the shop.

7. Hashing

A one-way hash function can be implemented with fewer resources than that required for encryption algorithms. The tag will contain a special memory location allocated for the hash function output. In this method, a tag can be in one of two states: locked or unlocked state. In the unlocked state, the tag is fully functional and can communicate with any reader within its region of operation.

The owner of the tag can lock it by calculating the hash value of some randomly generated key and transmit this value to the tag. This lock value is stored in the tag’s memory. When the tag is in the locked state it replies to all requests from any reader with the stored hash value. All the functionalities of the tag are disabled while the tag is in the
locked state. The tag can be unlocked only if the owner of the tag sends the key that was used to compute the hash value. The tag computes the hash value of the key using the same one-way function and compares the result with the value that was used to lock the tag. If the two values match, the tag is unlocked.

The tag replies to readers whether it is in the locked state or not. The difference is in the form of the reply. If it is unlocked then the reply contains its serial number and if it is locked then it is its hash value. Therefore, the tag always announces its existence.

This method solves most of the privacy violation issues associated with the RFID technology. Only the authorized readers who hold the unlock key can get access to the tag’s contents. It is better to periodically unlock locked tags and then relock them with different keys because otherwise the attacker can track the association between the tag and its holder since the tag’s reply will be the same hash value over and over.

By using hashing, one can authenticate the RFID readers but doesn’t address tag authentication because of the low-cost requirement of these tags. Tag authentication is very important because a special type of attacker, known as man-in-the-middle attacker, can query the locked tag to get its hash value reply and then use this value to communicate with the tag’s authorized reader. The authorized reader will be fooled by this impersonation attack and will send the key to the attacker thinking that it is its associated tag. Afterward, the attacker can unlock the tag using this key. However, for this type of attack to work the attacker needs to have physical access to the legitimate readers.

8. Reader’s Signal-to-Noise ratio analysis

As the distance between the reader and the tag increases the Signal-to-Noise ratio will decrease because of fading, path loss and many other factors. Generally speaking, authorized readers are likely to be very close to the tagged-items so their Signal-to-Noise ratio is expected to be high whereas attackers’ readers are usually far away from the tagged-item and thus their Signal-to-Noise ratio is going to be low. Therefore, a tag can find a rough estimate of how far the reader is by analyzing the Signal-to-Noise ratio and act accordingly. If the reader is far away, the tag should provide little information and as the reader gets closer the tag can supply more information. This method is not very accurate since distance is not the only factor but it can protect the customers’ privacy to a large extent.

9. Public Policy Decisions

In addition to technical methods for solving the privacy and security threats of RFID technology, there is a need to regulate the use of technology using policies. Initially, there was proposal known as RFID Bill of Rights that suggested five principles for RFID deployment and these are as follows:
1. The right to known whether a product contains an RFID tag or not.
2. The right to have the RFID tag removed when the product is purchased.
3. The right to first-class RFID alternatives. Consumers should not lose other rights right if they decide to remove the RFID tag.
4. The right to know the information that is stored inside their RFID tags. If this information is incorrect, there must be some way to correct it.
5. The right to know when, where and why an RFID tag is being read.

The above proposal was mostly implemented by federal legislation to force labeling RFID-tagged items and consumer privacy protections. The legislation is known as the RFID Right to Know Act of 2003.
IV. RFID Right to Know Act of 2003

As we have seen in the security over RFID, if we want to develop a secure RFID system we must have the rules that specify the aspects of the RFID tags usage and to determine what is allowed and what is not allowed in all aspects concerned with the RFID Tags and RFID readers.

Thus there is a proposed federal legislation to mandate labeling of RFID-enabled products and consumer privacy protections

[Authored for CASPIAN by Zoe Davidson, Boston University Legislative Clinic]

This ACT is known as the “RFID Tight to Know ACT of 2003” see Appendix A for the full text of the ACT.

This ACT is simply a first step in managing the usage of RFID tags and which will be used in activating the RFID, which can be used to punish who misuse the RFID Technology in any aspect.
V. Future of RFID

As we have seen before RFID are in the evolving stages in its life cycle. They introduce to us a lot of facilities but with some threats and security issues. We have seen also the development of the RFID ACT which is the first step in making RFID usage legally and governed by government laws.

