Department of Computer Science

Richard Grunzke

Risk Analysis of the applied RFID System

Project Stolpen

Computer Science
C-level thesis (10p)

Date:	07-01-12
Supervisor:	Simone Fischer-Hübner
Examiner:	Martin Blom
Serial Number:	C2007:01

Karlstads universitet 651 88 Karlstad
Tfn 054-700 10 00 Fax 054-700 14 60
Information@kau.se www.kau.se

Risk Analysis of the applied RFID System - Project Stolpen

Richard Grunzke

This thesis is submitted in partial fulfillment of the requirements for the Bachelors degree in Computer Science. All material in this thesis which is not my own work has been identified and no material is included for which a degree has previously been conferred.

Richard Grunzke

Approved, 12.1.2007

Opponent: Hans Hedbom

Advisor: Simone Fischer-Hübner

Examiner: Martin Blom

Abstract

This thesis will be a risk analysis of a RFID-system for a logistical application. The system works as follows: Around Karlstad in Sweden there are three new weighing machines for lorries. The load weight will be measured for the police to control overweight and for logistical reasons such as issuing invoices and optimising the supply chain. The lorries do not have to stop to be weighed. They have to drive slowly over the weighing machine, so the loss of time is minimal. The lorries will be identified via RFID-tags. So every time a lorry will be driven over the weighing machine, the identification number and the measured weight will be logged and send to a database. In the future it is planed to store the weight on the tag itself. The task is now to analyse the RFID-communication and the transmission to the database. The thesis will contain several parts. First RFID in general and how RFID will be used in the application-scenario will be described. Next sections will be about the security and privacy requirements and the risks in detail. Then possible solutions are outlined and concrete suggestions are presented. Finally a conclusion will be drawn, which will show that the application has a low level of security.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

RFID is a technology to automatically recognise the identity of objects and subjects. It will probably reach a wide adaptation in the next years. One example of today's application of RFID technology are the new european passports. RFID in such a wide deployment is a new area, which has many open security and privacy issues. Another application that uses RFID and is subject of this thesis is Project Stolpen, which is a RFID application for the automatic registration of the weights of trucks. In the future it is planned to include more features on the tags, for instance data about the status of the brakes. The weighting stations of Project Stolpen are residing around Karlstad in Sweden, but it is planned to deploy more weighting stations in other parts of Sweden and possibly in other countries as well. Unfortunately it was not possible for me to gather all the information in detail about the project I wanted. The following thesis will discuss the security and privacy risks in Project Stolpen. The term risk analysis in this thesis means the following; It is the evaluation of dangers to a specific project, which also includes the associated probabilities and consequences. In general, first the application will be studied in detail to understand how it works. Then the actual risk analysis will be conducted to realise the risks to the project. It will be accomplished in this thesis like the following. Chapter 2 the thesis will provide the technical background about RFID. It consists of the technique itself, the

RFID system architecture, application areas and privacy issues. It is intended to give a solid introduction to RFID. In chapter 3 the Project Stolpen will be introduced. First its functionality will be presented. Then the risks to Project Stolpen will be investigated in chapter 4. This chapter is divided into tree sections containing of business process risks, business intelligence risks and privacy risks. After that, countermeasures will be presented in chapter 5. This chapter is partitioned in management controls, operational controls and technical controls. In chapter 6 concrete and reasonable countermeasures for Project Stolpen will be given. It is intended to make the project more secure in sensible way. Finally a conclusion will be drawn in chapter 7.

Chapter 2

RFID

The essence of RFID (Radio Frequency IDentification) is to automatically and uniquely identify and localise objects and subjects using radio frequencies.

2.1 Technique

A RFID system usually contains three parts: The tag, which identifies the objects or subjects. The reader, which reads the information from the tag, is also called interrogator. The term reader is somehow misleading because depending on the tag the reader can write too. At last, the system in the back end, which usually consists of servers and databases. It uses data registered by the reader to query a database and possibly store it in the database. Usually an unique identifier is stored on the tag which is then used as a pointer to a certain database entry. This usually holds more specific information, for example tracking information or information about the carrier of the tag. In more sophisticated tags these data can also be stored on the tag itself. A sample tag is shown in figure 2.1.

Tags consists of an antenna, an analogue circuit, a digital circuit and a memory. They have several properties like frequencies, bandwidth, lifetime, price, memory and range. The tag sends information to the reader by manipulating the electromagnetic field sent by

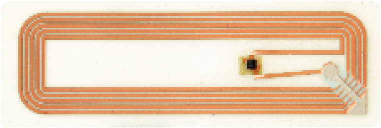

Figure 2.1: A 13,56 MHz Tag [1]

the reader. An exemplar of a reader is shown in figure 2.2.

2.1.1 Classification of tags by their characteristics

Several possibilities to split up tags are presented in the following clauses. They help to get a glance at the variety of technology in tags.

Division by energy supply

There are passive tags, which do not have an internal power supply and active ones which have a power supply. The passive tags get the power by loading up a capacitor with the energy induced by the reader. The signal to do that is called *Continoues Wave*. The signal has to be sent all the time during the transmission. An characteristic is that the range is very limited but usually the possible lifetime is longer then with active tags. They use their internal power supply to power their ICs that generate the outgoing signal. Active tags are more reliable, meaning that they have fewer transmission errors, they are more resistant to disruption of the signal for instance by water. They also usually have a higher range and more memory. But their lifetime is more limited, and they are much more expensive.

Division by the used frequency bands

Tags with low frequencies like 30 to 500 kHz have a short range and a very limited bandwidth. They are cheap and resistant to environmental influences. They are used for instance in automobile immobilisation devices. The ones with high frequencies like 3 to 30 MHz have a higher range and more bandwidth but are also more expensive. They are

Figure 2.2: A reader with a range up to 85m

used in smart tags. Tags with very high frequencies like 850 to 950MHz, 2,4 to 2,5 GHZ and 5,8 GHz have a very high range; 3 to 6 meters for passive tags and 30m and more for active tags. They are used for example in automated toll collections systems.

Division by the access type

Another important distinction is by the ability to only read tags or to also be able to write them. Only very basic tags have just read access. This has the advantage that data stored on the tag cannot be altered in an unauthorised way. They are also cheaper besides being more secure. But only tags that can be altered after the production can use the full potential of the RFID technology.

Division by their cryptographic capabilities

Basic cheap tags do not support cryptography at all. More advanced tags are capable of executing stripped down cryptographic algorithms. The final stage are advanced tags with support of full cryptographic algorithms. Broader support comes also with higher costs for the tags.

