Information Security Course Case Study: Royal Dodge Airlines RFID Programme

Christian Luijten (496505), Bram Senders (511873),
and Paul van Tilburg (459098)

November 16, 2004

Abstract

A case study on the RFID programme of the Royal Dodge Airlines, with respect to the security issues that are at stake. The study will include risk analyses, solutions and security advisories using the CIA security paradigm.

Solutions include the use of encryption for authenticity, a central transaction server taking care of pseudonimity, discourage the use of injected tags in favour of RFID tag cards to avoid traceability problems. Availability and accountability risks can be solved with detection systems.

Without implementing solutions for privacy issues, customers will reject the service.

Contents

1 Introduction

The Royal Dodge Airlines (RDA) wants to be an efficient, yet customer-friendly airline company. Customers are business passengers, who demand reliable, fast and personal services.

In order to improve these services and thereby strengthen their market position, the board of directors decided to study the the use of RFID chips injected in the arms of passengers for identification.

Wikipedia says on [1] about RFID:

> "Radio Frequency Identification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. RFID tags contain antennae to enable them to receive and respond to radio-frequency queries from an RFID transceiver."

The technique as such is fairly old, officially invented by Harry Stockman in 1948 in his report "Communication by Means of Reflected Power", but already being used during World War II by the UK to distinguish English airplanes from German ones. Recently, RFID got a lot of attention due to the implementation of it in very small chips, capable of being attached to all kinds of objects to track them or to store information about the object on.

Previous implementations from the 60s and 70s were single-bit and only capable of telling that 'an object' was present, for instance in anti-theft measures in department stores. In this time, much effort was put to get RFID to a higher level; letting it do more, like an attempt to get electronic license plates in various states of the USA. Most attempts failed, but the technology matured very quickly due to this.

The modern RFID tags can for example replace barcodes in supermarkets, making it possible to scan a complete shopping cart in an instant, without the need of putting every single product on the counter. They can also be used to identify and track certain objects, an idea which privacy advocates don't like because it is also possible to track identified persons who then have little or no privacy.

Currently there is a discussion going on about the use (and abuse) of RFID, about its advantages and disadvantages and also about the social changes the introduction of modern RFID will result.

This case study will go in detail about all these aspects, concentrating on the implementation of RFID chips in the business model of an airline company, leaving irrelevant details out of scope. First, observations about the case and current RFID topics are collected. Secondly, an inventarisation of the risks is

made, together with possible solutions to resolvable issues. Lastly, the case study will be concluded with an advise in the form of a security policy and a secure architecture to the board of Royal Dodge Airlines.

2 Observations

2.1 RDA requirements

The RDA has put out a few requirements to which the RFID service must provide an improvement.

- Reduce waiting times before check in (last-minute check in)
- Personalized service to customers
- Easy registration of special programs (e.g. frequent-flyer miles)
- Easy payment of additional services (e.g. consumables at the airport or tax-free shopping during the flight)

Each of them has to be taken into account, for they can be conflicting when considering security and ease of use.

2.2 Current status of RFID

RFID has various issues, technical as well as social ones.

2.2.1 Technical problems of RFID

As [2] states in the conclusion, "so long as this technology suffers from privacy issues, consumers will reject it". Meant with these issues are traceability attacks on three different layers inherent in the system. So not even the deliberate violation of privacy by the companies that use them to track objects or persons.

As said, RFID is vulnerable to traceability attacks on three layers, in [2] they are related to three of the seven OSI layers: physical layer, communication layer and the application layer. Some issues can be solved by RDA itself, others can not.

Application layer attacks In [2] three attacks on the application layer are treated:

1. Attack based on the non-randomness of the sent information
2. Attack based on refreshment avoidance
3. Attack based on database desynchronisation

Communication layer attacks

1. Threats due to lack of randomness
2. Threats due to uncompleted singulated session[1]

Physical layer attacks

1. Threats due to diversity of standards
2. Threats due to Radio Fingerprinting
3. Denial of service threats due to collision avoidance protocols

2.2.2 Social problems of RFID

Because the whole idea of RFID is to be able to track a tag, it leads to privacy issues when the tags are still active when they are sold along with tagged products; consumers get the feeling of being watched and distrust the company to attack their privacy.