A lot of well know Societies such as RSA have started to develop cryptographic algorithms to enhance the security of the RFID tags against authorized RFID readers. As said by John Leyden - a writer at the Register Web site- :” RSA 2005 Cryptographic researchers are working out ways to make RFID technology more palatable to consumers ahead of its expected widespread deployment over the coming years.”

RFID technology will fit into the general landscape of geographically and identity-aware technologies that are currently being deployed. RFID, however, it will poses unique challenges because of its low cost and growing ubiquity.

As the awareness of RFID’s utility has grown, it will has the chorus of consumer activists urging that the technology’s deployment be delayed or abandoned. Increasingly, these activists have the ear of lawmakers. Unless RFID proponents can articulate a clear message that shows how RFID’s promise can be realized without sacrificing privacy, it’s possible that new regulations will significantly limit its usefulness.

The fact that the debate about RFID systems’ privacy and security is taking place far ahead of the actual ubiquitous deployment is a good sign. We’re hopeful that this debate will enable the evolution of both technology and policy in a reasoned manner, and will eventually allow the technology to be deployed without compromising personal privacy.
VI. Conclusion

RFID is a promising technology and is expected to revolutionize many industries if used properly. However, it identification properties need to be considered from the security and privacy perspectives to insure that systems based on this technology are not abused by malicious parties. There have been many proposed solutions for the security threats and if implemented careful it is expected that the level of security provided by RFID will substantially improve. There is no such a 100% threats-free system but a secure enough system is desirable.
Appendix A: (RFID Right to Know Act of 2003)

AN ACT

To require that commodities containing radio frequency identification tags bear labels stating that fact, to protect consumer privacy, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. SHORT TITLE.

This Act may be cited as the 'RFID Right to Know Act of 2003'.

SEC. 2. AMENDMENTS TO THE FAIR PACKAGING AND LABELING PROGRAM.

15 U.S.C. 1453 is amended--
(1) by inserting the following under subsection (a) paragraph (6):

'(7) A consumer commodity or package that contains or bears a radio frequency identification tag shall bear a label as provided in paragraph (9) of this subsection.

'(8) For purposes of paragraph (7) of this subsection the term "radio frequency identification" or "RFID" means technologies that use radio waves to automatically identify individual items; and the term "tag" means a microchip that is attached to an antenna and is able to transmit identification information.

'(9) A label required by paragraph (7) of this subsection shall:

'(A) state, at a minimum, that the consumer commodity or package contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and

'(B) be in a conspicuous type-size and location and in print that contrasts with the background against which it appears.'.

SEC. 3. AMENDMENTS TO THE FEDERAL FOOD, DRUG, AND COSMETIC ACT RELATING TO MISBRANDING.

21 U.S.C. 321 is amended--

(1) by inserting the following under subsection (mm):

'(nn) (1) The term "radio frequency identification" or "RFID" means technologies that use radio waves to automatically identify individual items.

'(2) The term "tag" means a microchip that is attached to an antenna and can transmit identification information.'.

21 U.S.C. 343 is amended--

(1) by inserting the following under subsection (v):

'(w) Radio Frequency Identification (RFID) Tags
'If the food or package contains an RFID tag, unless it bears a label

'(1) stating, at a minimum, that the consumer commodity or package contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and

'(2) in a conspicuous type-size and prominent location and in print that contrasts with the background against which it appears.'.

21 U.S.C. 352 is amended--

(1) by inserting the following under subsection (t):

'(u) Radio Frequency Identification (RFID) Tags

'If the drug or device or package contains an RFID tag unless it bears a label

'(1) stating, at a minimum, that the consumer commodity or package contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and

'(2) in a conspicuous type-size and prominent location and in print that contrasts with the background against which it appears.'.

21 U.S.C. 362 is amended--

(1) by inserting the following under subsection (f):

'(g) Radio Frequency Identification (RFID) Tags

'If the cosmetic or package contains an RFID tag unless it bears a label

'(1) stating, at a minimum, that the consumer commodity or package contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and

'(2) in a conspicuous type-size and prominent location and in print that contrasts with the background against which it appears.'.

SEC. 4. AMENDMENTS TO THE FEDERAL ALCOHOL ADMINISTRATION ACT.