Table 2.1: Another classification: EPC Tag Classes [2]

Class	Type	Comments
Class 0	Read only passive identity tags	Factory programmable (64 bit only)
Class 1	Write once passive identity tags	WORM with provisions for read/write (96 bit min.)
Class 2	Passive tags with added functionality,e.g. memory or encryption	Shorter range (i.e. 4 inch - 18 feet) Read/write (multiple),user memory
Class 3	Semi-passive RFID tags Battery Assisted reader activates, battery powers	Medium range (i.e. 10 feet - 50 feet) Read.write, user memory,sensors, encryption
Class	Active tags communicate with readers and other tags on the same frequency band Active battery powered	Long range (i.e. 300 feet) Read/write, user memory, sensors,etc
Class 5	Essentially readerscan power class I, II and III tags, as well as, communicating with class IV and with each other	

Division by price

The price for tags differ a lot depending on memory, computational power, supported standards and bought quantities. EPC supporting tags in extended quantities (one billion) will cost about 10 cent soon as mentioned in [10]. In 2005 about 600 million tags were sold, as stated in [8].

2.1.2 EPC - Electronic Product Code

EPC is a very important standard in regard to RFID. The current version is EPC Generation 2. As stated in [6]; "EPC Generation 2 is a new standard for RFID tags, specifying the operation of the tag and the communication protocol for interoperability with EPC readers." A rich chapter about the origin, development and appearance of EPC is included in [14]. An overview about EPC tag classes and their features is given in figure 2.1.

The evolution from the barcode to EPC

Applications implementing the EPC standard can be seen as the successor of the barcode. They have several advantages over barcodes.

- Tags do not have to be in sight in order to be read. That means tags can be built into plastic cases, so they are more resistant to environmental stress.
- Tags do not have to be exactly positioned. That has the big advantage that tagged goods can be easier and faster recognised.
- Tags are read much faster, in optimal conditions over 1000/s.
- Also the reading distance can be much greater. This for example makes the supply chain faster and easier to handle and for instance an inventory audit in a supermarket will be much faster.
- A tag can store, depending on its memory, much more information than a bare identifier.
- Tags uniquely identify objects not only classes of objects. That means it identifies a book not as *Dictionary Swedish - German* but as *Dictionary Swedish - German* with a specific ID that is unique to that specific book.

All these are advantages making RFID e.g. immensely useful for the supply chain or warehouses and supermarkets. This leads to be possibility that products can be traced all the way from the manufacturer to the supermarket. The supply chain can be optimised and therefore, be cheaper. Theft can be stemmed, and a fully electronic checkout may be possible in the future. In whole the supply chain can be automated to a higher degree. Tags can be, furthermore, combined with sensors to greatly increase the potential of RFID. For example tags could include temperature sensors and a GPS listener to measure the temperature at a certain location and radio transmit it via a reader to a database.

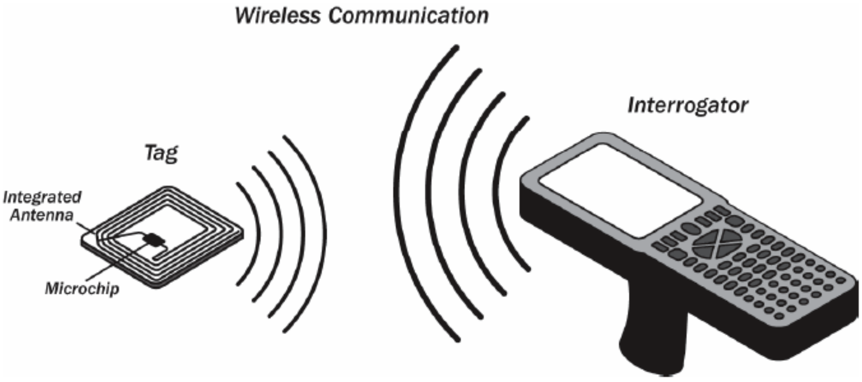

Figure 2.3: A basic RF subsystem [12]

2.2 RFID system architecture

The RFID architecture will be divided into three parts to break down its complexity, which can vary greatly depending on the implementation. Every system contains of a RF subsystem and most also of an enterprise subsystem. RFID systems aiding the supply chain often also contains an inter-enterprise subsystem. This chapter is based on [12].

2.2.1 RF Subsystem

The RF Subsystem enables the unique wireless identification. It consists of tags and the readers. Tags are used to mark an object or subject. Readers are then used to communicate with the tags in order to register their ID, store information on the tag or invoke more advanced operations. An illustration is provided in figure 2.3. For more details we refer to the previous chapter.

2.2.2 Enterprise Subsystem

The enterprise subsystem contains the middleware, analytic systems and the network infrastructure. The middleware filters the raw data from the readers for the back end ap-

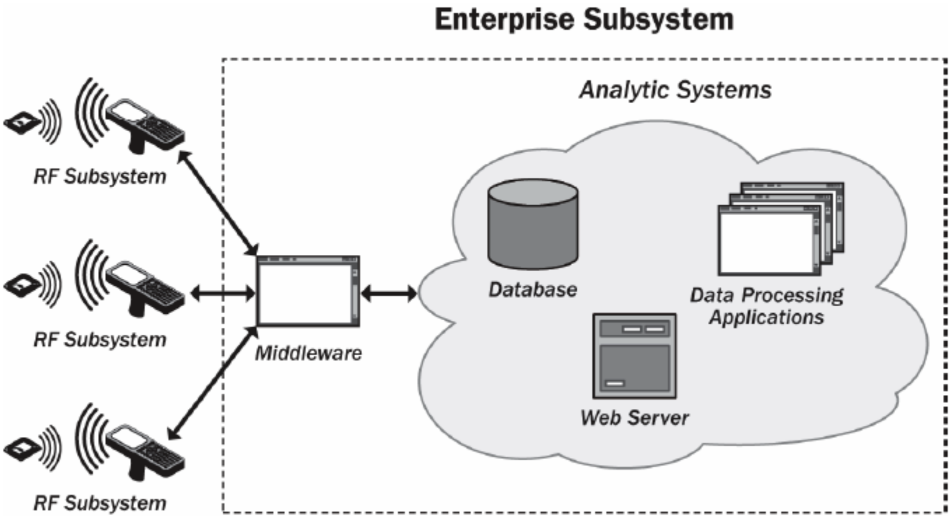

Figure 2.4: An example of the enterprise subsystem [12]

plications. It filters for example faulty and duplicate data. This reduces complexity. The analytic systems only get the data they need to know. Middleware systems are also used for monitoring and managing the readers. Analytic systems are processing the output of the middleware system. This could mean to get further information according to the IDs on that tags and to analyse and aggregate the available data to optimise the supply chain. Data could also be made available on Web servers for access to authorised users. The network infrastructure provide the communication means to connect the RF subsystem with the enterprise subsystem and to connect the discrete parts of the enterprise subsystem. Important characteristics are for example the physical and logical topology and the protocols. The enterprise subsystem is illustrated in figure 2.4.