As long as companies cannot give their customers the feeling that they don't use the RFID tags to spy on them, consumers will reject them—they will want to be able to see at a glance which active tags are available, otherwise they will not know whether they might be spied upon. Also, if there isn't something to gain for them, they will reject them.

3 Risk assessment

This section considers risks concerning use of an RFID system. The risks are assessed in a categorized manner using the CIA[2] security paradigm. Next to these three categories accountability is considered as well.

[1] A session targeted at a specific tag, without changing its static identifier during this session

[2] Confidentiality, Integrity and Availility.

3.1 Regarding Confidentiality

For confidentiality, the risk of disclosure and privacy are assessed.

3.1.1 Risk of disclosure

Radio transmits through the air, without taking much care of walls or windows. Any data that is transmitted through radio must therefore already be secured and may not contain any open information.

Furthermore, any third party needing access to the tag information, for instance shopholders in the airline's private lounge, must be controlled to get limited access to the information connected to the tag.

3.1.2 Privacy

Privacy is a hot issue in the RFID debate. Tagholders can be identified by their distributors, other parties can only read the RFID tag identifier and cannot get to the personal information. However, the fact that the identifier is readable at all times, this might lead to breaches in the unlinkability of the holder.

While the tagholder is initially unlinkable, the use of the tag will expose more information about him. Also, the use of other tags produced by other manufacturers will give a profile of a person by using data mining techniques based on data received on the physical or communication layer as described in [2] and Section 2.2.1.

Four facets of privacy are considered, these being anonymity, pseudonimity, unlinkability and observability.

Anonymity Customers are only truly anonymous when they can perform the actions presented in Section 2.1 without disclosing their identity to anybody. Since a customer's true identity must always be known to RDA (because of e.g. accountability and billing), and this identity must be linked in some way to the RFID tag (for authenticity reasons), RDA will always know what actions customers have performed. Therefore there is no way to provide anonymity.

Pseudonimity Pseudonimity means that a customer can use a resource and be accountable for that use—but not necessarily with knowing the true identity of the customer. This is a risk, because if it would be possible to spoof a customer's pseudonym, then the spoofer is able to carry out actions in the name of the spoofee.

Unlinkability When a customer uses two different resources, then these uses should not be linkable to the same person. This means that e.g. when a customer buys something from two different tax-free shops at the airport, these shops should not be able to know of each other that he has bought a product at the other's store. This poses a problem, since even while the customer may just be a number to these stores (and therefore do not know the user's identity), they can inquire each other about their customers' behaviour.

Observability A customer is unobservable when he can carry out actions without others being able to observe that actions are being carried out. The usage of RFID tags is not really an issue for observability, since customers are already observable without these tags: when you pick up a product in a store, then anybody can see that you are going to buy that product.

3.2 Regarding Integrity

For integrity, the three aspects authenticity, non-repudiation and accuracy are considered.

3.2.1 Authenticy

Implanted RFID tags are very limited in memory because of their physical size, usually something in between 64 and 128 bits of ROM. Therefore, the tags can only carry an identifier and no information. Anyone having access to this identifier can clone a tag and abuse it.

Getting access to this identifier is fairly easy, since that was the whole idea of RFID. Cloning a tag is also very cheap, since a single tag costs no more than about thirty cents. Since RFID scanners can scan tags from a distance of several meters (and scanners that do not conform to power regulations can scan tags from a distance of up to one hundred metres, according to [2]), finding targets to scan is not hard either. This brings the cost of duplicating a tag and thus breaking authenticy to the investment of an RFID scanner plus 30 cents for a tag.

If tags can be cloned, then authenticy is at risk, for then there is no way of knowing whether the customer is actually who the tag says he is.

Another concern for authenticity is that one actually might not know who is the one to perform some transaction is: if several people are present in an airport shop, and one wants to buy a consumable, then how is the shop owner to know who wants to buy the product in the vicinity of the RFID reader?