27 U.S.C. Ch.8, Subch. II is amended--

(1) by inserting the following under section 215:

'§ 215a. Labeling requirement; radio frequency identification tags

'(a) Statement required on container

'A person shall not manufacture, import, or bottle for sale or distribution in the United States any alcoholic beverage unless its container bears a label:
'(1) stating, at a minimum, that container contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and

'(2) in a conspicuous type-size and prominent location and in print that contrasts with the background against which it appears.

'(b) The Secretary shall prescribe appropriate penalties for violations of this section.’.

SEC. 5. AMENDMENTS TO TITLE 15, CHAPTER 36--CIGARETTE LABELING AND ADVERTISING.

15 U.S.C. Ch.36 is amended--

(1) by inserting the following under section 1333:

'§ 1333a. Labeling requirement; radio frequency identification tags

'(a) Statement required on package

'A person shall not manufacture, import, or package for sale or distribution in the United States any cigarettes unless its package bears a label:

'(1) stating, at a minimum, that the package contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and

'(2) in a conspicuous type-size and prominent location and in print that contrasts with the background against which it appears.’.

'(b) The Secretary shall prescribe appropriate penalties for violations of this section.’.

SEC. 6. AMENDMENTS TO TITLE 15, CH. 94--PRIVACY.

15 U.S.C. Ch.94 is amended--

(1) by inserting the following under Subchapter II:

'SUBCHAPTER III--AGGREGATION OF NONPUBLIC PERSONAL INFORMATION AND RADIO FREQUENCY TAG IDENTIFICATION INFORMATION

'§ 6831. Privacy protection for consumers

'(a) (1) A business shall not combine or link an individual's nonpublic personal information with RFID tag identification information, beyond what is required to manage inventory.

'(2) A business shall not, directly or through an affiliate, disclose to a nonaffiliated third party an individual's nonpublic personal information in association with RFID tag identification information.

'(3) A business shall not, directly or through an affiliate or nonaffiliated third party, use RFID
tag identification information to identify an individual.

'(b) Safeguards

'The Federal Trade Commission shall establish appropriate standards for the businesses described in subsection (a) of this section--

'(1) to insure the integrity and confidentiality of an individual's records and information;

'(2) to insure that RFID tag records do not identify individuals;

'(3) to protect against anticipated threats or hazards to the security of an individual's records and information; and

'(4) to protect an individual against substantial harm or inconvenience, which may result from unauthorized access to or use of an individual's records and information.'.

'§ 6832. Consumer and Business Education

'(a) The Federal Trade Commission shall publish and disseminate documents with the purpose of educating the general public about RFID technology. The documents, at a minimum, shall describe RFID technology and how companies, marketers and government agencies can use RFID technology to collect an individual's nonpublic personal information.

'(b) The Federal Trade Commission shall publish and disseminate documents with the purpose of educating businesses about RFID technology and the importance of protecting an individual's privacy. The documents, at a minimum, shall describe RFID technology, advocate privacy protection, and explain how businesses must conform their actions to comply with the provisions of this Act.'.

'§ 6833. Relation to State laws

'A State may afford an individual greater protection than the protection provided under this subchapter.'.

'§ 6834. Rulemaking

'The Federal Trade Commission shall prescribe regulations necessary to carry out and enforce the mandate of this subchapter.'.

'§ 6835. Definitions

'(a) The term "radio frequency identification" or "RFID" means technologies that use radio waves to automatically identify individual items.

'(b) The term "tag" means a microchip that is attached to an antenna and can transmit identification information.

'(c) The term "business" means a corporation, partnership or other entity that collects or aggregates an individual's nonpublic personal information.
'(d) The term "nonpublic personal information" means information that a business can use to identify an individual. Such information includes, at a minimum, name, address, social security number, and financial data.'.
References


[2] T. Claburn, G.V. Hulme,” Security -- and its high cost -- appears to be the next hurdle in the widespread adoption of RFID.” Nov. 15, 2004
URL: http://www.informationweek.com/shared/printableArticle.jhtml?articleID=52601030


URL: http://www.theregister.co.uk/2005/02/18/rsa_rfid/print.html
Published Friday 18th February 2005 21:16 GMT

[6] “WHAT IS RFID?”
URL: http://www.spychips.com/what-is-rfid-print.html