2.2.3 Inter-Enterprise Subsystem

The inter-enterprise subsystem connects enterprise subsystems. This is used when data needs to be shared between different companies. RFID systems with an inter-enterprise subsystem are also called open or online systems. Without this they are called closed or

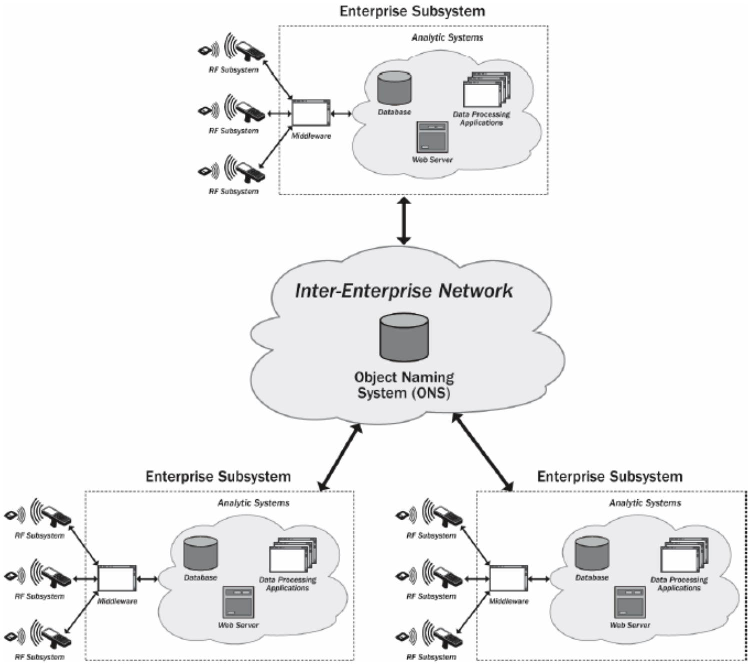

Figure 2.5: A scheme of the inter-enterprise subsystem [12]

offline systems. Common examples for open systems are applications in the supply chain that are supporting the EPC standard. An other part is the Object Naming Service (ONS). It is used in a supply chain application to connect the ID on the tag to further information about the product the tag is attached to. It is designed to work across company boundaries. ONS is somehow similar to DNS (Domain Name Service). The ID on the tag, is resolved to an address where further information can be accessed. Another alternative to resolve the IDs on the tag is to use the EPC Discovery Service. It is similar to search engines. Different addresses can be returned which might correspond to a specific point in the life cycle of the object. An illustration of the inter-enterprise subsystem is provided in figure 2.5.

2.3 Application Areas

Based on the NIST RFID study [12], we will present several application types.

2.3.1 **Asset management -** Determine the presence of an item

This applications are used to manage inventory of tagged items. This, in comparison to barcodes, offers an increased speed of common tasks like performing an inventory. The result is an improved operational efficiency and effectiveness. An example is Electronic Article Surveillance (EAS) which is used to keep track of items in a retail store. Tags are attached to goods and when a consumer checks out, the clerk deactivates the tag. So when a consumer tries to leave the shop with still activated tags, he has probably not checked out correctly. This can be used to controvert theft.

2.3.2 **Tracking -** Determine the location of an item

Here the main purpose is the keep track of the location of tagged objects. This is done by recording the location of the last interrogator that read the tag. In contrast to asset management applications, many spacial distributed readers are needed that are connected via a network and managed by an application server. It may be used in the supply chain to always know where specific items are.

2.3.3 **Matching -** Ensure affiliated items are not separated

Two tags are tuned to each other. This is done to make sure, when tags are brought together that do not match, an alarm will be triggered. A technique like that could be used in an airport to match passengers and luggage to prevent theft. This could be done like the following. A passenger has a ticket with a tag inside, and the luggage is tagged too. Both tags are tuned to each other. When now someone takes the luggage from the conveyor belt, the person needs to have the according ticked, or otherwise a security officer could be alarmed.

2.3.4 **Process control -** Correlate information for decision making

Here information associated with the tag is used to trigger tag-specific actions. An example could be the tagging of an item in a factory. As the tagged item is migrating through the factory different actions according to the tag are performed on the tag. An example could be painting it in a specific colour. The scenario is more complex because additional data is associated to the ID on the tag, like the colour.

2.3.5 **Access control -** Authenticate a person

In this application the tag, in form of a non-contacting smart card, is used as a credential to access a building or to be able to logically access information. Each person has a unique smart card, so it is possible to grant and forbid access for each person individually. A possible use is an included tag in an employee badge that automatically opens the door to a restricted area. Another common use is in automobile immobilisers, here a tag in the key must be present. A reader in the car notices that the tag is present, thus the driver is able to start the car.

2.3.6 **Automated payment -** Conduct a financial transaction

In this application area tags are used to automatically initiate payments. Like in the access control application good security measurements, like encryption, are needed because an abuse will directly let the owner loose money. Widespread uses are the toll collecting systems in the U.S., where payments are triggered when a car is driving by which is equipped with a tag. The account of the driver is then debited according to the driven miles. Another common use is on cruise ships, there the tags are linked to credit card accounts. The consumer now can pay for drinks or gifts without the need of handling cash or credit cards.

2.3.7 Supply Chain Management

It consists of the monitoring of products while they proceed in the supply chain from the manufacturer to the retail store. This is done by attaching a, EPC supporting, tag to each product and the stationing of readers throughout the supply chain. The information, which tag is when at what place is recorded in a database for further analysis. This area combines several previously named areas like asset management, tracking, process control and payment systems. The application promises huge advantages for the industry, like better preventing out of stock situations and automated invoicing and payment.

2.4 Privacy

Privacy has been defined as the right to be left alone bye Warren/Brandeis in 1890. Another famous definition of privacy is the following by Alan Westin in [16].

”Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others.”

There is also much criticism about RFID and big privacy concerns are at hand. In some years tags will be on many consumer products, often unnoticed by the owner. This means that a person will carry or wear tagged objects with unique IDs. This person can be traced or even identified if the IDs are combined with the checkout information from the store, where he bought the items. When this is used, combined with many widespread readers, movement profiles of person might be merged. The life of the people can be monitored to a high degree.

Amongst others, according to [15] and [9] the following privacy threats could be possible when using RFID in the supply chain or in other applications.

- A database with the information who has contact with whom can be build. This is done by using the information when tags leave a person's specific set of tags and move into another person's set meaning that it is maybe given as a present or sold to that person.

- Another example for a threat is that somebody bought a knife with an embedded tag and it is stolen from him. If the robber then uses it to commit a crime, the knife will be still associated with the buyer. This can lead to serious trouble for the buyer.

- Another variant of this is that if tags can be cloned, a criminal could virtually carry another persons identity. He then could commit a crime and leave false traces.

- A big problem is that most consumers do not only not know that they carry tags, but they also have no control over the data and who is able to read it. This is partly due to a lack of transparency. An implication of the unintended exposure of tag information is that people who carry more expensive goods are in the future more likely to be victim to robbery.