3.2.2 Non-repudiation

Non-repudiation is the concept of ensuring that a contract cannot later be denied by one of the parties involved. Since authenticy is not guaranteed (yet), it is not possible to achieve full non-repudiation.

Should authenticy and identity be fully guaranteed, even then the customer can repudiate an action since there is no action from his side needed to read the information on the tag and to come to a contract. It might even have happened without his knowledge.

3.2.3 Accuracy

The ISO 18000-6 standard [4] describes accuracy solutions for RFID. When data is received from the tag by the reader it is validated by means of the CRC[3] algorithm. When errors are detected, the same data can be queried again. This method of operation ensures that data is transmitted error-free.

It may also seem to be a problem when two or more devices respond at the same time. However, this is also dealt with in the ISO standard. When the reader detects collisions, it requires the devices sequentially.

3.3 Regarding Availability

While privacy may be a big concern to customers, availability may be a bigger problem to RDA itself.

RFID protocols usually use *slotted Aloha* [2] to be able to distinguish between multiple RFID tags. Using this technique, the reader tries to single out one RFID tag when several are present. However, it is possible to jam the communication between an RFID tag and the reader trying to communicate with it by emitting a radio signal on all channels that the reader is expecting RFID replies on, thereby creating a collision so that the signal from the tag will never reach the reader. This is an effective Denial of Service attack which is not easily countered, and therefore a serious threat to system availability.

3.4 Regarding Accountability

Since the RFID tags are passive components, accountability is a somewhat inherent problem of the system. The RFID tag doesn't store who tries to gain access to the data contained in the tag, so tracing usage back to the responsible persons is almost impossible.

[3] Cyclic Redundancy Check

4 Conclusion

This section contains proposed solutions for the problems described in the risk assessment. These problems are categorized in the same manner as the previous section.

4.1 Confidentiality policy

RDA must provide a privacy policy to its customers. Since RFID is a very hot topic in the privacy debate, this can be crucial for the success of the new service.

We advise RDA *not* to use injected RFID tags for privacy reasons. It would be better to have tags in a credit card format, because customers can leave that at home. This will give customers the choice not to be traceable, and it won't affect service on board and at the airport.

For the confidentiality, we advise to use crypto as proposed in [3]. The simple encryption method ensures a secure transmission of the data while holding the possibility to use a cheap and small RFID tag. It also provides a solution to the risk of cloning of a tag by using dynamic identifiers.

4.2 Integrity policy

There must be a central server for authenticating clients by their RFID tag identifier. This server must provide methods of payment to users of RFID readers. The third party's reader, as used by e.g. airport shops, will forward the encrypted data to the server which decrypts and validates the information in it. This way the user maintains his pseudonimity and transactions performed on behalf of different parties remain unlinkable by these parties, except for RDA itself.

Since RFID has a scanning range, it is possible to have two clients in the same proximity of an RFID reader. This makes it impossible to determine which tag to use for authentication. This can be solved by using short-range readers and showing a photograph of the tagged person to be matched with the person that is standing in front of the operator.

4.3 Availability policy

The denial of service possibility poses a problem for the entire system. The solution would be a detection and localisation system with security personnel to maintain service.

4.4 Accountability policy

The only way to keep track of persons accessing tag data is to place listening devices on the premises for logging purposes. Since it isn't possible to place these devices all over the world, there is an obvious accountability problem. However, since the tags are only in use at RDA controlled areas, this poses no significant problem.

References

[1] *Wikipedia RFID entry.*
`http://en.wikipedia.org/wiki/RFID`

[2] Gildas Avoine and Philippe Oechslin.
RFID Traceability: A Multilayer Problem (draft version).
Lausanne, Switzerland: October 2004.

[3] Martin Feldhofer.
A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags.
Stiftung Secure Information and Communication Technologies SIC: 2003.

[4] ISO JTC 1/SC31 technical comittee.
Radio freqency identification for item management.
Geneva, Switzerland: August 2004.