- An also quite negative scenario in a some years will be that robbers might be equipped with readers and at night are going from house to house and figuring out where they can rob the most and at the lowest risk. They might find out whether the people are not at home because they register the missing of loyalty cards, identify cards and implemented tags(assuming that it is common or even mandatory in some years). They also might find out remotely if a domestic animal is present(And even if it is a dangerous dog if they have access to the animal registration database, which might not be well protected because that data is not accounted as too sensitive). They might even find out if and what kind of security systems are installed, assuming that there are tags in that products. This is not implausible considering to the probable wide spread use of tags in some years. All in all, RFID might improve the business of robbers quite a lot.

But not only private persons are at risks. Companies that use RFID are exposed to some similar and some innate threats. For example the data stored on a tag is often trusted with no justified reason. This makes a RFID virus possible as shown in [11]. Further risks will be discussed in chapter 4.

Chapter 3

Project Stolpen

3.1 Introduction

A RFID system to identify trucks will be descripted in detail in this section. It is called Project Stolpen. An official description is the following as stated in [13].

”The Project Stolpen is a reference project that aims to build a quality secured information and service node (hub) in the Logistic Value Chain that will give Logistic companies, transport buyers and authorities a picture of activities in the logistic chain in real time. This gives the actors possibilities to guarantee the quality of their services and facilitate that laws and regulations are followed which gives fair competition. The data capture is done automatically with the RFID technology that will be distributed to the partners in XML format and can easily be read at the Internet.”

3.2 Current System

In the current stage the project is for measuring the weights of trucks for several uses. The trucks are identified via RFID tags. They are weighted at three stations around Karlstad. A part of one station can be seen in figure 3.1. The stations are equipped with weighing

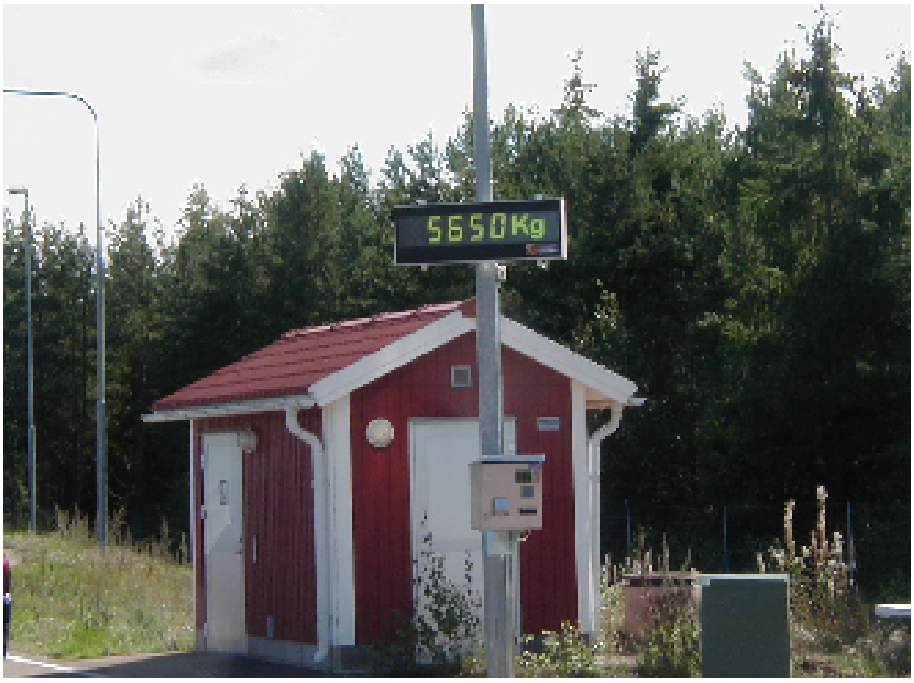

Figure 3.1: Display showing the measured weight [13]

machines, RFID readers and an application server for controlling the readers and handling the gathered data. The installation of a weighting machine is shown in 3.2. The trucks do not have to stop while being weighed, they slowly drive over the weighing machine. While being weighed the trucks are automatically identified using fixed readers and active RFID tags with a frequency of 2.45GHz which cost 270 SEK. Both axle load and gross weight are measured. An application server at the station will connect the ID from the tag and the measured weights and send them to the database where the values will be stored to be accessible for further purposes. One purpose will be the checking whether trucks are overloaded or not. This data then can be used for: weight bills, specified weight bills, weight bills mediation, invoicing, payment, accounting, filing and statistics. Possible customers are able to see via a web page if the logistic company works according to the rules. Access to the website is granted by Project Stolpen. The readers are connected via LAN with the application server in the weighting station, and the company one.com is

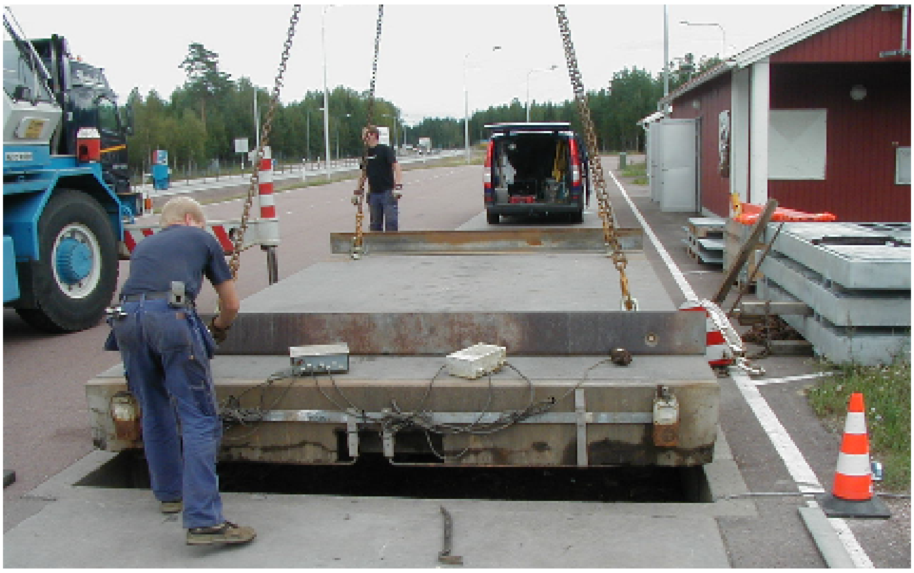

Figure 3.2: Installation of the weighing machine [13]

hosting the MySQL database. Several other data might be collected using the ID on the tag. For instance arrival times, driving time, resting time and speed. This information could be integrated into fleet management systems for optimising purposes. In the current version, however, only an unique ID is stored on the tag.

3.3 Outlook

In later stages the system will be advanced to also support the following functions: brake check, brake light check, side light check, tyre scanning and digital tachograph reading. The resulting data will be stored on the tag itself, so that the police will be able to check using mobile readers, if everything is according to the laws. This for example means that they can control if overweight occurs.

Chapter 4

Risks

The risks to the project Stolpen will be divided into three groups. The business process risks, the business intelligence risks and the privacy risks are to be examined. Concrete risks for Project Stolpen will be presented. Each section will include factors that influence the risks. A factor can either mitigate or intensify a risk. Besides the concrete risks we will discuss the impact, the likelihood,the plausible trend of the risk in the future and to whom exactly this poses a threat. The structure of this chapter is partly based on [12].

4.1 Business Process Risk

The business process risk means that this can cause the whole system to fail. It can be caused by human actions, either unintended or malicious, and from damages due to forces of nature.

4.1.1 Influencing Factors

The business process risk is influenced by the following factors.

The importance of the RFID system to the organisation.

The RFID system is the mission of Project Stolpen, so it is uttermost important that it is not failing, or otherwise it will have a huge impact on the performance of the company.

The possibility that reparation is performed quickly in case of failing.

It is important that the company is able to act fast if a part of the system, for instance a weighting station, or the whole system, possibly caused by the non-availability of the database, is failing. It is so important because the longer it takes to repair the damage, the more money will the whole incident cost.

The environment in which the RFID technology is located.

It is negative that the readers and the application servers are in remote locations. The application server is only protected by the locked doors of the station and an alarm. It is possible that radio frequency interference exists. The system uses active tags operation on a frequency of 2.45GHz. This means that it is vulnerable to technology operating on the same frequency, like bluetooth satellite or 2.45GHz cordless phones. The tags on the trucks are exposed to vibrations, which means that the tags have to be resistant to long term exposure of vibrations. The tags also have to be resistant to extreme temperatures and humidity because they will occur. Temperatures from -25 to 35 degree celsius, rain and snow in several months of the year are very likely around Karlstad. This problem gets even more serious when the system will be implemented in different regions, where more extreme temperatures may occur.

The existence of competitors with the motivation and the capability to perform RFID attacks

This is very hard to measure. It might depend on the largeness of the competitor, for example if he has enough means to conduct such an attack. Also the more widespread the system will be and the more will be weighted the more likely attacks are. Around Karlstad, for example, a load of a truck has roughly a value of 7,500SEK to 36,000SEK. The higher the value is the more likely attacks are.

4.1.2 Concrete Risks

Cloning of tags

This means to take the data from one tag and put it on another tag. The goal is that a reader cannot distinguish between the original tag and the newly cloned tag. This attack can have different outgrowths. For one, the truck company could clone a tag to pretend that a truck is allowed to load more than it actually can. It could be done by cloning a tag with the ID of a larger truck. The cloned tag will then be attached to the smaller truck. Now the smaller truck can load more cargo without raising suspicion. Accidents are more likely to occur because of the constant overloading of the truck with fake tags. So the clear victims are the other road users who might get involved in accidents. Competitors of the company using the fake tags would also be victims because they would suffer from a corporate disadvantage. This attack will be more relevant in the future with the wider deployment of Project Stolpen. And the more it is used and the more companies are using it, the more likely this attack is. Another scenario would be that a competitor could overwrite a tag with the ID of another truck which is only able to load less. So when the truck is fully loaded according to its original weight, it would always seems to be overloaded because the tag only allows a lower weight. The motivation of a competitor to do this would be quite high, because not much equipment is needed and it would severely damage the reputation of the truck company which tags were altered. This might result in much less contracts from companies which want their goods to be transported. It would also cause trouble with the police, although it would be quite easy for the police to check how much the truck can actually load. They would compare the possible weight in the papers of the truck with the possible weight associated with the ID of the truck in the database. That could be a way to find out whether the ID was altered. In both scenarios Project Stolpen would be a victim because the publication of such cases occurring in the public would have negative effects on the reputation of Project Stolpen. Truck companies might start to boycott the system and further deployments would be at risk.

Jamming of the radio communication

This is done by overlaying the used frequencies with electromagnetic waves on the same frequency. It makes it much harder for the reader to work correctly or even the whole radio communication could be prevented. If the sender has enough output power, it could be hidden many meters away from a station. It would render the station unusable for days or even longer if the sender cannot be found. It could also be achieved by placing a blocker tag in the range of the reader. It was first discussed 2003 by Juels, Rivest and Szydlo in [7]. A blocker tag is a tag that responds like if all possible tags were present. The reader now thinks that all possible tags are present. This means he cannot register the right tag. So no communication is able to take place. An attacker who would want to do this could be an start-up competitor to Project Stolpen. This start-up could try to ruin the reputation of Project Stolpen in order to gain an advantage in the possible upcoming business competition. Another motivation would be for the driver of the truck to avoid a stop and search operation by the police. But it depends on the pressure to always have clean records on the website. The website will show if overload was measured, if no overload is shown the records are clean. The pressure will be rather high because a possible ordering party wants clean records. The jamming could be done if the truck is overloaded, or in later versions of the project if for instance the wheels are rather old. If the jamming by the driver is not done too often, it might not attract attention because a missing record could also be due to a regular radio transmission error. So there will not be any unclean records, only missing ones. And only the truck company itself would be able to notice missing records, but not the ordering party. The victims would be other road user, due to the possible decrease of safety of the trucks. Also the other truck companies and Project Stolpen would be victims. The truck companies would suffer from business disadvantages and Project Stolpen might sustain a loss of reputation. When a jamming sender is used, it will also suffer a loss of money, because it is paid per transmission. It is hard to predict the future in this case. The blocking techniques might get more sophisticated but anti-blocking techniques might evolve too.

Unauthorised modification of the data on the tag

If the tags do not have access controls, data on the tag can easily be modified. This could mean to overwrite the data with meaningless data to disturb the whole system. Or a competitor could overwrite the ID of a tag with an ID of another company to insert false data into the database of Project Stolpen. The whole database could get useless because nobody could rely on the data anymore. An attacker could also alter the data on the tag in such a manner that additional data is added. So when the data is processed by a server the software only expects data in a valid format and does no check that. Due to that a buffer overflow attack can be performed, so a virus could infect the application server. This is only possible due to poor software engineering practises. For further information about this, please refer to [11], which leads to more information about such an attack. Here the victims would be the other truck companies and Project Stolpen. The companies would pay the usual monthly fee but getting no service in return and Project Stolpen would loose reputation if this gets public. And due to that it would loose money because of the decreased usage.

Invalidation of the unique connection between tag and truck

This could be simple done by unscrewing the tag from the truck. A competitor could do this to cause trouble and furthermore costs for a truck company. This results in a business disadvantage. But it is quite improbable because the competitor needs physical access to the truck. A tag could also be detached by the truck company itself to attach it to another truck, so that this one could load more without attracting attention. This risk is quite high if the police does not check if the right tag is attached to the truck. The police can only do that, if there are truck specific information in the database or on the tag as well. A possible way would be to store the license plate number on the tag. In the current system this is not the case. The trend in the future might be that this risk will be mitigated due to more information in the database or on the tag. Also fines and sanctions might help to reduce fraud.

Coherence between ID and measured weight

The problem is to make sure that when a weight is measured the correct tag has to be registered. This is not a trivial problem because it could easily happen that another truck is right behind the truck, or even when a truck is driving on the road in the wrong moment. The problem is very real since readers today do not read the nearest tag first, they register all tags in range and then go through them one by one. If at least two tags are in range it would be pure chance that the right ID is used. So a wrong pair of weight and ID would be send to the database. This is even more probable if the tag on the truck that is intended to be weighted is damaged. This flaw could be used to disturb a station and the whole system. An attacker could place a stolen tag or a tag with the correct data format near a station to trigger the flaw intentionally. No one could rely on the data anymore, as wrong ID-weight pairs would be send to the database. The likelihood will immensely increase depending on how many companies will use the system. This is so because the more trucks are around, the more likely for the reader it is, that a wrong tag will be used.

Failure of the tag

That could be a problem when nobody notices that a tag is not working anymore. Or it would only be noticed long after the tag ceased to work. Whether this is noticed when the weight measurement is made, depends on whether it is shown that the measurement worked or not. The risk could undermine the system. In the first time it will be quite unlikely because all the tags are new. But as time is advancing more and more tags will fail, and if this problem will not be addressed it might result in gaps in the database. Also, for example, a competitor could intentionally destroy tags. The victims are the truck companies and Project Stolpen because the truck companies would get gaps in the database and Project Stolpen would get a unreliable database. It could be mitigated by the truck company by comparing the data on the website with their own information, or regular checks at the truck depot if the tags are still working. This however leads to additional cost for the truck company. The risk in the future could also decrease because if the police adopts the system, it will notice a not working tag and inform the driver.

Demolition of a station

This risk may include the theft or destruction of readers, servers and technical equipment in or around the station. The effects can vary quite much. The stolpen project will surly loose a lot of money due to missing or destroyed equipment and due to loss of income because the station will be unusable for some time. This has to be repaired quickly or otherwise a loss of reputation will occur too. Severe consequences might also lie in loss of data on the application server, if that data is not backed up regularly. The motivation for an attacker could just be a greedy or destructive mood.

Manipulation of the weighting machine

A technician who installed the weighting machine could do that. He could manipulate it so that it always measures, for example, 10 percent less weight. All the trucks only using that station would be able to load more without raising any suspicion. The victims would be the other road users because of the increase accident rate with trucks. Project stolpen might loose general trust by the public in the whole system.

Bankrupt of provider

The database provider one.com could go bankrupt, resulting in a possible disruption of the business. This could have big consequences if no one.com independent backup is made. It has to be made sure that it is defined what exactly happens in such a case. Project stolpen should be able to force the release of the data in such a case. Project stolpen could loose much money due the reduced income for transmissions. The reputation could also suffer.

Hardware failures

As hardware ages it will fail. This holds true for all the parts of the system like readers, server and also the weighing machine. This risk is peculiar significant for parts of the system, on that many other parts depend. If, for instance, the database server fails, the whole system will cease to function. This risk is unavoidable unless much money is spend to redundant servers and databases. It is therefor important that the damage is quickly repaired, so the impact it kept low. The risk could be mitigated with low afford by using redundant parts, like RAID arrays and an uninterruptible electric power supply. Hardware failures will have an increased impact in the future, because the longer stations exists the more likely failures will be. An appropriate backup concept should be implemented as well.

Draining of energy

A rough reader placed near a truck depot of a competitor could provoke continuos activation of tags, this might quickly empty the batteries of the active tags. The competitor could cause much annoyance and disturbance at the particular truck company with low afford.

Internet attacks

Internet connected servers could be infected with worms, meaning that when services are offered for clients, the worm could use that entry point to exploit a security vulnerability. The result could, for example, be just a slowdown of the machine because it is used as a spam server, or even the complete deletion of the whole hard drive. In either case backups are needed because one cannot be sure if important data was altered if a worm infected the system. The infection with malicious software could mean failure or a decreased performance.

4.2 Business Intelligence Risk

The business intelligence risk stands for the possibility that competitors, to the carrying companies, might gather data and use it to harm the RFID-using company.

4.2.1 Influencing Factors

Several factors affect this risk.

The type of information stored on the tag

Currently only an ID is stored on the tag. So competitor cannot gather data directly connected to the truck. But with well placed readers a competitor could track all the trucks of a company to get information about how well the company is doing. In the future this factor will have a larger impact, as more information will be stored on the tag.

The existence of competitors with the motivation and the capability to perform RFID attacks

This is hard to tell. The competitor would need the knowledge, the motivation and the tools to perform attacks. Also a disgruntled employee might pose danger. This is actually very severe because he already knows the inside of the system and how it works in detail. If no capable competitor is known, it does not mean that there is not any.

The usefulness or relevance of information available to the competitor

This depends on the data that is stored on the tag because currently only an ID is stored not much information can be gathered by a competitor. Only, with much effort, moving profiles of the trucks of a company. But especially in a larger competitor this could be valuable information.

The location of the RFID components

The RFID components are in public places rather than access controlled facilities, so this factor has a big impact on the business intelligence risk. The radio communication can easily be eavesdropped, because it is taking place in a public area. In a controlled area, only people with access could eavesdrop.

4.2.2 Concrete Risks

Eavesdropping

A competitor could be eavesdropping the communication. He would record the radio transmitted data with a reader. This would be done to get, possibly valuable information, about the business of the competitor. The information could be used to gain a business advantage. An attacker could also break into a station and steal the hard drive. This could have the same effect and mentioned before, depending on how much information is stored on that server. The motivation might be high because as margins grow thinner, even little advantages over a competitor can be important. Eavesdropping is very likely to happen because much information can be gained and the risk for the attacker is very small. In the future the eavesdropping risk is likely to get more important as more people gain knowledge about RFID and its weaknesses.

4.3 Privacy Risk

The privacy risk means that the privacy of the truck driver might be affected.

Personal data as stated in [3] is defined as the following; "'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;".

The data on the tag, the data in the database of Project Stolpen and the information in the database of the truck companies are alone not personal data. Only if the data sets are associated with each other it becomes personal data.

4.3.1 Influencing Factors

Factors with an impact on the privacy risk are the following.

- If and which personal information is stored on the tag.
- The possibility to link data on the tag with data in the backend, which would result in personal data.
- If tags include the possibility to disable them after they are not used anymore.

4.3.2 Concrete Risks

Violation of privacy

The privacy of the truck driver is affected. The data in the database of Project Stolpen alone is not personal data, because it is not recorded who drives the truck. When it is aggregated with the data of the truck company it becomes personal data. Because now one can find out which driver controlled what truck where and at what time. This leads to the possibility of generating movement profiles. This risk is borne by the truck driver and by Project Stolpen, because Project Stolpen could violate legal obligations.

Chapter 5

Countermeasures

This chapter presents countermeasures applicable to Project Stolpen. It is divided into the following three categories. The categories are *management controls*, *operational controls* and *technical controls*. The chapter is based on the structure of categories similar as in [12].

5.1 Management Controls

In this section management solutions will be presented, in particular policies, which may describe the demand the management has in regard to security.

5.1.1 RFID Usage Policy

This section describes the allowed and illicit uses of the RF subsystem. Also roles will be assigned to the staff according to the tasks that need to be done in the RF subsystem. For instance, when a application server fails. Who is responsible? Who will organise help? What exactly has to be done? The policy for instance defines the responsibilities in advance, so no time is wasted in case of an emergency. A definition of roles and responsibilities also enables the management to take legal actions against persons that failed to fulfil their responsibilities. A policy should be carefully developed so that it is easy to handle for the staff that needs to follow it. Also penalties should be included because the policy alone does not ensure that it will be followed.

5.1.2 IT Security Policy

This policy describes the security of the whole system and not just the RF subsystem. The following points should be addressed.

- Access control: who is able to read/write what information
- Firewalls, to restrict the possible information flow down to the minimum that is needed
- Key management for encryption to be used
- Enterprise subsystem security for managing the security of the middleware and database
- RFID security training should be conducted
- Intrusion Detection system should be used, to detect common attacks

A good security policy helps mitigating the risks. It also helps the staff to manage their work, if they follow the policy they are unlikely to do anything completely wrong.

5.1.3 Agreements with External Organisations

The collected data will be shared with other organisations like the police and clients of the truck companies. Formal agreements have to be made to make sure the organisations keep the data safe and use it only for the specified purposes. This helps to mitigate the danger misuse of the data. It also serves as a legal safeguard in case of a legal dispute.

5.1.4 Minimising Sensitive Data Stored on Tags

As long as no sensitive data is stored on the tag or could be associated with the data stored on the tag, the security does not need to be extremely tight. The data can be much better secured on the database because databases exist for a long time and it is known how they can be best secured. This also greatly mitigates the risk of eavesdropping. It however does not help in regard to the privacy risk of the drivers, because a truck still has a specific ID. With that ID the drivers could be traced.

5.2 Operational Controls

This chapter will inspect operational solutions. Here we describe what should be done on a regular basis during the operation of the system.

5.2.1 Physical Access Control

This for example means to control access to the station house. The truck companies should restrict access to their truck depot as well, to mitigate the risk of a competitor unscrewing tags from trucks. It also mitigates the energy draining risk. But these controls are very limited, because most parts of the RFID system are in a public area. A downside is that the restricted access to the truck depot does not thwart the risks of manipulation by radio communication means completely.

5.2.2 Operator and Administrator Training

This is needed to make sure that the staff is able to comply with the policies and with agreements with external organisations. The training should at least address the following points.

- How to detect a security breach.

- How to analyse it.

- What exactly should be done in case of a security breach.

However, security training alone is not able to thwart security breaches, it only can be a complimentary measurement.

5.3 Technical Controls

This chapter will examine technical solutions. This for instance will include the protection of the data on the tag. The section will be divided into two parts. One about tag data protection and one about the protection of the RF communication.

5.3.1 Tag Data Protection

Tag Access Control

This includes the ability to use a password for protecting the memory(the actual ID is excluded because it is needed for addressing the tag) and commands on the tag. When a reader wants to change the memory of a tag, it sends the password together with the command to the tag. Sometimes the distinction between read and write access is possible. This prevents the unauthorised reading of the memory. It however does not address the privacy risk, because the ID needs to be read as the reader has to be able to choose the right key. The key length, has to be long enough, or otherwise the key protection will be of little use. The key management is a huge problem. Every reader needs to get to know the key of every tag in a secure way. The key also needs to be hard to guess and should be changed on a regular basis. It would be possible to use one key for all tags. This however would significantly lower security, since the key only has to be learned once by an attacker and that would compromise the security of all tags.

Data encryption

This means that the data on the tag is encrypted, most commonly in the enterprise sub system. That means that the data will be encrypted and then stored on the tag. It is now much harder to make use of the data after the attacker gained unauthorised access. The encryption will cause a delay that might be unacceptable because the truck do not stop while being weighted, but this has to be tested. If the encryption is too slow, stripped down cryptography could be used. The encryption would make it much harder to provide mobile internet independent access to the data for the police. The mobile readers would have to be able to perform cryptographic functions. Again the key management problem would occur. It would also be possible to let a tag perform cryptographic commands. This, however, would not mitigate the key management problem, but it would lower the requirements for the mobile readers. Tags that support complex encryption are likely to be more expensive, as mentioned in chapter 2.1.1..

Authentication Mechanism

This is used to make sure that a reader communicates with the correct tag and vice versa. Or both at the same time is possible. The most important use for the project would be to make sure that the tag is read by authorised readers. This would much mitigate the risk of unauthorised access by rough readers and provides a high level assurance in transactions between tag and reader.

5.3.2 RF Interface Protection

Transmission Power Adjustment

A stated in [12], this means to lower the power of the reader in order to adjust the read range. This significantly lowers the coherence risk mentioned above, because the range of the reader would be limited, which results in a lower risk that more than one truck will be in that range. It also mitigates the risk of the communication being eavesdropped, and interference with other radio origins is less likely. But the read range has to be far reaching enough so that the registration also works during heavy rain and thunder-storm or otherwise the reader could fail to read the ID of trucks on the weighting machine.

Electromagnetic Shielding

This could be used to limit the direction whereto the reader is able to register tags. Shielding material could be constructed around the reader. Correctly deployed the reader would only be able to register tags that are roughly in the direction of the weighting machine. But it should not be too tight because the trucks do not stop on the weighting machine, so this countermeasure would limit the possible time frame for registration. Otherwise legitimate tags cannot be registered. This also would mitigate the likelihood of the coherence risk. It would also mitigate the risk of eavesdropping and interference.

5.3.3 Good Software Engineering Practices

As stated in [11] we quote the following steps that RFID middleware designers and administrators should take to mitigate the risks of viruses and SQL injection attacks.

1. **Bounds checking.** Bounds checking is the means of detecting whether or not an index lies within the limits of an array. It is usually performed by the compiler, so as not to induce runtime delays. Programming languages that enforce run-time checking, like Ada, Visual Basic, Java, and C#, do not need bounds checking. However, RFID middleware written in other languages should be compiled with bounds-checking enabled.

2. **Sanitise the input.** Instead of explicitly stripping off special characters, it is easier to only accept data that contains the standard alphanumeric characters (0-9,a- z,A-Z). However, it is not always possible to eliminate all special characters. For example,

an RFID tag on a library book might contain the publishers name, OReilly. Explicitly replicating single quotes, or escaping quotes with backslashes will not always help either, because quotes can be represented by Unicode and other encodings. It is best to use built-in data sanitising functions, like pg escape bytea() in Postgres and mysql real escape string() in MySQL.

3. **Disable back-end scripting languages.** RFID middleware that uses HTTP can mitigate script injection by eliminating scripting support from the HTTP client. This may include turning off both client-side (i.e. Javascript, Java, VBScript, ActiveX, Flash) and server-side languages (i.e. Server-Side Includes).

4. **Limit database permissions and segregate users.** The database connection should use the most limited rights possible. Tables should be made read-only or inaccessible, because this limits the damage caused by successful SQL injection attacks. It is also critical to disable the execution of multiple SQL statements in a single query.

5. **Use parameter binding.** Dynamically constructing SQL on-the-fly is dangerous. Instead, it is better to use stored procedures with parameter binding. Bound parameters (using the PREPARE statement) are not treated as a value, making SQL injection attacks more difficult.

6. **Isolate the RFID middleware server.** Compromise of the RFID middleware server should not automatically grant full access to the rest of the back-end infrastructure. Network configurations should therefore limit access to other servers using the usual mechanisms (i.e. DMZs)

7. **Code review.** RFID middleware source code is less likely to contain exploitable bugs if it is frequently scrutinised. Home grown RFID middleware should be critically audited. Widely distributed commercial or open-source RFID middleware solutions

are less likely to contain bugs.

5.4 Legal Controls

As stated in [4] and based on the European Data protection Directive [3] the following principles hold in regard to data processing.

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Table 5.1: RFID Controls Summary , [12]

Control	Business Process Risk	Business Intelligence Risk	Privacy Risk
RFID Usage Policy	X	X	X
IT Security Policy	X	X	
Agreements with External Organisations	X	X	X
Minimising Sensitive Data Stored on Tags	X	X	X
Physical Access Control	X	X	
Operator and Administrator Training	X	X	
Tag Access Control	X	X	X
Data encryption	X	X	X
Authentication Mechanism	X	X	X
Transmission Power Adjustment		X	
Electromagnetic Shielding		X	X
Good Software Engineering Practices	X	X	X

These privacy principles of the Data Protection Directive are implemented specifically for Sweden in the Personal Data Act (1998:204). The Personal Data Act is available at [5]. The mapping of which control mitigates which risk is illustrated in table 5.1

Chapter 6

Good practices to improve security in Project Stolpen

In this chapter we will take a look at good and possible countermeasures for Project Stolpen which will mitigate the risks with a reasonable effort.

6.1 Responsibilities

It is very important that it is known what the responsibilities are in case a security breach or a system failure happens. Only when that is clear, help can be organised quickly and the downtime can be kept small. Thus it helps saving money. It has to be thought about who is responsible at what time and for what exactly. The night has also to be covered. The according person will be responsible for dispatching the problem as soon as possible.

6.2 How to get Help

It is very important that the person in charge knows how to get help as soon as possible. Telephone numbers have to be easily available so no time will be wasted while thinking about who for example will repair or replace a reader. The optimal thing would be that the responsible person could do most of the reparation by oneself.

6.3 Documentation

All information about the system has to be quickly accessible so that in case of emergency the person in charge does not have to search for it and waste time while doing it.

6.4 Transmission Power Adjustment

The power of the readers at the station should be lowered carefully, so that the range is limited to the station. This will reduce the coherence risk. For details about this we refer to the according clause in 4.1.2.

6.5 Secure Internet-Connected Computers

Firewalls have to be used and maintained. Patches have to be installed as fast as possible so avoid being vulnerable to security holes. An expert for computer security should be hired to evaluate and improve the security of the servers.

6.6 Future

As it is planed to store data on the tag itself, the data stored on the tag should be minimised. Because data that is not on the tag can not be unauthorised read and misused therefore it is safer.

Chapter 7

Conclusion

Project Stolpen was not planned with security in mind. No security scheme whatsoever is implemented. In this thesis it was shown that different kinds of risks exist and were identified together with potential impacts. An attacker could quite easily avert all radio communication. He could eavesdrop on all communications, no means at all against that are in place. The identifiers could be cloned so that one trucks appears as another to the system. All kind of frauds are possible. Even without an attacker the system is quite vulnerable to produce incorrect data. This is because of the risk that the station cannot be sure whether it registered the correct truck or a truck that is in range of the station. In the beginning that risk may be small, but the more the system is used, the more false data might be inserted into the database. To lower that risk without much efforts, the communication range of the stations should be lowered so that only trucks very close to the station may be registered. But this only lowers the risk, it does not eliminate it. An effective security policy has to be implemented. In this thesis a number of countermeasures were given, that should be implemented as soon as possible in order to limit the risks and associated costs due to security breaches. Preferably, security should be introduced as long as the system is still in design and trial phase, as introducing security at a later stage will be more complex and expensive.

References

[1] 13,56 mhz smartlabel, http://de.wikipedia.org/wiki/bild:transponder2.jpg, 2006.

[2] Auto id center/epcglobal; intermec.

[3] Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://www.cdt.org/privacy/eudirective/.

[4] The eight principles of data protection, http://www.e-lindsey.gov.uk/council/dp-and-foi/dp-principles.cfm.

[5] The personal data act, http://www.datainspektionen.se/pdf/ovrigt/pul-eng.pdf, 1998.

[6] Generation 2 - a user guide, www.adt.com/wscomm/images/referencelibrary/gen2userguide.pdf, 2005.

[7] M. Szydlo A. Juels, R. Rivest. The blocker tag: Selective blocking of rfid tags for consumer privacy. *8th ACM Conference on Computer and Communications Security*, 2003.

[8] Raghu Das. Rfid tag sales in 2005, http://www.idtechex.com/products/en/articles/00000398.asp, 2006.

[9] Ari Juels. Rfid security and privacy: A research survey. Technical report, RSA Laboratories, 2005.

[10] Tim Kröner. Rfid kosten, http://www.rfid-journal.de/rfid-kosten.html, 2006.

[11] Andrew S. Tanenbaum Melanie R. Rieback, Bruno Crispo. Is your cat infected with a computer virus? *IEEE PerCom*, 2006.

[12] NIST (National Institute of Standards and Technology). Guidance for securing radio frequency identification(rfid) systems. September 2006.

[13] KG Paulsson. Project stolpen - a presentation, 2006, unpublished.

[14] B. Rosenberg S. Garfinkel. *RFID Applications, Security, and Privacy.* Addison-Wesley, 2005.

[15] Ravi Pappu Simson L. Garfinkel, Ari Juels. Rfid privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy, pages 34-43*, May/Juny 2005.

[16] A. Westin. *Privacy and Freedom.* New York, 1987.